สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

รายงานการวิจัยฉบับสมบูรณ์

โครงการจัดตั้งห้องปฏิบัติการวิจัยและพัฒนา

Mobile Computing and Sensor Networks

ผู้วิจัย

ดร. สุเมธ ประภาวัต

QCH
ส443ค
2556

ตรหมู่.....
เลขทะเบียน 138020
วัน.เดือน.ปี 8 ก.ย. 2558

12681659
.b.....
.i.....

ได้รับทุนสนับสนุนงานวิจัยจากเงินรายได้ ประจำปีงบประมาณ 2556
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รายละเอียดโครงงานวิจัย

ชื่อโครงการ (ภาษาไทย) โครงการจัดตั้งห้องปฏิบัติการวิจัยและพัฒนา Mobile Computing and Sensor Networks

ชื่อโครงการ(ภาษาอังกฤษ) Mobile Computing and Sensor Networks Laboratory

แหล่งเงิน เงินรายได้ คณะเทคโนโลยีสารสนเทศ สจล.

ประจำปีงบประมาณ 2556 จำนวนเงินที่ได้รับการสนับสนุน 200,000 บาท

ระยะเวลาทำการวิจัย 18 เดือน ตั้งแต่ 1 ตุลาคม 2555 ถึง 31 มีนาคม 2557

หัวหน้าโครงการ

ชื่อ: ดร. สุเมธ ประภาวัต
หน่วยงาน: คณะเทคโนโลยีสารสนเทศ สจล.
Email: sumet@it.kmitl.ac.th

คำสำคัญ (Keywords): เครือข่ายไร้สายเฉพาะกิจ, Mobile Computing, Mobile Adhoc Networks, MANET, Delay Tolerant Networks, DTN, Multipath Networks, Multipath Routing

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทคัดย่อ

ในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทในชีวิตประจำวันอย่างมาก ไม่ว่าจะเป็นการใช้อินเตอร์เน็ตในการสืบค้นข้อมูลต่างๆ เป็นสื่อกลางในการติดต่อสื่อสารทั้งระยะใกล้และระยะไกล รวมทั้งเป็นสื่อสำหรับการเรียนการสอนและให้ความบันเทิงได้ในเวลาเดียวกัน ดังนั้นเพื่อรองรับการเจริญเติบโตของระบบเครือข่ายอินเตอร์เน็ต นักวิจัยจากสถาบันต่างๆจึงได้ให้ความสนใจและมีความพยายามที่จะพัฒนาระบบเครือข่ายให้มีประสิทธิภาพมากยิ่งขึ้น หรือยังคงให้บริการได้แม้โครงสร้างเครือข่ายพื้นฐานจะไม่สามารถทำงานได้ปกติ เป็นต้น

นอกจากนี้ การพัฒนาระบบเครือข่ายเชิงประยุกต์ก็ยังคงได้รับความสนใจมากขึ้นเช่นกัน ยกตัวอย่างเช่นการประยุกต์ใช้ระบบเครือข่ายผสานเข้ากับระบบระบุพิกัดบนพื้นโลก(GPS) เพื่อสร้างเป็นระบบนำทางสำหรับยานพาหนะ การใช้ระบบเครือข่ายในการติดต่อสื่อสาร สร้างสรรค์สังคมออนไลน์ที่สามารถใช้งานผ่านสมาร์ทโฟน หรือ การประยุกต์ใช้งานระบบเครือข่ายเพื่อใช้ในการรักษาความปลอดภัยตามพื้นที่ต่างๆโดยการใช้กล้องวงจรปิด หรือระบบการตรวจสอบลายนิ้วมือ

คณะเทคโนโลยีสารสนเทศที่เล็งเห็นถึงศักยภาพและโอกาสในการเติบโตของระบบเครือข่ายจึงได้มีแนวคิดในการจัดตั้งห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์ค (Mobile Computing and Sensor Networks) เพื่อสร้างงานวิจัยเพื่อส่งเสริมให้วิทยาศาสตร์มีความก้าวหน้ามากขึ้นและรวบรวมองค์ความรู้เกี่ยวกับระบบเครือข่ายเพื่อถ่ายทอดให้นักศึกษาที่สนใจ รวมทั้งสนับสนุนอุปกรณ์โมบายล์ อย่างเช่น สมาร์ทโฟน หรือแท็บเลตต่างๆ ในการนำไปใช้ในการศึกษาหรือทดลองแอพพลิเคชั่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Abstract

Information and communication technology (ICT) has advanced rapidly in recent years. It plays an important role in providing communication services for connecting people and information access. Moreover, Internet is commonly used for entertainment and be a source for self-learning. Many researchers try to enhance network technology and applications such as GPS navigation system for vehicles and social network application on smartphone. In addition, a self-configuring infrastructureless network of mobile devices connected by wireless is also a new research trend to facilitate robust and sustainable communication networks requiring no network infrastructure.

To respond the growth of demand and technology for next generation networks, the research laboratory for Mobile Computing and Sensor Networks is established to conduct advanced researches and innovations regarding mobile network technologies and applications, as well as other relevant fields. Research environment, including necessary knowledge and facilities are provided for interested faculty staff, researchers, and students. The outcomes of our research expected to provide theoretical and practical contributions are published in international conferences and national conferences.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

โครงการวิจัยนี้ได้รับการสนับสนุนทุนวิจัย จากเงินรายได้ประจำปีงบประมาณ 2556 คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เพื่อจัดตั้งห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์ค (Mobile Computing and Sensor Networks) ทำให้มีห้องปฏิบัติการวิจัยเฉพาะทาง ที่สนับสนุนบุคลากรคณะให้สามารถดำเนินการวิจัยเพื่อพัฒนางานวิจัยขั้นสูงได้เป็นผลสำเร็จ โดยวัดได้จากผลงานวิจัยที่ได้รับการเผยแพร่ในงานประชุมวิชาการ และจำนวนนักศึกษาที่มาร่วมทำวิจัยจนกระทั่งได้ผลงานไปใช้ประกอบการสำเร็จการศึกษา

คณะผู้วิจัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

	หน้า
รายละเอียดของโครงการวิจัย	i
บทคัดย่อภาษาไทย	ii
บทคัดย่อภาษาอังกฤษ	iii
กิตติกรรมประกาศ	iv
สารบัญ	v
สารบัญภาพ	viii
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์	1
1.3 ขอบเขตงานวิจัย	2
1.4 ระเบียบวิจัย	2
1.5 ประโยชน์ที่คาดว่าจะได้รับ	2
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง	3
2.1 เทคโนโลยีเครือข่ายไร้สายเฉพาะกิจที่ถูกพัฒนาขึ้นโดยมีพื้นฐานมาจากโปรโตคอล Dynamic Source Routing	4
2.1.1 Ad-Hoc On-demand Distance Vector Routing (AODV)	5
2.1.2 Optimized Link State Routing Protocol (OLSR)	6
2.1.3 Multiple Source Routing Protocol (MSR)	7
2.1.4 Split Multipath Routing Protocol (SMR)	8
2.1.5 Location-Aided Routing Protocol (LAR)	9
2.1.6 Distance Routing Effect algorithm for mobility (DREAM)	10

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

2.2 เทคโนโลยีเครือข่ายไร้สายเฉพาะกิจที่ถูกพัฒนาขึ้นโดยมีพื้นฐานมาจากโปรโตคอล Delay-Tolerant Network 11

2.2.1 Anti-Entropy และ n-Epidemic Routing 12

2.3 งานวิจัยและเทคโนโลยีที่สามารถนำไปสู่การประยุกต์ 14

2.3.1 เทคโนโลยีไวไฟไดเร็ค (Wi-Fi direct) 14

2.3.2 เทคโนโลยีระบุตำแหน่งบนพื้นโลก 15

บทที่ 3 งานวิจัยที่ได้ดำเนินการ 17

3.1 การปรับปรุงการแบ่งโหลดเพื่อกระจายข้อมูลหลายทางบนเครือข่ายเฉพาะกิจเคลื่อนที่ 17

3.2 การศึกษาความเป็นไปได้ในการลดโอเวอร์เฮดบนระบบเครือข่ายไร้สายเฉพาะกิจโดยการสร้างเงื่อนไขในการจำกัดการกระจายข้อมูลในขั้นตอนการค้นหาเส้นทาง 18

3.3 การปรับปรุงกลไกการแพร่กระจายข้อความเพื่อลดการแลกเปลี่ยนข้อมูลบนเครือข่ายดีทีเอ็น 21

3.4 การปรับปรุงกลไกค้นหาเกตเวย์เพื่อลดโอเวอร์เฮดจากการแลกเปลี่ยนข้อมูลในเครือข่ายเฉพาะกิจ 25

3.5 การกระจายโหลดเพื่อการส่งข้อมูลและรองรับการทำงานของทีซีพีเน็ตเวิร์ค 29

3.6 การพัฒนาเทคโนโลยีการสื่อสารผ่านดาวเทียมเพื่อใช้ในสถานการณ์ภัยพิบัติ 30

3.7 เครือข่ายเฉพาะกิจแบบดีทีเอ็นบนสมาร์ทโฟนสำหรับการสื่อสารในสถานการณ์ภัยพิบัติ 31

3.8 การศึกษาการประยุกต์ใช้เครือข่ายเซนเซอร์ในระบบควบคุมปัจจัยการเพาะปลูกอัตโนมัติ 32

3.9 การประยุกต์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉินแล้วตำแหน่งที่อยู่เพื่อขอรับบริการรถนำส่งและบริการทางการแพทย์ 34

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

หน้า

3.10 การประยุกต์ใช้สมาร์ทโฟนเพื่อการพิสูจน์ตัวตนด้วยข้อมูลพิกัดจีพีเอส 37

บทที่ 4 บทสรุป 39

บรรณานุกรม 40



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ

		หน้า
รูปที่ 2.1	แสดงตัวอย่างของ Mobile Ad hoc Networks[2]	3
รูปที่ 2.2	ตัวอย่างของเราติ้งโพรโทคอล DSR และ AODV	4
รูปที่ 2.3	ตัวอย่างของโพรโทคอลค้นหาเส้นทาง OLSR	7
รูปที่ 2.4	Location-Aided routing protocol scheme	9
รูปที่ 2.5	Distance Routing Effect algorithm for mobility scheme	10
รูปที่ 2.6	แสดงตัวอย่างของ Delay-Tolerant Networks[9]	11
รูปที่ 2.7	แสดงตัวอย่างกระบวณการทำงานของดีทีเอ็น [9]	12
รูปที่ 2.8	แสดงตัวอย่างลักษณะการเชื่อมต่อของ Wi-Fi Direct[15]	14
รูปที่ 2.9	แสดงตัวอย่างการหาเส้นทางแบบ Multi-Hop Routing ด้วย Wi-Fi Direct[15]	14
รูปที่ 2.10	Triangulation method	15
รูปที่ 2.11	หน้าจออุปกรณ์นำทางด้วยระบบ GPS	16
รูปที่ 3.1	Proposed protocol scheme	19
รูปที่ 3.2	กราฟแสงปริมาณโอเวอร์เฮดในระบบเครือข่าย	20
รูปที่ 3.3	กราฟแสดงอัตราความสำเร็จในการส่งข้อมูล	21
รูปที่ 3.4	กลยุทธ์การส่งข้อความแบบ n-Epidemic	22
รูปที่ 3.5	กลยุทธ์การส่งข้อความแบบ n-Anti Entropy	23
รูปที่ 3.6	กราฟแสดงผลรวมของจำนวนแพ็คแก็ตที่ถูกส่งออก	23
รูปที่ 3.7	กราฟแสดงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา	24
รูปที่ 3.8	แสดงตัวอย่างการหากลุ่มโหนด MPR	27
รูปที่ 3.9	แสดงผลการทดลองด้านจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด	27
รูปที่ 3.10	แสดงผลการทดลองด้านเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด	28

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

หน้า

รูปที่ 3.11	Block Diagram ของระบบ	33
รูปที่ 3.12	ภาพรวมของระบบ	34
รูปที่ 3.13.	หน้าจอปฏิบัติงานของเจ้าหน้าที่สำหรับรับการแจ้งเหตุฉุกเฉินต่างๆ	35
รูปที่ 3.14	ตารางเปรียบเทียบเส้นทางการนำส่งผู้ป่วย	35
รูปที่ 3.15	ข้อมูลเส้นทางที่ใช้ในการนำส่งผู้ป่วย	36
รูปที่ 3.16.	ภาพจำลองระบบการทำงาน	38

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญ

ในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทในชีวิตประจำวันอย่างมาก ไม่ว่าจะเป็นการใช้อินเตอร์เน็ตในการสืบค้นข้อมูลต่างๆ เป็นสื่อกลางในการติดต่อสื่อสารทั้งระยะใกล้และระยะไกล รวมทั้งเป็นสื่อสำหรับการเรียนการสอนและให้ความบันเทิงได้ในเวลาเดียวกัน ดังนั้นเพื่อรองรับการเจริญเติบโตของระบบเครือข่ายอินเตอร์เน็ต นักวิจัยจากสถาบันต่างๆจึงได้ให้ความสนใจและมีความพยายามที่จะพัฒนาระบบเครือข่ายให้มีประสิทธิภาพมากยิ่งขึ้นไม่ว่าจะเป็นด้านประสิทธิภาพการทำงานของระบบเครือข่าย หรือการรองรับการทำงานในสภาวะที่หลากหลาย ยกตัวอย่างเช่นระบบเครือข่ายที่มีความทนทานต่อสภาพแวดล้อมและสามารถให้บริการได้แม้จะอยู่ในสถานการณ์ฉุกเฉิน เป็นต้น

จากที่กล่าวมาข้างต้น คณะเทคโนโลยีสารสนเทศจึงเล็งเห็นประโยชน์ในการจัดตั้งห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์ค (Mobile Computing and Sensor Networks) เพื่อให้ความรู้แก่นักศึกษาที่สนใจและส่งเสริมให้เกิดความก้าวหน้าในวงการวิทยาศาสตร์ รวมทั้งผลักดันให้เกิดการสร้างผลงานที่เกี่ยวข้องกับระบบเครือข่ายออกสู่สังคม อาธิเช่น ระบบเครือข่ายไร้สายเฉพาะกิจ(MANET) ที่ใช้สมาร์ทโฟนที่สามารถพบเห็นได้ในชีวิตประจำวันมาสร้างเป็นระบบเครือข่ายที่ใช้ในการติดต่อสื่อสารในกรณีที่ระบบเครือข่ายแบบโครงสร้างไม่สามารถใช้งานได้ งานวิจัยระบบเครือข่ายเชิงประยุกต์ที่สามารถนำไปสนับสนุนให้กับหน่วยงานภาครัฐหรือภาคเอกชนเพื่อยกระดับการใช้ชีวิตของประชาชน การสร้างแนวคิดหรือโปรโตคอลใหม่ๆที่เกี่ยวข้องกับระบบเน็ตเวิร์ค นอกจากนี้ห้องปฏิบัติการยังคงสนับสนุนและให้บริการอุปกรณ์โมบายล์เพื่อนำไปใช้ในการทดลองหรือทดสอบการทำงานของแอพพลิเคชั่นต่างๆอีกด้วย

1.2. วัตถุประสงค์

1. เพื่อสร้างงานวิจัยที่เกี่ยวข้องกับอุปกรณ์โมบายล์ เครือข่ายอุปกรณ์โมบายล์ หรือเครือข่ายเซนเซอร์
2. เพื่อสร้างงานพัฒนาระบบสารสนเทศบนอุปกรณ์โมบายล์ หรือเครือข่ายเซนเซอร์
3. เพื่อสนับสนุนการพัฒนาเทคโนโลยีเครือข่ายอุปกรณ์โมบายล์ หรือเครือข่ายเซนเซอร์
4. เพื่อให้บริการอุปกรณ์สำหรับทดสอบการทำงานของแอพปลิเคชั่นบนอุปกรณ์โมบายล์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.3. ขอบเขตการดำเนินงาน

จัดตั้งห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์ค รวมทั้งผลิตผลงานวิจัยที่เป็นที่ยอมรับทั้งในระดับประเทศและระดับนานาชาติ และพัฒนาองค์ความรู้ให้แก่นักศึกษาที่มีความสนใจในด้านระบบเครือข่าย

1.4. ระเบียบการวิจัย

- ศึกษาทฤษฎีและเทคโนโลยีที่เกี่ยวข้องที่เป็นพื้นฐานในงานวิจัย
- ดำเนินการวิจัยและพัฒนาองค์ความรู้เกี่ยวกับเทคโนโลยีเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์ค
- จัดหาอุปกรณ์เพื่อสนับสนุนการทำวิจัย
- ทำการทดลอง วิเคราะห์ผล และอภิปรายผล เพื่อนำไปสู่การเสนอผลงานวิชาการระดับชาติและนานาชาติ

1.5. ประโยชน์ที่คาดว่าจะได้รับ

คณะเทคโนโลยีสารสนเทศพัฒนางานวิจัยที่มีศักยภาพมากพอที่สามารถทำให้นักศึกษาสามารถสำเร็จการศึกษาในระดับปริญญาตรีหรือสูงขึ้นไป และสร้างงานวิจัยที่เป็นที่ยอมรับจากองค์กรภายนอก ซึ่งส่งเสริมภาพลักษณ์ของคณะฯและสถาบันฯ ด้านความเป็นเลิศทางวิชาการ รวมถึงการมีบทบาทในสังคม

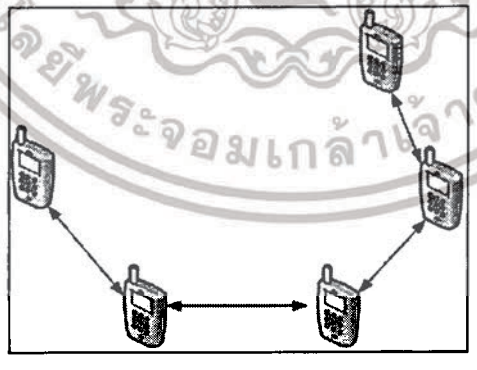
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

สำหรับห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์คนั้น ได้มีการศึกษาข้อมูลและความรู้เกี่ยวกับระบบเครือข่ายโดยสามารถแบ่งออกได้เป็นสองประเภทคืองานวิจัยเชิงทฤษฎีและหลักการที่เกี่ยวข้องในหัวข้อย่อย 2.1-2.2 และงานวิจัยเชิงประยุกต์ในหัวข้อ 2.3 โดยเนื้อหาที่จะกล่าวถึงในส่วนของงานวิจัยจะมีพื้นฐานมาจากระบบเครือข่ายไร้สายเฉพาะกิจเป็นหลัก ดังนั้นในช่วงต้นจะขอกล่าวถึงการทำงานพื้นฐานของเครือข่ายไร้สายเฉพาะกิจก่อน

เครือข่ายไร้สายเฉพาะกิจ (Mobile Ad Hoc Network - MANET) คือ ระบบพึ่งพาตัวเองของโหนดเคลื่อนที่แบบไร้สาย (Wireless Mobile Node) ที่สามารถเคลื่อนที่และจัดการตัวเองในขณะกำลังสื่อสารได้อย่างอิสระ ดังนั้นการเชื่อมต่อระหว่างกันของโหนดฯจึงมีการเปลี่ยนแปลงตลอดเวลา ด้วยเหตุนี้จึงเกิดการรวมกลุ่มของโหนดฯ เพื่อสร้างเครือข่ายสื่อสารชั่วคราวที่ไม่จำเป็นต้องมีโครงสร้างพื้นฐาน เช่น เสากระจายสัญญาณ (Base Station) และเปลี่ยนการควบคุมของศูนย์กลางการควบคุม (Centralized Administration) เป็นการอาศัยความร่วมมือกันระหว่างโหนดฯในการส่งต่อข้อมูล โดยโหนดฯจะปฏิบัติตัวเองเป็นเสมือนเราเตอร์ (Router) ส่งต่อข้อมูลระหว่างจากโหนดฯหนึ่งไปยังอีกโหนดฯหนึ่ง ต่อเนื่องไปจนถึงโหนดปลายทาง เรียกการส่งข้อมูลลักษณะนี้ว่า มัลติฮอป (Multi-Hop) เพราะฉะนั้นเครือข่ายไร้สายเฉพาะกิจจึงมีความยืดหยุ่น เพราะสามารถสร้างได้ทุกพื้นที่และทุกเวลาที่ต้องการ[1][2]



รูปที่ 2.1 แสดงตัวอย่างของ Mobile Ad hoc Networks[2]

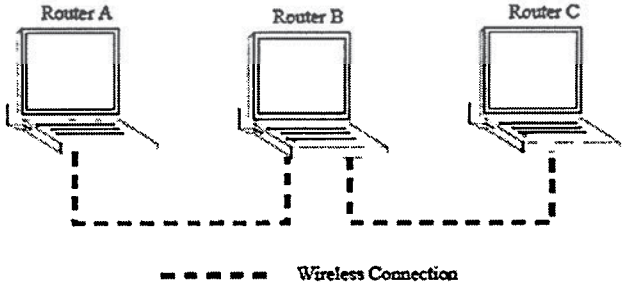
ในระบบเครือข่ายไร้สายเฉพาะกิจนั้น จำเป็นต้องมีโปรโตคอลหรือวิธีการที่ใช้ในการส่งข้อมูลโดยที่ปราศจากการช่วยเหลือของเสาสัญญาน ในส่วนถัดไปจะกล่าวถึงโปรโตคอลที่มีการศึกษาและถูกนำมาพัฒนาในห้องปฏิบัติการวิจัย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1 เทคโนโลยีเครือข่ายไร้สายเฉพาะกิจที่ถูกพัฒนาขึ้นโดยมีพื้นฐานมาจากโปรโตคอล Dynamic Source Routing

Dynamic Source Routing (DSR) [3] เป็น distance-vector protocols สำหรับเครือข่ายสื่อสารเฉพาะกิจ เนื่องจากเมื่อโหนดในระบบเครือข่ายไร้สายเฉพาะกิจต้องการส่งแพ็คเก็ตไปยังปลายทาง และโหนดต้นทางไม่รู้จักเส้นทางที่สามารถไปยังปลายทางได้ โหนดต้นทางจะเริ่มต้นขั้นตอนการค้นหาเส้นทาง ดังนั้น DSR จึงจัดเป็น โพรโทคอลแบบรีแอกทีฟ โดยข้อดีอย่างหนึ่งของ DSR คือไม่ต้องมีการส่งข้อมูลเส้นทางเป็นคาบ (Periodic Routing Packet) และการที่ DSR ทำการค้นหาเส้นทางเมื่อต้องการส่งข้อมูล (On-demand) นั้นมีส่วนช่วยในการควบคุมโอเวอร์เฮด (Overhead) ในเครือข่ายได้อีกด้วย

ในโปรโตคอล DSR มีกลไกหลักอยู่ 2 อย่าง คือ การค้นหาเส้นทาง (Route Discovery) และการบำรุงรักษาเส้นทาง (Route Maintenance) ในรูปที่ 2.2 แสดงให้เห็นตัวอย่างสำหรับ DSR โดยจากภาพกำหนดให้โหนด A โหนด B และโหนด C ทำงานในเครือข่ายสื่อสารเฉพาะกิจโดยที่โหนด A และโหนด C ไม่เชื่อมต่อกัน แต่ทั้งคู่เชื่อมต่อกับโหนด B สมมติว่าในตอนเริ่มต้นแคชเส้นทาง (Route Caches) ของโหนดทุกตัวยังว่างเปล่าอยู่ เมื่อโหนด A ต้องการส่งแพ็กเก็ต (Packets) ไปยังโหนด C โหนด A จะเริ่มบรอดแคสต์ (Broadcast) เพื่อเริ่มต้นการหาเส้นทาง โดยเมื่อโหนด B ได้รับการร้องขอ (เพราะอยู่ในช่วงการสื่อสารของโหนด A) แต่ทว่าโหนด B ยังไม่มีรายการเส้นทาง (Route Entry) ของโหนด C ที่เป็นปลายทางของการร้องขออยู่ในแคชเส้นทาง ดังนั้นโหนด B จึงต้องทำการบรอดแคสต์การร้องขอซ้ำ (Rebroadcasts Request) ที่ได้รับจากโหนด A โดยทำเปลี่ยนไอดี (ID) ในการร้องขอจากของโหนด A เป็นของตัวเอง (โหนด B) และเมื่อโหนด C ได้รับข้อความบรอดแคสต์คำร้องขอเส้นทาง ที่มาจากโหนด B จะตรวจสอบไอดีปลายทางว่าตรงกับไอดีของตัวเองหรือไม่ ถ้าตรงกันเส้นทางจากโหนด A ถึงโหนด C ก็จะถูกค้นพบขึ้น และเพื่อช่วยให้โหนดทุกตัวมี รายการเส้นทางที่ตรงกัน ในกรณีที่การเชื่อมโยงเป็นแบบสองทิศทาง (bi-directional) โหนด C จะส่งรายการเส้นทางกลับไปยังเส้นทางที่ได้รับการร้องขอเส้นทางซึ่งขั้นตอนนี้เป็นไปได้เพราะ ID ของโหนดตัวกลางทุกตัวนั้นมี ID ตรงกับที่อยู่ในการร้องขอเส้นทางซึ่งโหนดตัวกลางสามารถสร้าง ตารางเส้นทางได้เมื่อได้รับการตอบจาก C ดังนั้นเส้นทางจาก A ถึง C ถูกสร้างขึ้น



รูปที่ 2.2 ตัวอย่างของเราติ้งโพรโทคอล DSR และ AODV

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในระหว่างขั้นตอนค้นหาเส้นทางแต่ละโหนดจะทำการเก็บ ID ที่เพิ่งพบเมื่อเร็วๆนี้โดยการหลีกเลี่ยงการประมวลผลคำขอของเส้นทางเดียวกัน โดยการร้องขอนั้นจะถูกยกเลิกหากการร้องขอนั้นถูกประมวลผลไปในช่วงเวลาที่ผ่านมาไม่นาน เนื่องจากถือว่าเป็นรายการที่ซ้ำกัน และถ้าโหนดได้รับคำขอแล้วพบว่าไอดีของตัวเองอยู่ในรายการของโหนดตัวกลางโดยแต่ละโหนดจะไม่สนใจการร้องขอนี้เพื่อหลีกเลี่ยงการเกิดลูป

ขั้นตอนบำรุงรักษาเส้นทาง (route maintenance) จะใช้เมื่อเส้นทางกลายเป็นเส้นทางที่ไม่ถูกต้องเนื่องจากการเคลื่อนไหวที่ไม่แน่นอนของโหนดต่าง ๆ โดยโหนดแต่ละโหนดจะทำการตรวจสอบเส้นทางที่จะใช้เพื่อส่งต่อแพ็คเก็ต เมื่อเส้นทางถูกตัดขาด โหนดที่ทราบจะส่ง route error packet ทันทีเพื่อป้องกันเส้นทางที่เกี่ยวข้องไม่ให้ได้รับข้อมูลที่ผิด ดังนั้นเส้นทางที่ไม่ถูกต้องจะถูกยกเลิกอย่างรวดเร็ว เพื่อที่จะควบคุมการส่งข้อความควบคุม (control message) ให้มีความน่าเชื่อถือโปรโตคอล DSR จะอาศัยทั้งโพรโทคอลใน MAC Layer เพื่อรับประกันการจัดส่งและกลไกการส่งข้อความควบคุมซ้ำ (retransmits control message) เนื่องจากโปรโตคอล DSR เป็นโพรโตคอลแบบรีแอกทีฟเพราะฉะนั้นจึงไม่สามารถสรุปได้ว่าสามารถเชื่อมต่อปลายทางได้หรือ เส้นทางขาดหายไปจึงทำให้มีโอเวอร์เฮดมากกว่าการไม่มี MAC layer มาสนับสนุนการรับประกันการจัดส่ง และนี่คือปัญหาพื้นฐานสำหรับ โปรโตคอลค้นหาเส้นทางแบบรีแอกทีฟเพราะเมื่อไม่ได้รับข้อความตอบกลับ โหนดที่ใช้โปรโตคอลค้นหาเส้นทางแบบรีแอกทีฟจะไม่สามารถแบ่งข้อแตกต่างระหว่างการมีข้อผิดพลาดในการส่ง หรือกรณีของโหนดไม่สามารถเข้าถึงได้ ทั้งนี้โปรโตคอลค้นหาเส้นทางแบบรีแอกทีฟพยายามให้มีการทำ retransmission จำนวนน้อยๆเพื่อแก้ปัญหานี้ จึงกลายเป็นการเพิ่มโอเวอร์เฮดแต่สำหรับโพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟจะมีระยะเวลาในการบรอดแคสต์ข้อความควบคุมและ ลบรายการเส้นทางถ้าหมดเวลาที่กำหนดไว้ (time out) ดังนั้นจึงไม่มีปัญหานี้ แต่การที่ส่งการบรอดแคสต์ข้อความควบคุมเป็นระยะก็จะทำให้เพิ่มโอเวอร์เฮดด้วย

2.1.1 Ad-Hoc On-demand Distance Vector Routing (AODV)

Ad Hoc On-Demand Distance Vector Routing (AODV) [4] เป็นโปรโตคอลค้นหาเส้นทางแบบรีแอกทีฟในเครือข่ายสื่อสารเฉพาะกิจซึ่งคล้ายกับ DSR โดย AODV จะบรอดแคสต์เพื่อค้นหาเส้นทางในการเชื่อมต่อ โดยมีความแตกต่างกับ DSR คือ การนำจำนวน hop มาใช้ในการคำนวณค่าใช้จ่าย (cost) ในการบันทึกเส้นทาง (route record) โดยโหนดตัวกลางจะตั้งค่าเส้นทางในการเชื่อมต่อชั่วคราวในกลไกการค้นหาเส้นทาง โดยเส้นทางนี้จะชี้ไปที่โหนดที่ส่งการร้องขอเส้นทาง ดังนั้นข้อความตอบกลับ (reply message) จะถูกส่งกลับไปยังจุดเริ่มต้นเมื่อเส้นทางจะถูกค้นพบ และเมื่อโหนดตัวกลางได้รับข้อความตอบกลับก็จะนำข้อมูลที่อยู่ในข้อความดังกล่าวมาตั้งค่ารายการเส้นทาง ให้ตรงกับโหนดที่ส่งต่อไปด้วย โดยการป้องกันไม่ให้ข้อมูลเส้นทางเก่าถูกนำมาใช้เป็นคำตอบในการร้องขอเส้นทางล่าสุดจึงนำค่าหมายเลขซีเควนซ์ของปลายทาง (Destination Sequence Number) มาใช้ในแพ็กเก็ตร้องขอเส้นทาง และแพ็กเก็ตตอบกลับเส้นทาง (Route Reply Packet) ซึ่งค่าหมายเลขซีเควนซ์ที่สูงกว่าหมายถึงการร้องขอเส้นทางล่าสุด สำหรับกลไกบำรุงรักษาเส้นทาง โดยในโปรโตคอล AODV นั้นจะคล้ายคลึงกับ DSR โดยข้อดีอย่างหนึ่งของ AODV คือเป็นโปรโตคอล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ค้นหาเส้นทางที่มีลักษณะแบบไม่เกิดการวนซ้ำ (loop-free) เนื่องจากมีการใช้ค่าหมายเลขซีเควนซ์ของปลายทางในการค้นหาเส้นทาง และมีการใช้อัลกอริทึม Bellman-Ford เข้ามาช่วยหลีกเลี่ยงปัญหา "count of infinity " ดังนั้นจึงมีการแก้ไขเส้นทางเมื่อเครือข่ายมีการเปลี่ยนแปลง (convergence time) ที่รวดเร็วเมื่อมีการเปลี่ยนแปลงโครงสร้างของเครือข่าย (Topology) ซึ่งจะเกิดขึ้นเมื่อโหนดมีการเคลื่อนย้ายในเครือข่าย

โครงสร้างตัวอย่างของ AODV แสดงในรูปที่ 2.2 แสดงให้เห็นถึงกลไกค้นหาเส้นทางของ AODV จากภาพกำหนดให้โหนด A โหนด B และโหนด C ทำงานในเครือข่ายสื่อสารเฉพาะกิจ โดยที่โหนด A และ C ไม่เชื่อมต่อกัน แต่ทั้งคู่เชื่อมต่อกับโหนด B เมื่อโหนด A ต้องการส่งแพ็คเกตไปยังโหนด C โดยโหนด A จะเริ่มต้นกลไกค้นหาเส้นทางจากการบรอดแคสต์การร้องขอเส้นทางซึ่งภายในในแพ็กเก็ตที่ส่งจะทำการเพิ่มค่าหมายเลขซีเควนซ์ของปลายทางอีก 1 จากเดิมที่ได้รับมา ตัวอย่างเช่น ค่าหมายเลขซีเควนซ์ของปลายทางสำหรับโหนด C ที่โหนด A เป็น 0x00000000 ดังนั้นแล้วค่าหมายเลขซีเควนซ์ของปลายทางในแพ็กเก็ตการค้นหาเส้นทางจะมีการเปลี่ยนแปลงเพิ่มขึ้น 1 เป็น 0x00000001 ทั้งนี้โหนดตัวกลางจะทำการตอบกลับมาถ้าโหนดนั้นๆทราบเส้นทางไปยังปลายทางไปยังเส้นทางที่มีค่าหมายเลขซีเควนซ์ของปลายทางที่ตรงกันหรือสูงกว่า เช่น โหนด B ไม่มีเส้นทางที่บันทึก (Route Record) สำหรับไปที่โหนด C ดังนั้นโหนด B จะเริ่มต้นโดยทำการตั้งค่าการเชื่อมโยงชั่วคราวกลับไปยังโหนด A และในขั้นตอนถัดไปโหนด B จะทำการเพิ่มจำนวนของhopไปอีก 1 และทำการบรอดแคสต์การร้องขอเส้นทางซ้ำออกไปเพื่อค้นหาเส้นทางไปยังโหนด C โดยถ้าโหนด C ได้รับการร้องขอเส้นทางแล้วจะทำการสร้างค่าหมายเลขซีเควนซ์ของปลายทางใหม่และทำการส่งคำตอบกลับเส้นทางพร้อมกับค่าหมายเลขซีเควนซ์ ใหม่ซึ่งถูกสร้างโดยโหนด C โดยโหนดต้นทางและโหนดตัวกลางจะทำการสร้างรายการเส้นทาง (Route Entry) ด้วยค่าหมายเลขซีเควนซ์ใหม่เมื่อได้รับการตอบกลับ (reply) โดยจำนวนของhopสามารถนำมาใช้เพื่อหาเส้นทางที่สั้นที่สุดได้ และถ้าโหนดได้รับการตอบกลับเป็นจำนวนสองครั้งหรือมากกว่านั้นด้วยค่าหมายเลขซีเควนซ์ของปลายทางที่ตรงกัน ซึ่ง AODV จะใช้รูปแบบการจัดการกับการส่งที่ไม่น่าเชื่อถือของข้อความควบคุมที่คล้ายกับ DSR

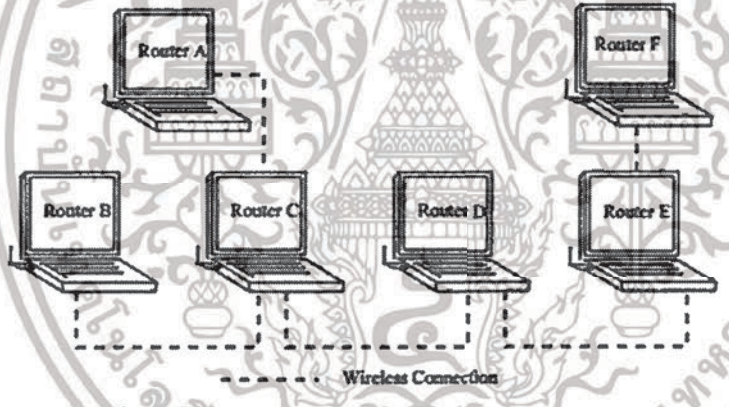
2.1.2 Optimized Link State Routing Protocol (OLSR)

Optimized Link State Routing Protocol(OLSR) [5] คือโปรโตคอลค้นหาเส้นทางแบบโพรแอกทีฟสำหรับเครือข่ายสื่อสารเฉพาะกิจซึ่งมีแนวคิดที่จะลดโอเวอร์เฮด โดยการลดจำนวนของการบรอดแคสต์ ซึ่งแนวคิดพื้นฐานที่สนับสนุนความคิดนี้คือการเลือกโหนดเอ็มพีอาร์ (MPR: Multipoint Relays Selection) โดยโหนด MPR นั้นเป็นกลุ่มของโหนดข้างเคียง (Neighbor nodes) ที่มีหน้าที่ในการส่งต่อข้อมูล (Retransmission) ซึ่งทุกโหนดที่เป็นโหนดข้างเคียงไม่จำเป็นต้องเป็นโหนด MPR โดยโหนดที่ทำหน้าที่ในการเลือกโหนด MPR จะถูกเรียกว่าผู้คัดเลือกโหนด MPR (MPR Selectors) และกลุ่มของโหนด MPR ก็สามารถเปลี่ยนแปลงได้ตลอดตามความเหมาะสมด้วย โดยในการคัดเลือกโหนด MPR นั้นจะเลือกจากโหนดที่เป็นโหนดข้างเคียงในระยะ 1 hop (One Hop Neighbors) ที่สามารถเชื่อมต่อกับโหนดข้างเคียงในระยะ 2 hop (Two Hop Neighbors) ที่มากที่สุด ซึ่งโหนดข้างเคียงในระยะ 1 hop คือ โหนดที่ตนเองสามารถเชื่อมต่อได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

(โหนดที่อยู่ภายในช่วงคลื่นสัญญาณของตนเอง) แต่โหนดข้างเคียงในระยะ 2 hop คือ โหนดที่ตนเองไม่สามารถเชื่อมต่อได้แต่สามารถเชื่อมต่อโดยผ่านโหนดข้างเคียงในระยะ 1 hop ได้ ซึ่งในกลไกนี้โหนดข้างเคียงในระยะ 2 hop จะต้องมีการเชื่อมต่อแบบสองทิศทาง (Bi-Directional Link) กับโหนดข้างเคียงในระยะ 1 hop เพื่อยืนยันว่าทั้งคู่สามารถสื่อสารโต้ตอบกันได้มิใช่เพียงแต่โหนดข้างเคียงในระยะ 1 hop ส่งข้อมูลไปยังโหนดข้างเคียงในระยะ 2 hop ได้เท่านั้น ดังนั้น OLSR จึงเป็นโพรโทคอลที่เหมาะสำหรับเครือข่ายขนาดใหญ่และมีความหนาแน่นของโหนดสูงที่มี MPRs ทำหน้าที่เป็นตัวกลางในการค้นหาเส้นทาง แต่เส้นทางที่ถูกค้นพบโดยโพรโทคอล OLSR นั้นอาจไม่ใช่เส้นทางที่สั้นที่สุด ซึ่งนี่คือข้อเสียที่อาจเกิดขึ้นจาก OLSR

โพรโทคอล OLSR แบ่งการทำงานออกเป็น 3 ส่วน ประกอบด้วย packet forwarding neighbor sensing และ topology discovery โดยที่ packet forwarding เป็นกลไกที่ทำการส่ง HELLO message เพื่อให้แต่ละโหนดทราบข้อมูลเกี่ยวกับโหนดข้างเคียง สำหรับ neighbor sensing นั้นเป็นกลไกที่ช่วยให้โหนดกระจายข้อมูลของตัวเองให้กับโหนดข้างเคียง และ topology discovery เป็นกลไกที่กำหนดโครงสร้างของเครือข่ายทั้งหมดรวมทั้งคำนวณหาตารางเส้นทางด้วย



รูปที่ 2.3 ตัวอย่างของโพรโทคอลค้นหาเส้นทาง OLSR

2.1.3 Multiple Source Routing Protocol (MSR)

Multiple Source Routing Protocol พัฒนาขึ้นโดยใช้หลักการของ Dynamic Source Routing Protocol และนำหลักการของการส่งแบบหลายเส้นทางมาประยุกต์ใช้ได้ง่าย เนื่องจากในการทำงานปกติของโปรโตคอล DSR เป็นแบบ Source Routing ซึ่งมีกลไกในการหาเส้นทางก่อนส่งข้อมูลและมีการเก็บข้อมูลเส้นทางที่หามาได้ไว้กับโมบายล์โหนดที่ทำการส่งข้อมูล ทำให้การประมวลผลการส่งแบบหลายเส้นทางมีความเป็นไปได้ที่จะนำมาใช้กับโปรโทคอล DSR ซึ่งโปรโตคอล MSR ใช้กลไก Route Discovery แบบเดียวกับ DSR ซึ่งจะนำข้อมูลเส้นทางหลายเส้นจาก Route Reply ที่ตอบกลับมาเก็บไว้ใน Route Cache ทำให้โปรโตคอลสามารถเลือกเส้นทางในการส่งข้อมูลจาก Route Cache ได้หลายเส้นทางโดยจะเลือกใช้เส้นทางที่ไม่ซ้ำกันมาใช้ก่อน จะทำให้สามารถใช้ทรัพยากรที่มีอยู่ได้อย่างมีประสิทธิภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในส่วนของกลไกการส่งแพ็คเก็ตในโปรโตคอล MSR นั้นจะมีรูปแบบเหมือนกับของโพรโทคอล DSR แต่จะมีกลไกการกระจายโหลดข้อมูลเพิ่มเข้ามา โดยจะมีการจัดสรรการส่งแพ็คเก็ตออกไปแบบ Round Robin วนตั้งแต่เส้นทางแรกที่พบภายใน Route Cache ไปจนถึงเส้นทางสุดท้าย ทำให้โพรโทคอล MSR สามารถส่งแพ็คเก็ตออกไปยังเส้นทางต่างๆ หลายเส้นทางได้

2.1.4 Split Multipath Routing Protocol (SMR)

Split Multipath Routing Protocol เป็นโปรโตคอลที่พัฒนาขึ้นมาโดยมีพื้นฐานของ Dynamic Source Routing Protocol โดยทำการปรับปรุงแก้ไขบางส่วนของกลไกต่างๆ ให้มีความสามารถในการส่งแบบหลายเส้นทาง กลไกที่ถูกทำการปรับปรุงแก้ไขได้แก่กลไกดังต่อไปนี้

อย่างแรกคือหลักการทำงานของกลไก Route Discovery ในโปรโตคอล SMR ระบบการทำงานจะคล้ายกับในโปรโตคอล DSR แต่ในโปรโตคอลนี้จะมีการกำหนดเงื่อนไขเพิ่มเติมดังนี้

1) โมบายล์โหนดที่ได้รับ Route Request (RREQ) จะไม่ทำการส่งแคชเส้นทาง (Route Cache) ที่ตนเองเก็บไว้กลับไปยังโหนดต้นทาง มีเพียงโมบายล์โหนดที่เป็นปลายทางเท่านั้น ที่จะสามารถส่ง Route Reply กลับไปยังโหนดต้นทางได้ เพื่อให้โพรโทคอลสามารถสร้างเส้นทางได้หลายเส้นทาง
2) เมื่อโมบายล์โหนดได้รับ RREQ ที่มี identification เดิมซึ่งเคยได้รับมาแล้วจะมีการตรวจสอบดังนี้
   - ตรวจสอบเส้นทางที่ได้รับ RREQ มา หากเป็น RREQ ที่ได้รับจากโมบายล์โหนดที่เคยได้รับมาแล้วจะทำการดรอปแพ็คเก็ต RREQ นั้นทิ้งไป
   - ถ้า RREQ ที่ได้รับมาจากโมบายล์โหนดที่ไม่เคยได้รับมาก่อน จะตรวจสอบจำนวนฮอป (Hop Count) เทียบกับ RREQ แรกที่ได้รับ ถ้ามีจำนวนฮอปมากกว่า RREQ แรกก็จะดรอปแพ็คเก็ต RREQ นั้นทิ้งเช่นกัน แต่หากมีจำนวนฮอปไม่เกิน RREQ แรกก็จะทำการเพิ่มแอดเดรสของตนเองลงในแพ็คเก็ต RREQ และบรอดแคสท์ RREQ นั้นต่อไป

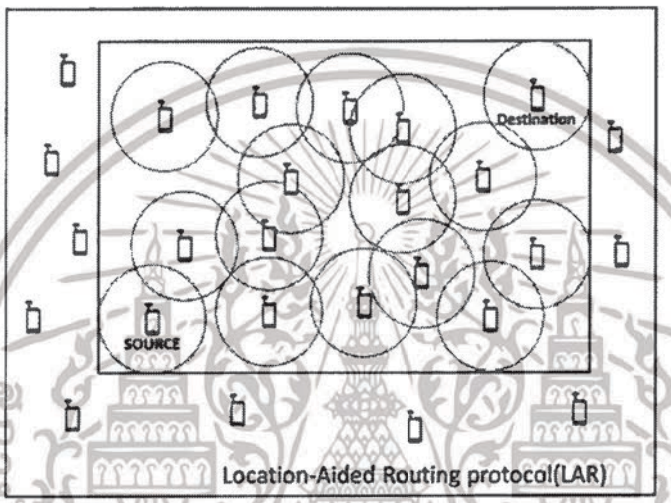
เงื่อนไขข้างต้นเป็นการเพิ่มโอกาสการสร้างเส้นทางหลายเส้นทางให้มากขึ้น และเส้นทางที่จะเกิดขึ้นจะเป็นเส้นทางที่มีการซ้อนทับกันน้อยกว่าการตรวจสอบเพียงแค่ Identification ของ RREQ

เมื่อโหนดปลายทางได้รับ RREQ แรก จะทำการส่ง Route Reply (RREP) กลับไปยังต้นทางทันทีและรอรับ RREQ ถัดไปที่ถูกส่งมาจากโมบายล์โหนดอื่นๆ เพื่อทำการหาเส้นทางอื่นๆ ที่จะใช้ในการส่งแบบหลายเส้นทางและทำการเลือกส่ง RREP กลับไปอีกหนึ่งแพ็คเก็ตโดยจะเลือกส่งไปในเส้นทางที่มีการใช้โหนดซ้ำกับเส้นทางแรกน้อยที่สุด หากมีเส้นทางที่ตรงกับเงื่อนไขดังกล่าวมากกว่า 1 เส้นทางจะทำการเลือกเส้นทางที่มีจำนวนฮอปน้อยที่สุดจากเส้นทางเหล่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนที่สองคือกลไก Route Maintenance จะถูกเรียกใช้งานเมื่อเส้นทางที่ใช้ส่งแพ็คเก็ตอยู่ถูกตัดขาด ทำให้ไม่สามารถทำการส่งแพ็คเก็ตได้ โมบายล์โหนดที่ส่งแพ็คเก็ตอยู่จะทำการส่ง Route Error Packet (RERR) กลับไปยังโมบายล์โหนดต้นทาง และต้นทางจะทำการลบข้อมูลเส้นทางทั้งหมดที่มีการใช้หรือส่งผ่านเส้นทางที่ขาดไป หลังจากนั้นจะเริ่มต้นกระบวนการ Route Discovery ใหม่

2.1.5 Location-Aided Routing Protocol (LAR)



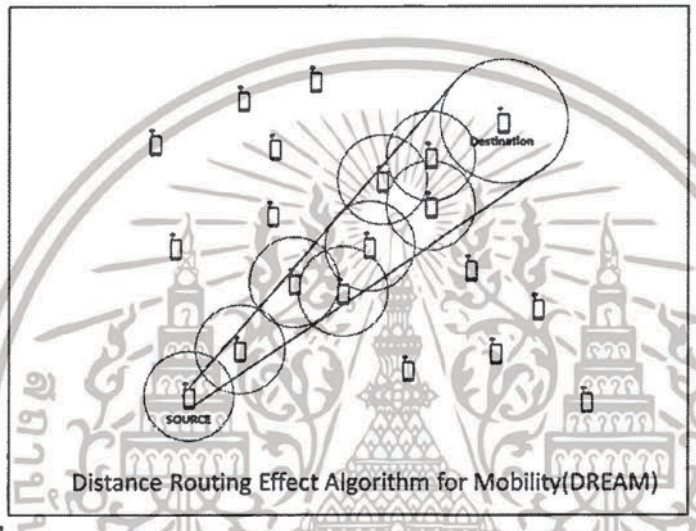
รูปที่ 2.4 Location-Aided routing protocol scheme

Location-Aided Routing protocol หรือ LAR [6] เป็นโปรโตคอลที่มีการพัฒนาต่อยอดมาจาก DSR โดยการใช้ระบบพิกัด GPS [7] เข้ามาช่วยในการคาดเดาตำแหน่งของปลายทาง ทำให้สามารถสร้างเงื่อนไขในการจำกัดการกระจายของข้อมูลได้ ในกระบวนการทำงานของโปรโตคอล LAR จำเป็นต้องรู้พิกัด GPS ของโหนดปลายทาง และความเร็วเฉลี่ยของโหนดปลายทางซึ่งได้มาจาก การทำ Route Discovery ครั้งแรกโดยใช้วิธีการแบบเดียวกับโปรโตคอล DSR โดย โหนดปลายทางจะเพิ่มข้อมูลความเร็วและพิกัด GPS ลงไปบนเฮดเดอร์ของ Route reply ก่อนที่จะส่งกลับมาที่โหนดต้นทางเพื่อที่จะใช้คำนวณความเป็นไปได้ที่โหนดปลายทางจะเคลื่อนที่จากจุดเดิมเป็นระยะเท่าไหร่ หรือเรียกว่า expected zone จากนั้นจึงสร้างเงื่อนไขในการกระจายของข้อมูลให้อยู่ในพื้นที่ที่กำหนด ซึ่งจะถูกเรียกว่า forwarding zone จากรูปที่ 2.4 จะสังเกตได้ว่า expected zone คือพื้นที่วงกลมที่ล้อมรอบโหนดปลายทาง และ forwarding zone คือกรอบสี่เหลี่ยมที่มีโหนดต้นทางอยู่ที่ปลายของเส้นทแยงมุมที่ทำกับโหนดปลายทาง จากนั้นโปรโตคอล LAR จะเริ่มขั้นตอนการทำ Route Discovery เช่นเดียวกับโปรโตคอล DSR เพื่อค้นหาเส้นทางในการติดต่อสื่อสารต่อไป โดยที่โปรโตคอล LAR ยังคงมีการใช้ Route Cache เช่นเดียวกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.6 Distance Routing Effect algorithm for mobility (DREAM)

Distance Routing Effect algorithm for mobility (DREAM) [8] เป็นโปรโตคอลที่ทำงานอยู่บนพื้นฐานของการบรอดแคสข้อมูล โดยทุกๆโหนดจะมีการบรอดแคสข้อมูลพิกัด GPS และความเร็วของตัวเองอยู่ตลอดเวลา ในกรณีที่โหนดต้นทางต้องการส่งข้อมูลไปยังโหนดปลายทาง โหนดต้นทางจะตรวจสอบว่า ตนเองรู้จักพิกัด GPS และความเร็วของโหนดปลายทางหรือไม่ ในกรณีที่รู้จัก โหนดต้นทางจะสร้าง forwarding zone เป็นรูปกรวยดังรูปที่ 2.5



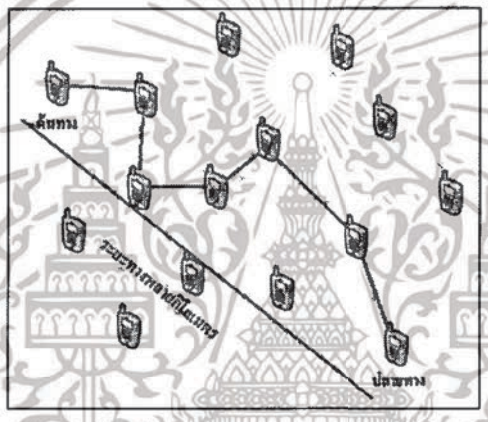
รูปที่ 2.5 Distance Routing Effect algorithm for mobility scheme

โดยที่โหนดในพื้นที่ดังกล่าวจะทำหน้าที่เป็นตัวกลางในการส่งข้อมูลไปยังปลายทางโดยวิธีการบรอดแคส ซึ่งจะแตกต่างจากโปรโตคอล DSR และ LAR ที่จะสร้างเส้นทางขึ้นมาก่อนแล้วส่งข้อมูลแบบยูนิแคส ในกรณีที่โหนดต้นทางไม่ทราบถึงพิกัด GPS และ ความเร็วของโหนดปลายทาง โหนดต้นทางจะบรอดแคสข้อมูลออกไปทั่วเครือข่ายจนกว่าโหนดปลายทางจะได้รับข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 เทคโนโลยีเครือข่ายไร้สายเฉพาะกิจที่ถูกพัฒนาขึ้นโดยมีพื้นฐานมาจากโปรโตคอล Delay-Tolerant Network

ดีทีเอ็น เป็นเทคโนโลยีสำคัญที่ทำให้เกิดการติดต่อสื่อสารบนพื้นที่เฉพาะ(Regions) ซึ่งเทคโนโลยีเครือข่ายในปัจจุบันไม่สามารถนำไปใช้ในทางปฏิบัติได้ เนื่องจากการสื่อสารบนพื้นที่เฉพาะนั้น โหนดและช่องทางการเชื่อมต่อระหว่างโหนด(Link) อาจจะมีปัญหาในเรื่องความน่าเชื่อถือ เช่น มีโอกาสในการเชื่อมต่อกันได้ยาก หากเกิดการเชื่อมต่อก็จะเกิดขึ้นเพียงแค่ในช่วงระยะเวลาสั้นๆเท่านั้น อันเป็นสาเหตุให้เกิดความผิดพลาดของข้อมูล ข้อมูลบางส่วนขาดหายระหว่างส่ง หรือการขาดการเชื่อมต่อของเครือข่ายเป็นเวลานาน ซึ่งปัญหาเหล่านี้ก็จะส่งผลกระทบต่อความแปรปรวนของ Hop (ช่องทางการส่งข้อมูลระหว่าง router หนึ่งๆ) หรือช่องทางการส่งข้อมูลของ router [9]

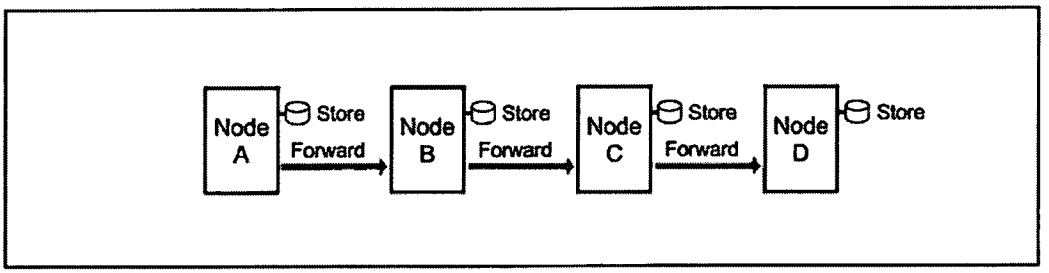


รูปที่ 2.6 แสดงตัวอย่างของ Delay-Tolerant Networks[9]

โดยทั่วไป ศักยภาพหลักของดีทีเอ็น คือการสร้างการเชื่อมต่อระหว่างอุปกรณ์ Mobile Device ในสถานการณ์ที่ Network ไม่สามารถสร้าง End to End Connection ได้ เพื่อให้เกิดการติดต่อสื่อสาร ซึ่งจะเป็นการทำให้ Network มีความกว้างขึ้น จากเทคโนโลยี Wire และ Wireless

กระบวณการทำงานของดีทีเอ็นนั้น จะมีลักษณะการทำงานโดย ทำการเชื่อมโยงโปรโตคอลของเครือข่าย ที่ยอมให้สามารถเกิดการติดต่อกันระหว่างอุปกรณ์สัญญาณได้ แม้ว่า Network จะไม่ได้มีการเชื่อมต่ออยู่ตลอดเวลาก็ตาม ซึ่งโหนดระหว่าง Sort และ Destinatoin Node อาจจะต้องทำหน้าที่ในการช่วยรับข้อมูลแล้วส่งต่อ ทำให้การส่งสามารถส่งถึงปลายทางได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.7 แสดงตัวอย่างกระบวณการทำงานของดีทีเอ็น [9]

2.2.1 Anti-Entropy และ n-Epidemic Routing

ความท้าทายของเทคโนโลยีเครือข่ายดีทีเอ็นคือ การสร้างกลยุทธ์การส่งข้อความ บนเครือข่ายที่ไม่สามารถทราบได้ถึงการเชื่อมต่อระหว่างโหนดใดๆ เพื่อสร้างเส้นทางการสื่อสารจากต้นทางไปยังปลายทางได้เลย ซึ่ง Jones E., Li L., Schmidtke J. และ Ward P. ได้เสนอกลยุทธ์การส่งข้อความเพื่อแก้ไขจุดบกพร่องดังกล่าว โดยใช้ข้อมูลจากเครือข่ายประมาณเวลาที่ข้อความบนโหนดจะถูกส่งต่ออีกครั้ง [10] นอกจากนั้น Jones E. และ Ward P. ได้ศึกษารวบรวมกลยุทธ์ในการส่งข้อความหลากหลายรูปแบบ ที่ได้ถูกสร้างขึ้นมาเพื่อแก้ไขโจทย์หัวข้อต่างๆ ซึ่งเป็นอุปสรรคต่อการสื่อสารบนเครือข่ายดีทีเอ็น [11] เช่น Tree-Based Flooding, Epidemic Routing, Link Metrics เป็นต้น

ในสถานการณ์การสื่อสารปกติของเครือข่ายดีทีเอ็น นิยมใช้กลยุทธ์การส่งข้อความแบบฟลัด ที่อาศัยการคัดลอกข้อความส่งไปยังโหนดเพื่อนบ้านโดยรอบ เพื่อเพิ่มประสิทธิภาพในการแพร่กระจายข้อความ ซึ่งหมายถึงโอกาสที่ข้อความจะถูกส่งต่อไปยังโหนดปลายทางมีโอกาสมากขึ้น เมื่อเปรียบเทียบกับกลยุทธ์รูปแบบอื่น แต่ทั้งนี้กลยุทธ์ดังกล่าวก็เป็นต้นเหตุให้เกิดความคับคั่งของปริมาณข้อความบนเส้นทางการสื่อสาร นอกจากนี้การส่งข้อมูลแบบบรอดแคสต์ของอุปกรณ์ไร้สาย ยังทำให้พลังงานในแหล่งพลังงานสำรองสูญเสียไปกับการเคลื่อนที่ของโหนด และการส่งข้อความจำนวนมากเกินความจำเป็น

Epidemic Routing มีวิธีการส่งข้อความชนิดหนึ่งเรียกว่า Anti-Entropy ซึ่งมีจุดประสงค์เพื่อลดความคับคั่งของปริมาณข้อความบนเส้นทางการสื่อสาร โดย Alan D. และคณะ ได้เสนอแนวคิดให้โหนดมีการแลกเปลี่ยนรายชื่อของข้อความ เพื่อตรวจสอบสถานะ ก่อนการส่งข้อความจริง [9] หลังจากนั้น Anti-Entropy ก็มีการพัฒนาอย่างต่อเนื่อง จนกระทั่ง Vahdat A., Becker D. และ คณะ ได้พัฒนากระบวนการดังกล่าว ให้เหมาะสมกับการใช้งานมากขึ้น โดยให้โหนดร้องขอเฉพาะข้อความที่ตนเองต้องการได้ [12]

แต่อย่างไรก็ตามการลดปริมาณการสูญเสียพลังงานของโหนด ก็เป็นอีกหนทางหนึ่งในการแก้ไขปัญหา จากการศึกษา n-Epidemic Routing ของ Lu X. และ Pan H. ซึ่งมีแนวคิดที่จะลดจำนวนครั้งการส่งข้อความ โดยการกำหนดให้มีการส่งข้อมูลแบบบรอดแคสต์ เมื่อมีโหนดเพื่อนบ้านครบตามจำนวนที่กำหนด เงื่อนไขดังกล่าวส่งผลให้การสูญเสียพลังงานจากการส่งข้อมูลลดลง อีกทั้งยังทำให้การส่งแต่ละครั้งมีโหนดที่ได้รับข้อความเพิ่มมากขึ้น[13] นอกจากนี้ De R. และ Amelio S. ยังได้พัฒนาต่อยอดให้ n-Epidemic Routing มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กลไกในการเลือกส่งต่อข้อความ (Dynamic Forwarding) โดยพิจารณาจากความหนาแน่นของโหนดในแต่ละกลุ่มเป็นสำคัญ[14]

และเพื่อเป็นการพิสูจน์ว่า ประสิทธิภาพการกระจายข้อความของกลยุทธ์การส่งข้อความที่นำเสนอไม่ได้ลดลงไปจากกลยุทธ์ต้นแบบ ในหัวข้อการวิเคราะห์และประเมินผล จึงได้มีการนำสัดส่วนของจำนวนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา เมื่อเทียบกับจำนวนโหนดทั้งหมด ของแต่ละกลยุทธ์การส่งข้อความ มาแสดงผลเปรียบเทียบในรูปแบบของกราฟ ซึ่งการเปรียบเทียบลักษณะนี้ถูกใช้สำหรับการวิเคราะห์และประเมินผลในหลากหลายบทความ[12][13][14] โดยสัดส่วนโหนดที่ได้รับข้อความในช่วงเวลา t สามารถคำนวณได้จากสูตร

$$R(t) = \frac{m(t)}{Node}$$

โดย $R(t)$ = สัดส่วนโหนดที่ได้รับข้อความในช่วงเวลา t

$m(t)$ = จำนวนโหนดทั้งหมดที่ได้รับข้อความ ณ เวลา t

$Node$ = จำนวนโหนดทั้งหมด

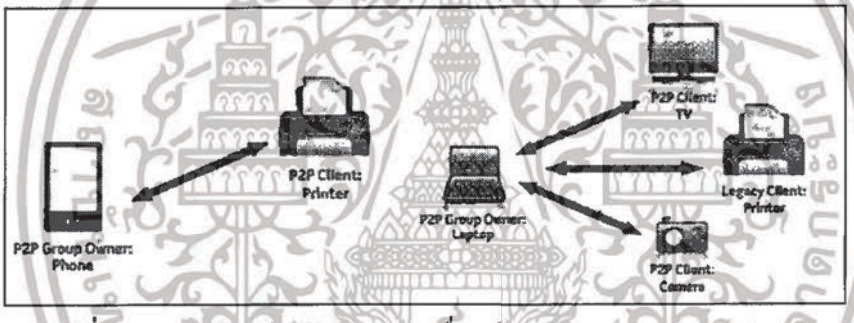
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3 งานวิจัยและเทคโนโลยีที่สามารถนำไปสู่การประยุกต์

2.3.1 เทคโนโลยีไวไฟไดเร็ค (Wi-Fi direct)

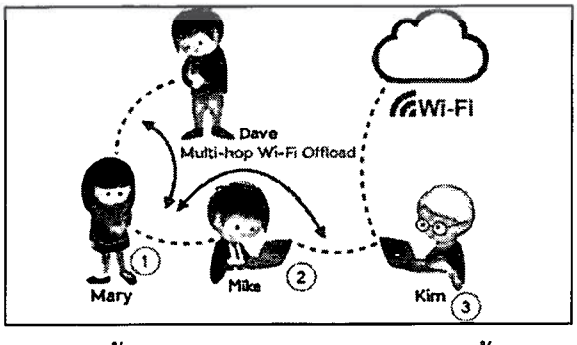
Wi-Fi Direct คือ เทคโนโลยีการสื่อสารตามมาตรฐาน Wi-Fi มีการเชื่อมต่อลักษณะ Peer-to-Peer โดยผู้ใช้สามารถเชื่อมต่อกับอุปกรณ์อื่นๆได้โดยตรง ไม่จำเป็นต้องติดต่อกับเครือข่ายโครงสร้างพื้นฐาน (Infrastructure network)

การทำงานของ Wi-Fi Direct เริ่มต้นโดยอุปกรณ์จะส่งสัญญาณไปยังอุปกรณ์ใกล้เคียงที่สามารถสร้างการเชื่อมต่อได้ใน 1 Hop กับอีกอุปกรณ์หนึ่งโดยตรง เมื่อผู้ใช้ร้องขอการเชื่อมต่อกับอุปกรณ์ใกล้เคียงจาก Wi-Fi Protected Setup โดยรักษาความปลอดภัยในการเชื่อมต่อด้วย industry-standard WPA2 security และอุปกรณ์ทั้งสองเชื่อต่อกัน การเชื่อมต่อจะอยู่ในรูปแบบของ Wi-Fi Direct Group ขณะนี้อุปกรณ์จะสามารถบริการได้ทุกอย่างที่อยู่บนมาตรฐานของ Wi-Fi Direct



รูปที่ 2.8 แสดงตัวอย่างลักษณะการเชื่อมต่อของ Wi-Fi Direct[15]

แต่ Wi-Fi Direct มีข้อจำกัดคือรองรับการเชื่อมต่อเพียง 1 Hop ซึ่งปกติแล้วเส้นทางการติดต่อสื่อสารระหว่างต้นทางกับปลายจะประกอบไปด้วยเส้นทางย่อยหลาย Hop เรียกว่า Multi-Hop จึงต้องอาศัยเทคนิคการหาเส้นทางแบบหลาย Hop (Multi-Hop Routing) หรือการส่งต่อในลักษณะ DTN บนเครือข่ายที่มีการเชื่อมต่อแต่ละ Hop ด้วยเทคโนโลยี Wi-Fi Direct[15][16]

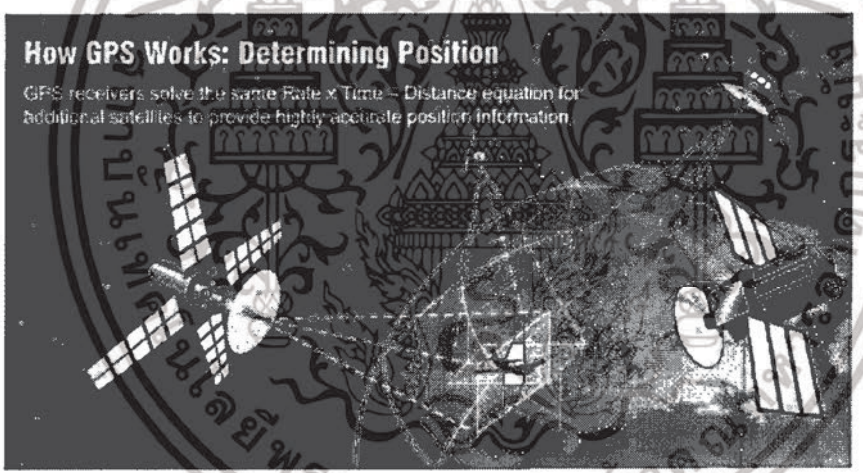


รูปที่ 2.9 แสดงตัวอย่างการหาเส้นทางแบบ Multi-Hop Routing ด้วย Wi-Fi Direct[15]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.2 เทคโนโลยีระบุตำแหน่งบนพื้นโลก

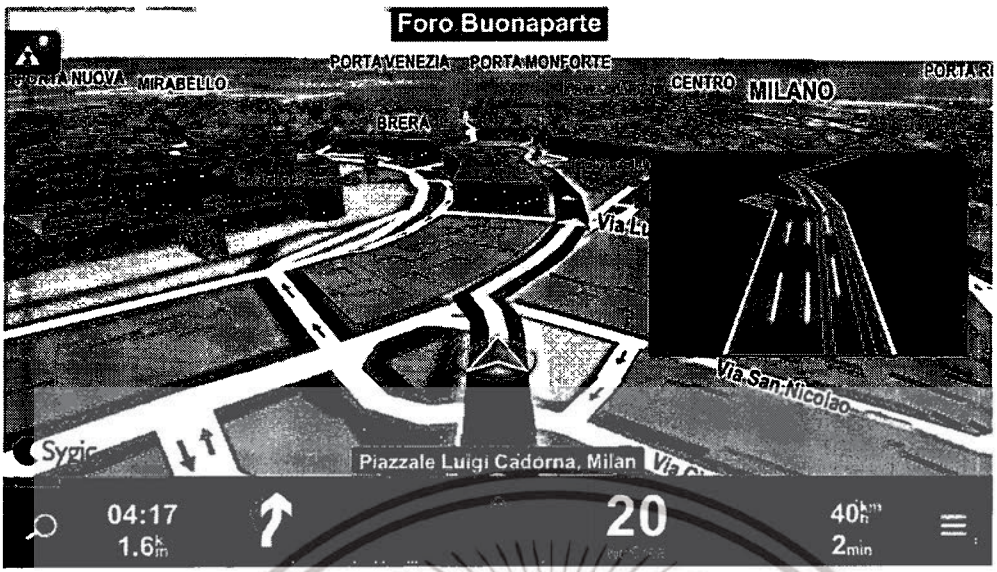
เทคโนโลยีสารสนเทศที่ถูกกล่าวถึงมากในปัจจุบันอีกประเภท นั่นก็คือเทคโนโลยีการระบุตำแหน่งบนพื้นโลกหรือจีพีเอส (Global Positioning System: GPS) โดยระบบดาวเทียมนำร่อง (Navigation Satellite) ถูกพัฒนาขึ้นเพื่อระบุพิกัดสำหรับอ้างอิงตำแหน่งบนพื้นโลก อย่างเช่น ระบบจีพีเอส [7] ซึ่งเป็นหนึ่งในระบบนำร่องสำหรับการระบุตำแหน่งที่ถูกใช้กันอย่างแพร่หลาย โดยใช้ดาวเทียมเข้ามาช่วยในการคำนวณตำแหน่งต่างๆ ดังรูปที่ 2.9 ซึ่งในการระบุตำแหน่งต่างๆ นั้น ภายในอุปกรณ์ที่จะถูกระบุตำแหน่งจำเป็นต้องมีอุปกรณ์รับสัญญาณจากดาวเทียมติดตั้งอยู่ จากนั้นในการคำนวณตำแหน่งของอุปกรณ์รับสัญญาณจะประมวลผลจากการรับสัญญาณดาวเทียมมากกว่าสามตัวขึ้นไป เพื่อหาพื้นที่คาบเกี่ยวระหว่างดาวเทียมทั้งหมดโดยใช้ Triangulation Method ซึ่งจะทำให้ทราบว่า อุปกรณ์รับสัญญาณนั้นอยู่ในพิกัดละติจูดและลองจิจูดที่เท่าไร นอกจากระบบจีพีเอสแล้วยังมีอีกหลายระบบอาทิเช่น โกลนาสของรัสเซีย กาลิเลโอของยุโรป คอมพาสของจีน เป็นต้น แต่ระบบเหล่านี้ส่วนใหญ่ยังไม่ถูกรองรับในอุปกรณ์สมาร์ทโฟนในไทย



รูปที่ 2.10 Triangulation method

(เครดิตรูปภาพ http://avionicswest.com/Images/Triangulate.png)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.11 หน้าจออุปกรณ์นำทางด้วยระบบ GPS

(เครดิตรูปภาพ https://play.google.com/store/apps/details?id=com.sygic.aura)

ระบบจีพีเอสถูกนำมาประยุกต์ใช้งานหลากหลาย [17]–[19] เช่น ระบบนำทาง (Navigation System) ดังรูปที่ 2.11 หรือระบบติดตามยานพาหนะ (Vehicle Tracking) หรือระบบสนับสนุนการวางแผนการเดินทาง ซึ่งนอกจากใช้ในการเดินทางส่วนบุคคลแล้วยังใช้กำหนดเส้นทางส่งของในระบบลอจิสติกได้อีกด้วย ฯลฯ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

บทที่ 3

งานวิจัยที่ได้ดำเนินการ

ห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์คแบ่งงานที่ถูกพัฒนาขึ้นมาเป็นสองส่วน ในหัวข้อที่ 3.1-3.6 เป็นส่วนของการพัฒนางานวิจัยเชิงทฤษฎีซึ่งหัวข้อที่ 3.5 และ 3.6 มีการทำวิจัยร่วมกับต่างประเทศ ในส่วนของหัวข้อที่ 3.7 เป็นต้นไปเป็นงานวิจัยเชิงแอพพลิเคชั่น โดยมีผลงานทั้งหมดดังต่อไปนี้

3.1 การปรับปรุงการแบ่งโหลดเพื่อกระจายข้อมูลหลายทางบนเครือข่ายเฉพาะกิจเคลื่อนที่

ความล้มเหลวของการสื่อสารบนเครือข่ายเฉพาะกิจ มักมีสาเหตุมาจากเส้นทางที่ใช้งานอยู่ถูกตัดขาดอันเนื่องมาจากการสูญหายของโมบายล์โหนด เช่น การเคลื่อนที่ของโมบายล์โหนด พลังงานที่จำกัดของโมบายล์โหนด เป็นต้น งานวิจัยนี้จึงพัฒนารูปแบบวิธีการส่งข้อมูลโดยใช้การส่งข้อมูลหลายเส้นทาง และวิธีการเลือกเส้นทางของโปรโตคอลซึ่งส่งผลให้สามารถใช้งานเส้นทางที่ถูกเลือกได้อย่างมีประสิทธิภาพ จากผลการจำลองการส่งข้อมูลระหว่างโมบายล์โหนด แสดงให้เห็นถึงการเพิ่มขึ้นของอัตราสำเร็จในการส่งข้อมูล และเวลาที่ใช้ในการทำงานลดลง

งานวิจัยฉบับนี้[20] ได้รับการตอบรับจากการประชุมทางวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศครั้งที่10 (National Conference on Computing and Information Technology 2014)

3.1.1 ปัญหาที่ต้องการแก้ไข

ปัญหาของการสร้างเครือข่าย MANET ด้วยเทคโนโลยี Wi-Fi ก็คือ โมบายล์โหนดในเครือข่าย MANET มีโอกาสสูงที่จะขาดการเชื่อมต่อจากกัน เพราะเทคโนโลยี Wi-Fi ไม่เหมาะสมกับการใช้งานกับเครือข่ายที่โมบายล์โหนดมีการเคลื่อนที่ เนื่องจากเทคโนโลยีดังกล่าวมีระยะการเชื่อมต่อค่อนข้างสั้น ทำให้มีโอกาสที่โมบายล์โหนดจะเคลื่อนที่ออกนอกจากระยะการเชื่อมต่อ ส่งผลให้มีโอกาสเกิดการขาดการเชื่อมต่อระหว่างโมบายล์โหนดต้นทางและปลายทาง ซึ่งนำไปสู่ปัญหาความยั่งยืนทนทานของเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

138020

3.1.2 ไอเดียที่ถูกนำเสนอ

ผู้วิจัยจึงทำการนำเสนอแนวคิดการพัฒนาโปรโตคอล MSR ที่มีอยู่เดิมโดยจะปรับปรุงรูปแบบการส่งแพ็คเก็ตเดิมที่ใช้แบบ Round Robin ผู้วิจัยนำเสนอรูปแบบการส่งแพ็คเก็ตแบบ Weight-Round Robin (WRR) แทนการใช้รูปแบบการส่งแบบเดิม เนื่องจากในการส่งแพ็คเก็ตแบบ Round Robin นั้นมีการกระจายโหลดของเส้นทางเท่าๆ กัน จึงมีโอกาสที่เส้นทางที่มีดีเลย์สูงจะถูกเรียกใช้งานเท่ากับเส้นทางที่มีดีเลย์ต่ำ ซึ่งค่าดีเลย์วัดได้จากกการจับเวลาตั้งแต่ส่งแพ็คเก็ต Route Request ออกไปและได้รับ Route Reply กลับมาผ่านเส้นทางนั้นๆ

3.1.3 ผลการทดลอง

จากผลการทดลองสามารถบอกได้ว่าอัลกอริทึมที่นักวิจัยนำเสนอนั้น สามารถทำงานได้ดีกว่าอัลกอริทึม DSR และ MSR ในสถานการณ์ที่มีจำนวนโมบายล์โหนดสูง หรือมีการเคลื่อนที่ด้วยความเร็วมาก เป็นผลมาจากการเพิ่มอัลกอริทึมค้นหาเส้นทางให้มีการกำหนดน้ำหนักให้กับเส้นทาง ทำให้ไม่เกิดความคับคั่งในเส้นทางใดเส้นทางหนึ่ง และสามารถดึงประสิทธิภาพของโมบายล์โหนดออกมาใช้งานได้อย่างเต็มที่

3.2 การศึกษาความเป็นไปได้ในการลดโอเวอร์เฮดบนระบบเครือข่ายไร้สายเฉพาะกิจโดยการสร้างเงื่อนไขในการจำกัดการกระจายข้อมูลในขั้นตอนการค้นหาเส้นทาง

การทำงานของโปรโตคอล DSR นั้น ในขั้นตอนการค้นหาเส้นทางจะมีการสร้างแพ็คเกตที่ไม่มีประโยชน์ต่อการสื่อสารระหว่างโหนดบนระบบเน็ตเวิร์คหรือที่เรียกว่าโอเวอร์เฮดออกมาเป็นจำนวนมาก ในบทความฉบับนี้ได้นำเสนอวิธีการจำกัดการกระจายของข้อมูลในระบบเน็ตเวิร์คเฉพาะกิจเพื่อลดจำนวนโอเวอร์เฮดในระบบ จากการศึกษาพบว่าแนวคิดที่นำเสนอขึ้นใหม่นั้น สามารถลดจำนวนโอเวอร์เฮดลง ในขณะที่ยังคงรักษาอัตราความสำเร็จในการสร้างช่องทางการติดต่อสื่อสารกันระหว่างโหนดได้

งานวิจัยฉบับนี้[21] ได้รับการตอบรับจากการประชุมวิชาการระดับชาติด้านเทคโนโลยีสารสนเทศครั้งที่6 (National Conference on Information Technology 2014)

3.2.1 ปัญหาที่ต้องการแก้ไข

ในงานวิจัยชิ้นนี้ให้ความสนใจไปที่การลดโอเวอร์เฮดหรือข้อมูลที่ไม่มีประโยชน์ต่อการสื่อสารบนระบบเครือข่ายไร้สายเฉพาะกิจเนื่องจากข้อมูลเหล่านี้จะส่งผลให้เกิดความคับคั่งในระบบเครือข่ายถ้ามีมากจนเกินไป โดยงานวิจัยนี้ทำงานอยู่บนพื้นฐานของโปรโตคอล DSR ซึ่งแก้ไขปัญหาโดยการจำกัดพื้นที่เมื่อ

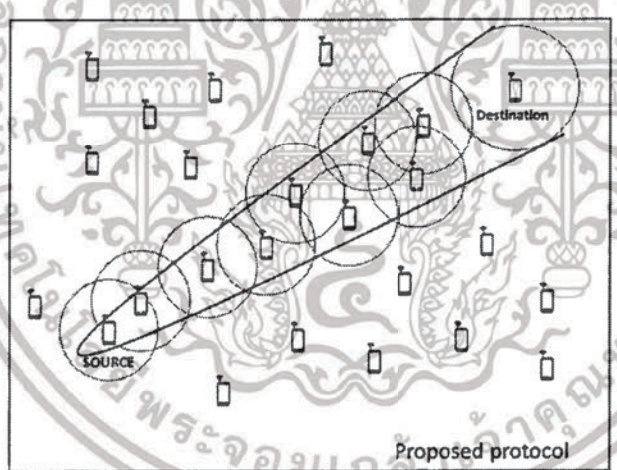
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เกิดการบรอดแคสต์แพ็คเกทในขั้นตอนการทำ Route discovery เพื่อค้นหาและสร้างเส้นทางระหว่างโหนด

3.2.2 ไอเดียที่ถูกนำเสนอ

จากการศึกษาลักษณะการทำงานบนโปรโตคอล DSR และ LAR แล้ว ผู้วิจัยเล็งเห็นถึงประโยชน์ของการจำกัดการกระจายข้อมูลในขั้นตอน Route discovery ว่าสามารถช่วยลดปัญหาการเกิดโอเวอร์เฮดได้ แต่เนื่องจากเงื่อนไขการจำกัดการกระจายข้อมูลยังไม่รัดกุมมากพอ จึงทำให้มีแนวคิดในการเพิ่มประสิทธิภาพในการทำงานของโปรโตคอลให้สามารถช่วยลดโอเวอร์เฮดได้มากยิ่งขึ้น

การนำพิกัด GPS เข้ามาช่วยในการติดต่อสื่อสารในระบบเครือข่ายเฉพาะกิจ ทำให้โหนดต้นทางสามารถกำหนดทิศทางการกระจายข้อมูลไปยังโหนดปลายทางในขั้นตอน Route discovery ได้ ดังนั้น ผู้วิจัยจึงได้มีแนวคิดในการปรับเปลี่ยนเงื่อนไขในขั้นตอน Route discovery รูปภาพที่ 3.1 แสดงถึงรูปแบบการจำกัดพื้นที่ของโปรโตคอลใหม่



รูปที่ 3.1 Proposed protocol scheme

ขั้นตอนการทำงานของโปรโตคอลใหม่นั้นโหนดต้นทางจะต้องทราบถึงพิกัด GPS และความเร็วเฉลี่ยของโหนดปลายทางก่อน โดยจะนำข้อมูลดังกล่าวบรรจุลงไปใน RREQ message เพื่อใช้ในการกำหนดบทบาทให้กับโหนดทุกโหนดในระบบเน็ตเวิร์ค ซึ่งในขั้นแรกจะต้องคำนวณพื้นที่ที่โหนดปลายทางมีโอกาสที่จะเคลื่อนที่ไป (expected zone) ก่อน หลังจากคำนวณ expected zone แล้ว จะนำรัศมีของ *expected zone* มาใช้ในการกำหนดบทบาทให้กับโหนดที่จะทำหน้าที่เป็นตัวกลางในการกระจายข้อมูล หรือเรียกว่า forwarding node

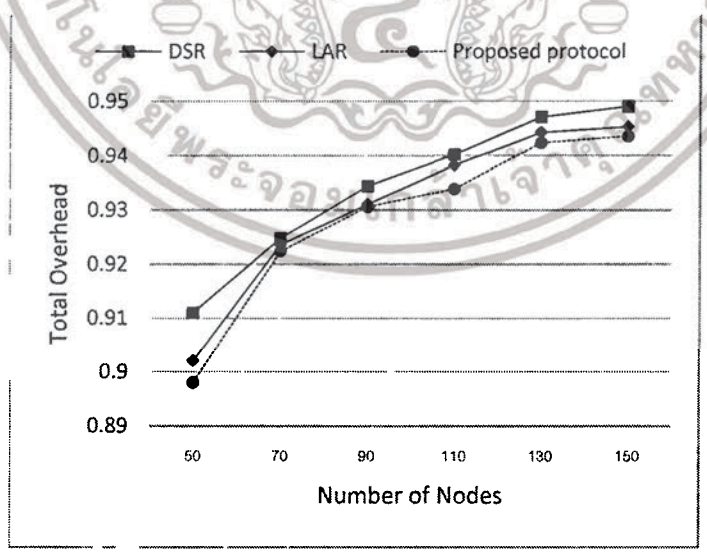
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากนั้นโหนดต้นทางจะเริ่มกระบวนการ Route discovery ซึ่งโหนดทุกตัวในระบบเครือข่ายจะทำการตรวจสอบว่าตัวเองนั้นเป็น Forwarding node หรือไม่ ถ้าใช้จะทำการกระจายข้อมูลต่อ แต่ถ้าไม่ใช้ก็จะทำการดร็อปแพ็คเกตทิ้งไป จนกว่าแพ็คเกตจะไปถึงโหนดปลายทาง จากนั้นโหนดปลายทางจะส่งแพ็คเกต *Route reply* ที่บันทึกข้อมูลของ *forwarding node* ทั้งหมดที่จำเป็นต้องใช้ในการติดต่อตามลำดับกลับมาที่โหนดต้นทางเพื่อสร้างช่องทางการติดต่อสื่อสารกันต่อไป

3.2.3 ผลการทดลอง

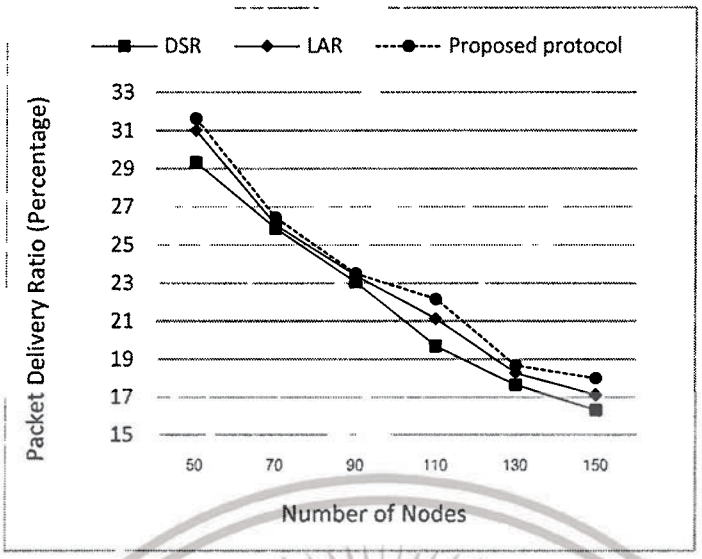
จากรูปที่ 3.2 จะเห็นได้ว่าโปรโตคอลที่นำเสนอสามารถลดจำนวนโอเวอร์เฮดได้เมื่อเปรียบเทียบกับโปรโตคอล DSR และ LAR เนื่องจากการเปลี่ยนเงื่อนไขในการกระจายข้อมูลให้มีความรัดกุมมากยิ่งขึ้น โดยค่าโอเวเวอร์เฮดนั้นเป็นสัดส่วนระหว่างจำนวนแพ็คเกตที่ใช้ในการค้นหาเส้นทางต่อจำนวนแพ็คเกตทั้งหมดที่เกิดขึ้นในระบบเครือข่าย

ในส่วนของวิธีการจำกัดพื้นที่ในการกระจายข้อมูลเพื่อลดโอเวอร์เฮดที่นำเสนอนั้นมีจุดประสงค์เพื่อลดจำนวน forwarding node ลง การกำหนดเงื่อนไขเพื่อควบคุมจำนวน forwarding node ให้เหมาะสมจะส่งผลกระทบต่ออัตราความสำเร็จในการส่งข้อมูล จากรูปที่ 3.3 แสดงให้เห็นว่าโปรโตคอลที่นำเสนอนั้นสามารถช่วยลดโอเวอร์ได้ ในขณะเดียวกันยังช่วยเพิ่มอัตราความสำเร็จในการส่งข้อมูลอีกด้วย ในกรณีของโปรโตคอล LAR และ DSR ที่มีอัตราความสำเร็จในการส่งข้อมูลน้อยกว่าเนื่องจากโอเวอร์เฮดที่เกิดจากขั้นตอน route discovery ส่งผลกระทบต่อระบบเครือข่ายทำให้เกิดความแออัดในระบบเน็ตเวิร์คจนกระทั่งเกิดการชนกันของข้อมูล ซึ่งเป็นการขัดขวางการส่งข้อมูลจากต้นทางไปยังปลายทาง



รูปที่ 3.2 กราฟแสงปริมาณโอเวอร์เฮดในระบบเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.3 กราฟแสดงอัตราความสำเร็จในการส่งข้อมูล

3.2.4 แนวทางการพัฒนาต่อยอด

งานวิจัยฉบับนี้ได้มีการพัฒนาต่อยอด และปรับปรุงผลลัพธ์ของการลดโอเวอร์เฮดให้ดีขึ้นในชื่อ Overhead Reduction Location-Aided Routing protocol ซึ่งผู้วิจัยกำลังเตรียมพร้อมที่จะส่งผลงานวิจัยไปยังงานประชุมวิชาการระดับนานาชาติ

3.3 การปรับปรุงกลไกการแพร่กระจายข้อความเพื่อลดการแลกเปลี่ยนข้อมูลบนเครือข่ายดีทีเอ็น

เครือข่ายสื่อสารเฉพาะกิจมีหน้าที่เก็บและส่งต่อข้อความจากโทรศัพท์มือถือเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ซึ่งในทางปฏิบัติ กระบวนการดังกล่าวทำให้เครือข่ายต้องรองรับข้อความจำนวนมาก ส่งผลให้เกิดความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสาร และการที่โทรศัพท์มือถือต้องสูญเสียพลังงานในการส่งข้อความทำให้จำนวนโทรศัพท์มือถือที่สามารถช่วยส่งต่อข้อความลดลงอย่างต่อเนื่อง เพราะฉะนั้นการพัฒนา n-Anti Entropy ซึ่งได้ดัดแปลงข้อดีของ Anti-Entropy และ n-Epidemic โดยผลการทดสอบในโมเดลจำลองแสดงให้เห็นว่า n-Anti Entropy มีแนวโน้มในการแก้ไขปัญหาข้างต้นได้ดีกว่ากลยุทธ์การส่งข้อความรูปแบบอื่นๆซึ่งสะท้อนให้เห็นถึงประสิทธิภาพของการสื่อสารในสถานการณ์จริงได้เป็นอย่างดี

งานวิจัยฉบับนี้[22] ได้รับการตอบรับจากการประชุมวิชาการระดับชาติด้านเทคโนโลยีสารสนเทศครั้งที่6 (National Conference on Information Technology 2014)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

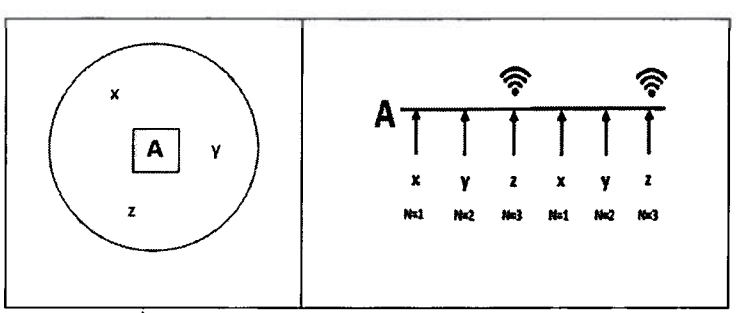
3.3.1 ปัญหาที่ต้องการแก้ไข

ความท้าทายของเทคโนโลยีเครือข่ายดีทีเอ็นคือ การสร้างกลยุทธ์การส่งข้อความ บนเครือข่ายที่ไม่สามารถทราบได้ถึงการเชื่อมต่อระหว่างโหนดใดๆ เพื่อสร้างเส้นทางการสื่อสารจากต้นทางไปยังปลายทางได้เลย ในสถานการณ์การสื่อสารปกติของเครือข่ายดีทีเอ็นนิยมใช้กลยุทธ์การส่งข้อความแบบฟลัด ที่อาศัยการคัดลอกข้อความส่งไปยังโหนดเพื่อนบ้านโดยรอบ เพื่อเพิ่มประสิทธิภาพในการแพร่กระจายข้อความ ซึ่งหมายถึงโอกาสที่ข้อความจะถูกส่งต่อไปยังโหนดปลายทางมีโอกาสมากขึ้น เมื่อเปรียบเทียบกับกลยุทธ์รูปแบบอื่น แต่ทั้งนี้กลยุทธ์ดังกล่าวก็เป็นต้นเหตุให้เกิดความคับคั่งของปริมาณข้อความบนเส้นทางการสื่อสาร นอกจากนี้การส่งข้อมูลแบบบรอดแคสต์ของอุปกรณ์ไร้สาย ยังทำให้พลังงานในแหล่งพลังงานสำรองสูญเสียไปกับการเคลื่อนที่ของโหนด และการส่งข้อความจำนวนมากเกินความจำเป็น

3.3.2 ไอเดียที่ถูกนำเสนอ

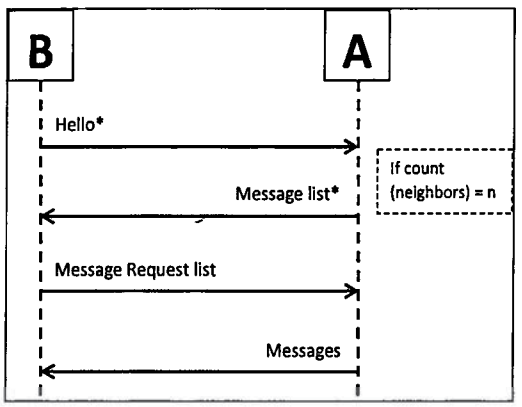
การทำงานในส่วนก่อนการส่งข้อความ นั้นจะใช้ประโยชน์จาก n-Epidemic ซึ่งจะเริ่มการส่งข้อมูลเมื่อโหนดมีจำนวนโหนดเพื่อนบ้านครบตามที่กำหนด ทำให้ไม่จำเป็นต้องส่งข้อมูลทุกครั้งที่พบโหนดอื่นๆ ในเครือข่าย โดยn-Epidemic อาศัยการส่งข้อมูลแบบบรอดแคสต์ ทำให้ในการส่งเพียงหนึ่งครั้ง โหนดเพื่อนบ้านจะได้รับข้อมูลทั้งหมด ส่งผลให้พลังงานที่โหนดสูญเสียไปกับการส่งข้อมูลแต่ละครั้งลดลง ตามรูปที่ 3.4

ในกระบวนการคัดเลือกและส่งต่อข้อความ ผู้วิจัยใช้ประโยชน์จากกระบวนการส่งข้อมูลด้วย Anti-Entropy ทำให้โหนดส่งเฉพาะข้อความที่โหนดเพื่อนบ้านต้องการเท่านั้น ปริมาณข้อมูลที่ต้องถูกส่งในแต่ละครั้งจึงลดลงอย่างมาก โดยหลักการทำงานที่ได้รับการพัฒนา เพื่อรองรับการทำงานต่อจากส่วนรอคอยการติดต่อจากโหนดเพื่อนบ้าน สามารถอธิบายการทำงานได้ตามรูปที่ 3.5 โดยแรกเริ่มโหนดแต่ละโหนดจะบรอดแคสต์ Hello แพ็คเก็ตออกไป เพื่อเป็นสัญญาณให้โหนดอื่นๆรู้ถึงการมีอยู่ของตน จากนั้นเมื่อโหนด A ได้รับสัญญาณจากโหนดต่างๆครบตามจำนวนที่กำหนด โหนด A จะบรอดแคสต์รายชื่อข้อความ (Message List) ที่มีออกไป และส่งข้อความ (Messages) ไปให้แต่ละโหนดตามที่ระบุไว้ในรายชื่อข้อความที่แต่ละโหนดต้องการ (Message Request List)



รูปที่ 1.4 กลยุทธ์การส่งข้อความแบบ n-Epidemic

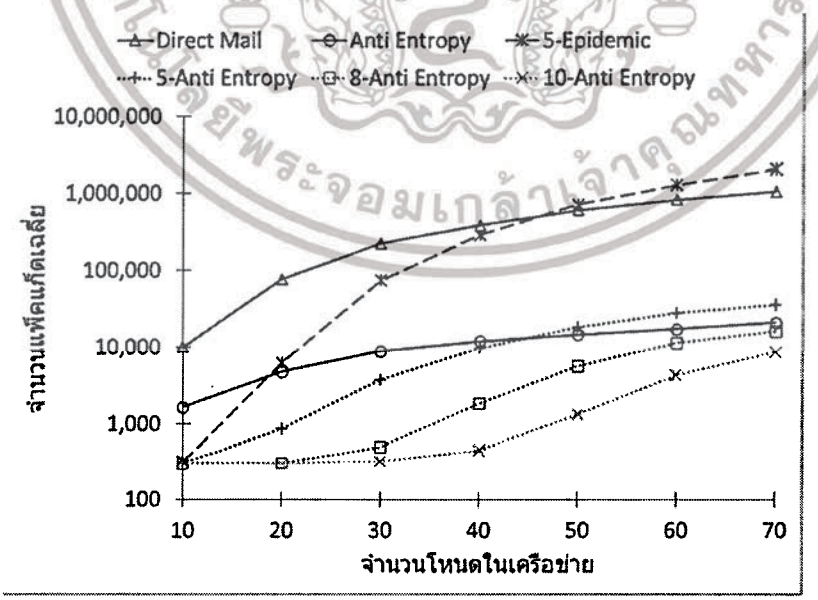
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.5 กลยุทธ์การส่งข้อความแบบ n-Anti Entropy

การที่ผลรวมของจำนวนข้อความที่ถูกส่งออกของโหนดทั้งหมดในเครือข่ายลดลง ย่อมหมายถึงการที่โหนดทั้งหมดมีจำนวนข้อมูลที่ส่งในแต่ละครั้ง หรือจำนวนครั้งการส่งข้อมูลลดลงตามไปด้วย เพราะฉะนั้นจากการที่ n-Anti Entropy ซึ่งได้นำส่วนที่ดีของ n-Epidemic และ Anti-Entropy มาทำงานร่วมกัน แสดงให้เห็นว่าการลดลงของจำนวนดังกล่าว ส่งผลให้ความคับคั่งของข้อมูลบนเส้นทางการสื่อสารได้รับการแก้ไขหรือบรรเทาลง ในขณะเดียวกันการสูญเสียพลังงานอันเนื่องมาจากการส่งข้อมูลของโหนดก็ลดลงเช่นกัน

3.3.3 ผลการทดลอง

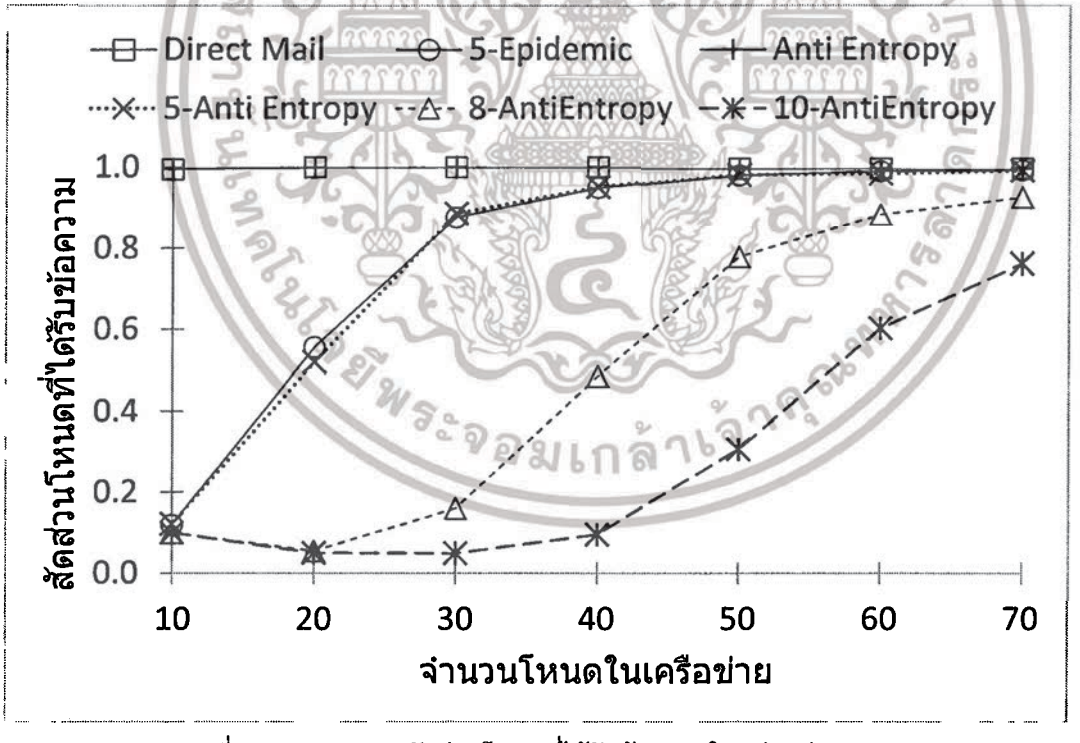


รูปที่ 3.6 กราฟแสดงผลรวมของจำนวนแพ็คแก็ตที่ถูกส่งออก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.6 เป็นกราฟซึ่งแสดงให้เห็นถึงแพ็คเกจทั้งหมดที่ถูกส่งออกจากระบบเน็ตเวิร์คที่ถูกจำลองขึ้นโดย Direct Mail มีระดับจำนวนแพ็คแก็ตสูงที่สุด เนื่องจากการที่โหนดส่งข้อความทั้งหมดที่ตนมี เมื่อมีการแลกเปลี่ยนข้อมูลเกิดขึ้น ซึ่งระดับดังกล่าวถูกทำให้ลดลงด้วย Anti-Entropy ที่อนุญาตให้โหนดส่งเฉพาะข้อความที่ถูกร้องขอเท่านั้น และเมื่อไม่นานมานี้ n-Epidemic ได้มีการเสนอแนวคิดที่น่าสนใจเพื่อลดจำนวนครั้งการส่งข้อความ ซึ่งจากกราฟแสดงให้เห็นว่า สามารถลดจำนวนแพ็คแก็ตได้ อย่างมากเมื่อมีการกำหนดจำนวนโหนดที่ต้องรอคอยให้เหมาะสมกับจำนวนโหนดในเครือข่าย

เนื่องจาก n-Anti Entropy เป็นกลยุทธ์การส่งข้อความที่ได้รวมเอาข้อดีของ Anti-Entropy และ n-Epidemic ทำให้จำนวนแพ็คแก็ตที่ถูกส่งออกไปในเครือข่ายน้อยกว่ากลยุทธ์อื่นๆที่เปรียบเทียบ และเมื่อมีการเพิ่มจำนวนโหนดเพื่อนบ้านของ n-Anti Entropy ก็ยิ่งทำให้ระดับของจำนวนแพ็คแก็ตลดลงมากยิ่งขึ้น แต่เมื่อพิจารณาจุดที่เครือข่ายมีโหนดมากกว่า 50 โหนด เส้นกราฟ 5-Anti Entropy จะมีจำนวนแพ็คแก็ตมากกว่า Anti-Entropy ซึ่งแสดงให้เห็นว่า การนำ n-Anti Entropy มาใช้ในการสื่อสารเพื่อลดจำนวนแพ็ตแก็ตที่ถูกส่งออกไปยังเครือข่าย จำเป็นต้องรักษาสมดุลระหว่างจำนวนโหนดที่รอคอยกับจำนวนโหนดในเครือข่ายให้สอดคล้องกันมากที่สุด



รูปที่ 3.7 กราฟแสดงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา

ในรูปที่ 3.7 กราฟแสดงให้เห็นถึงสัดส่วนของโหนดที่ได้รับข้อความครบ ต่อโหนดทั้งหมดในเครือข่ายในช่วงเวลาหนึ่งๆซึ่งจากการพิจารณากราฟแต่ละเส้นสามารถสรุปได้ว่า เมื่อหยุดการจำลองวินาทีที่ 300

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

วินาที โหนดทั้งหมดในเครือข่ายที่ใช้กลยุทธ์การส่งข้อความแบบDirect Mail และAnti-Entropy ได้รับข้อความครบทั้งหมด หรืออีกนัยหนึ่งหมายความว่าข้อความถูกส่งไปยังปลายทางครบทั้งหมดแล้ว แต่สำหรับn-Epidemic และn-Anti Entropy สัดส่วนของโหนดที่ได้รับข้อความจะเพิ่มขึ้นตามความหนาแน่นของโหนด อีกทั้งการเพิ่มจำนวนโหนดเพื่อนบ้านที่ต้องรอคอย ส่งผลให้ความชันของสัดส่วนโหนดที่ได้รับข้อความเมื่อเทียบกับความหนาแน่นของโหนดลดลง

3.4 การปรับปรุงกลไกค้นหาเกตเวย์เพื่อลดโอเวอร์เฮดจากการแลกเปลี่ยนข้อมูลในเครือข่ายเฉพาะกิจ

ระบบเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด (Mobile Ad hoc Network: MANET) คือระบบเครือข่ายไร้สายที่ไม่จำเป็นต้องพึ่งพาโครงสร้างพื้นฐาน อีกทั้งยังสามารถขยายขอบเขตการเชื่อมไปยังระบบเน็ตเวิร์คอื่นๆโดยใช้โหนดเกตเวย์เป็นตัวกลางการเชื่อมต่อซึ่งมีข้อจำกัดเรื่องวิธีการค้นหาเกตที่มีอยู่ในปัจจุบันมีโอเวอร์เฮดในการแลกเปลี่ยนข้อมูลสำหรับการค้นหาเกตเวย์จำนวนมาก ดังนั้นในงานวิจัยนี้จึงทำการลดโอเวอร์เฮดดังกล่าวเพื่อปรับปรุงกลไกค้นหาเกตเวย์ ซึ่งอาจส่งผลให้การใช้แบนด์วิดธ์ (Bandwidth) และพลังงานของโมบายล์โหนดในการค้นหาเกตเวย์ลดลง

งานวิจัยฉบับนี้ได้รับการตอบรับจากการประชุมวิชาการระดับชาติด้านเทคโนโลยีสารสนเทศครั้งที่6 (National Conference on Information Technology 2014) [23]

3.4.1 ปัญหาที่ต้องการแก้ไข

ในเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด แต่ละโหนดจะส่งต่อแพ็กเก็ตให้กับโหนดข้างเคียงโดยอาศัยการเชื่อมต่อแบบโหนดต่อโหนด (Peer-to-Peer) ผ่านคลื่นความถี่วิทยุ (Radio Frequency) เช่น เครือข่ายระหว่างยานพาหนะ (VANET : Vehicular ad hoc network) แต่รูปแบบการเชื่อมต่อดังกล่าวทำให้เกิดปัญหาการจำกัดทางด้านขอบเขตของเครือข่าย และในการที่โมบายล์โหนดต้องทำหน้าที่ทุกอย่างไม่ว่าจะเป็น การค้นหาโหนดปลายทาง การสร้างเส้นทาง และการส่งข้อมูล ซึ่งส่งผลให้เกิดปัญหาการใช้พลังงานที่มีอยู่อย่างจำกัด (จากแบตเตอรี่) ของโมบายล์โหนด ผู้วิจัยจึงศึกษารูปแบบการหาเส้นทางบนเครือข่ายเฉพาะกิจของโมบายล์โหนด ให้สามารถหาเส้นทางเชื่อมต่อที่ผ่านเกตเวย์ออกไปยังโครงสร้างพื้นฐานได้ (อย่างเช่น เครือข่ายอินเทอร์เน็ต) เพื่อขยายขอบเขตเครือข่ายในการติดต่อสื่อสารให้กว้างขึ้น ทำให้ติดต่อสื่อสารออกไปนอกพื้นที่ได้ และเพื่อลดการใช้พลังงานที่มีอยู่อย่างจำกัดของโมบายล์โหนดให้ทำงานได้นานขึ้น ซึ่งทำให้ลดโอกาสเกิดความไม่ต่อเนื่องในเครือข่าย โดยเป็นการพัฒนาเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนดให้มีประสิทธิภาพมากยิ่งขึ้นอีกด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

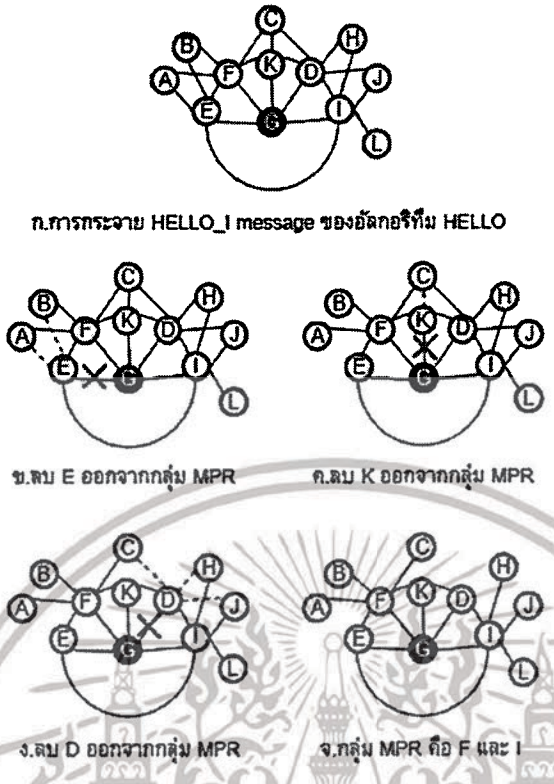
3.4.2 ไอเดียที่ถูกนำเสนอ

วิธีการที่จะนำเสนอนั้นจะมีพื้นฐานมาจากอัลกอริทึม HELLO[24] แต่เพื่อลดการบรอดแคสต์ข้อมูลที่มีปลายทางซ้ำ ๆ กันโดยไม่จำเป็นในระบบเครือข่าย ผู้วิจัยจึงนำวิธีการลดจำนวนโหนดที่ทำการบรอดแคสต์ ซึ่งกลไกนี้แต่เดิมจะถูกใช้ในโพรโทคอลค้นหาเส้นทาง OLSR และมีชื่อเรียกว่าการเลือกโหนดเอ็มพีอาร์ (MPR: Multipoint Relays Selection) มาผนวกเข้ากับอัลกอริทึม HELLO โดยโหนด MPR นั้นเป็นกลุ่มของโหนดข้างเคียง (Neighbor nodes) ที่มีหน้าที่ในการส่งต่อข้อมูล (Retransmission) ซึ่งทุกโหนดที่เป็นโหนดข้างเคียงไม่จำเป็นต้องเป็นโหนด MPR โดยโหนดที่ทำหน้าที่ในการเลือกโหนด MPR จะถูกเรียกว่าผู้คัดเลือกโหนด MPR (MPR Selectors) และกลุ่มของโหนด MPR ก็สามารถเปลี่ยนแปลงได้ตลอดตามความเหมาะสมด้วย

โดยในการคำนวณหาโหนด MPR นั้นจะเริ่มจากการคำนวณโหนดเกตเวย์ และเมื่อคำนวณเสร็จเรียบร้อยแล้วเกตเวย์จะทำการส่ง HELLO_I message ที่บรรจุข้อมูลเกี่ยวกับโหนด MPR ที่เกตเวย์คำนวณได้ออกไป เพื่อระบุว่าโหนดใดเป็นโหนด MPR ไปยังโหนดข้างเคียงในระยะ 1 hop จากนั้นเมื่อโหนดข้างเคียงที่เป็น MPR ได้รับ HELLO_I message ดังกล่าวก็จะทำการคำนวณหาโหนด MPR ของตนต่อไป และส่ง HELLO_I message ไปยังโหนด MPR ที่คำนวณได้ต่อไปเรื่อยๆ พร้อมทั้งบันทึกเส้นทางไปยังเกตเวย์ตามอัลกอริทึม HELLO ที่ได้กล่าวไว้ในส่วนที่ 2 แต่สำหรับโหนดข้างเคียงที่ได้รับ HELLO_I message ไม่ใช่โหนด MPR ก็จะไม่ส่งต่อ HELLO_I message แต่บันทึกเส้นทางไปยังเกตเวย์เพียงเท่านั้น

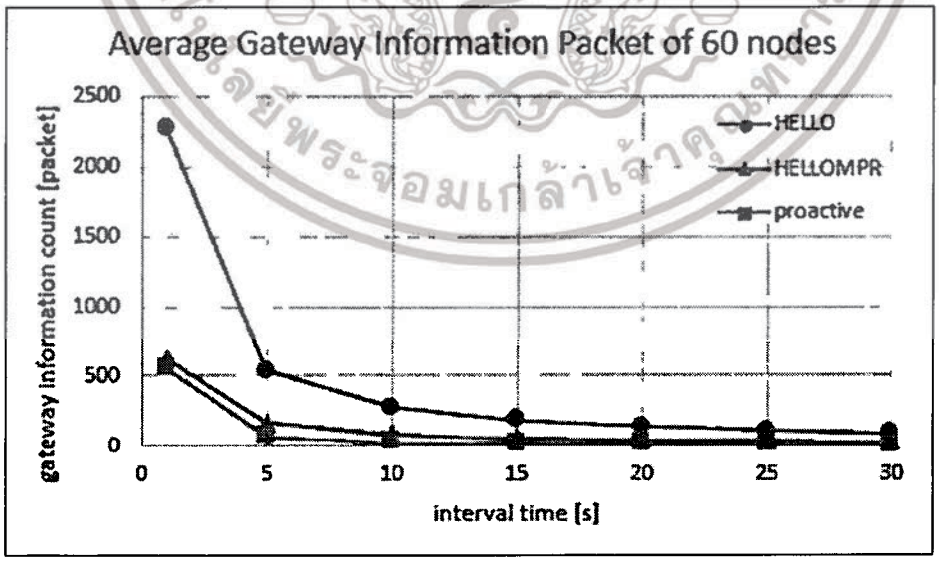
ดังนั้นจึงสรุปได้ว่าอัลกอริทึมที่เราได้พัฒนาได้มีการลดโอเวอร์เฮดจากการแลกเปลี่ยน HELLO_I message ของอัลกอริทึม HELLO คือ การลดจำนวนโหนดที่ทำหน้าที่กระจาย HELLO_I message ซึ่งอาจให้เกิดความซ้ำซ้อน ดังรูปที่ 3.8 (ก) ที่ทุกโหนดต้องทำหน้าที่บรอดแคสต์ข้อความ แต่สำหรับอัลกอริทึมที่เราได้พัฒนาขึ้นโดยขอเรียกว่า HELLOMPR จะมีเพียงบางโหนดที่ทำหน้าที่ในการบรอดแคสต์ ตัวอย่างเช่น ในรูปที่ 3.8 (ก) ที่ใช้อัลกอริทึม HELLO ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด E และ F เมื่อเปรียบเทียบกับรูปที่ 3.8 (จ) ที่ใช้อัลกอริทึม HELLOMPR ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด F เท่านั้น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.8 แสดงตัวอย่างการหากลุ่มโหนด MPR

3.4.3 ผลการทดลอง



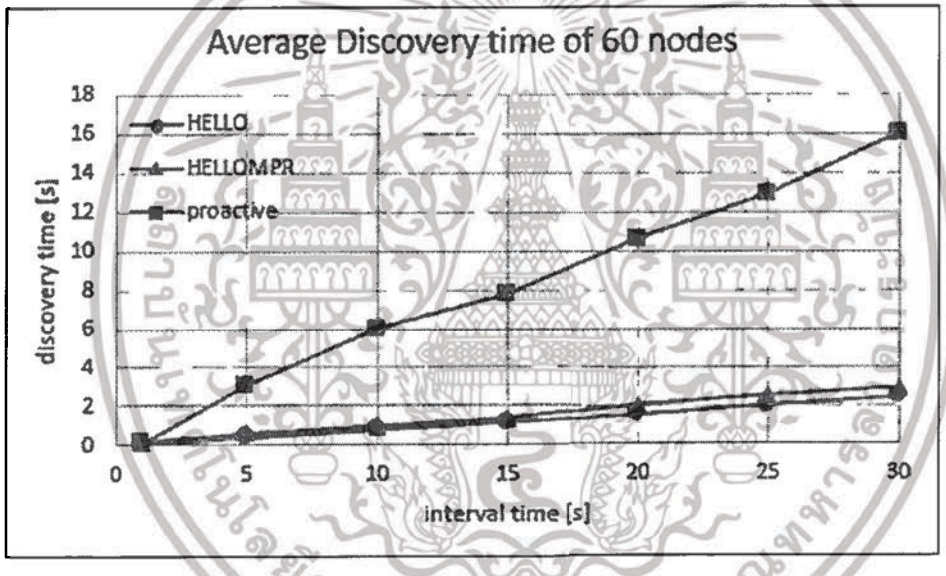
รูปที่ 3.9 แสดงผลการทดลองด้านจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากผลลัพธ์สำหรับอัลกอริทึมที่ถูกนำเสนอ(HELLOMPR)ในรูปที่ 3.9 นั้นแสดงให้เห็นว่ามีจำนวนข้อความในระบบน้อยกว่าอัลกอริทึม HELLO แบบดั้งเดิมก่อนพัฒนา เนื่องจากได้มีการนำกลไกในการลดจำนวนโหนดที่ใช้ในการส่งข้อมูลเส้นทางของโพรโทคอล OLSR เข้ามาเป็นกลไกเพิ่มเติมทำให้มีจำนวนข้อความน้อยลงในระดับที่ใกล้เคียงกับจำนวนข้อความของอัลกอริทึมแบบโพรแอกทีฟ

ในรูปที่ 3.10 นั้นแสดงให้เห็นถึงผลลัพธ์ของการทดลองในตัวชี้วัดด้านเวลาที่ใช้ในการค้นหาเกตเวย์ (Gateway Discovery Time) สำหรับเครือข่ายที่มีโหนดจำนวน 60 โหนด โดยจะเริ่มจับเวลาตั้งแต่เกตเวย์เริ่มประกาศข้อมูลเกี่ยวกับเส้นทางจนกระทั่งถึงเวลาที่โหนดที่สนใจรู้เส้นทางในการติดต่อไปยังเกตเวย์

ซึ่งเห็นได้ชัดเจนว่าอัลกอริทึมแบบโพรแอกทีฟนั้นมีเวลาที่ใช้ในการค้นหาเกตเวย์เป็นครึ่งหนึ่งของช่วงเวลาในการส่งข้อความ ซึ่งถ้าช่วงเวลาดังกล่าวเพิ่มขึ้นเวลาที่ใช้ในการค้นหาเกตเวย์ก็จะเพิ่มขึ้นจนกระทั่งมีค่าสูงมาก ๆ



รูปที่ 3.10 แสดงผลการทดลองด้านเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด

ส่วนอัลกอริทึม HELLO ถึงแม้ช่วงเวลาของการส่งข้อความมากขึ้นแต่เวลาที่ใช้ในการค้นหาเกตเวย์กลับเพิ่มขึ้นเพียงเล็กน้อย แต่ในส่วนของอัลกอริทึม HELLOMPR เมื่อช่วงเวลาในการส่งข้อความเพิ่มขึ้นก็มีเวลาที่ใช้ในการค้นหาเกตเวย์เพิ่มเพียงเล็กน้อยเช่นเดียวกับอัลกอริทึม HELLO แต่เมื่อเทียบกับอัลกอริทึม HELLO แล้วยังมีเวลาที่ใช้ในการค้นหาเกตเวย์มากกว่าเล็กน้อย เพราะผลของกลไกการเลือกโหนดบรอดแคสต์ทำให้บางครั้งโหนดที่สนใจจะได้รับ HELLO_I message ช้ากว่าในกรณีที่โหนดที่สนใจนั้นอยู่ใกล้กับโหนดที่ไม่ได้ถูกเลือกให้บรอดแคสต์มากกว่าโหนดที่ถูกเลือกให้บรอดแคสต์ ดังนั้นโหนดที่สนใจจึงได้รับ HELLO_I message ช้ากว่าอัลกอริทึม HELLO อีกทั้งยังมีเรื่องของระยะห่างระหว่างโหนดที่บรอดแคสต์และโหนดที่สนใจที่แตกต่างกันอีกด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.4.4 แนวทางการพัฒนาต่อยอด

งานวิจัยฉบับนี้ได้มีการพัฒนาต่อยอด และปรับปรุงผลลัพธ์โดยการนำอัลกอริทึมดังกล่าวไปทดสอบในเน็ตเวิร์คที่โหนดมีการเคลื่อนที่และได้รับการตอบรับจากการประชุมทางวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศครั้งที่10 (National Conference on Computing and Information Technology 2014) [25]

3.5 การกระจายโหลดเพื่อการส่งข้อมูลและรองรับการทำงานของทีซีพีเน็ตเวิร์ค

เนื่องจากการใช้งานระบบเครือข่ายในปัจจุบันมีความต้องการส่งข้อมูลจำนวนมากในเวลาเดียวกัน ทำให้ระบบเน็ตเวิร์คจำเป็นต้องขยายขนาดของแบนด์วิธเพื่อรองรับความต้องการของผู้ใช้ แต่ในขณะเดียวกันแนวคิดการใช้วิธีการส่งข้อมูลแบบหลายเส้นทาง (Multipath Routing) ก็ได้ถูกนำมาใช้เป็นวิธีแก้ปัญหาเพื่อส่งข้อมูลจำนวนมากๆ โดยไม่จำเป็นต้องขยายขนาดของแบนด์วิธ ในงานวิจัยฉบับนี้ ผู้วิจัยได้นำเสนอโมเดลการกระจายโหลดที่จะนำมาใช้เพื่อลดความคับคั่งในระบบเน็ตเวิร์ค ลดโอกาสการเต็มของบัฟเฟอร์ และลดการเกิดปัญหาแพ็คเกตรีออร์เดอร์ริ่ง(Packet Reordering) บนระบบเครือข่ายแบบ TCP

งานวิจัยฉบับนี้[26] ได้รับการตอบรับจากการประชุมวิชาการระดับนานาชาติ IEEE International Conference on Information Technology and Electrical Engineering (ICITEE 2013)

3.5.1 ปัญหาที่ต้องการแก้ไข

ในปัจจุบันการส่งข้อมูลแบบหลายเส้นทางนั้นได้มีการพัฒนาไปหลากหลายรูปแบบ โดยมีจุดประสงค์หลักในการเพิ่มความน่าเชื่อถือให้แก่ระบบเน็ตเวิร์คโดยการลดโอกาสที่ระบบเน็ตเวิร์คจะเกิดความผิดพลาดจนกระทั่งไม่สามารถให้บริการได้ เพื่อจะทำให้การส่งข้อมูลแบบหลายเส้นทางมีประสิทธิภาพ [27], [28] การสร้างกลไกเพื่อทำให้เกิดความสมดุลในแต่ละเส้นทางจึงเป็นปัญหาหลักในงานวิจัยชิ้นนี้

3.5.2 ไอเดียที่ถูกนำเสนอ

งานวิจัยชิ้นนี้สนใจการส่งข้อมูลผ่านทราฟฟิคหลายเส้นทาง ในกรณีที่แต่ละเส้นทางมีดีเลย์หรือแบนด์วิธไม่เท่ากัน กลไกที่นำเสนอคือ LDM-EXRED จะใช้กลไก EXRED[29] เป็นตัวทริกเกอร์ ในการสวิชทราฟฟิค จากเส้นทางที่มีความคับคั่งมากไปสู่เส้นทางที่มีความคับคั่งน้อย ซึ่งงานชิ้นนี้ได้มีการพัฒนาต่อยอดมาจากงานวิจัยก่อนหน้าที่ใช้ RED เป็นตัวทริกเกอร์[30]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.5.3 ผลการทดลอง

จากการทดสอบกลไกที่นำเสนอผ่านระบบซิมูเลชั่น(LDM-EXRED) แสดงให้เห็นถึงการกระจายโหลดมีความราบลื่นมากยิ่งขึ้น ในกลไกเก่าที่นำได้เสนอไว้ก่อนหน้า(LDM-RED)นั้นในกรณีที่ระบบเน็ตเวิร์คมีความหนาแน่นไม่มากนักจะไม่ทำการกระจายโหลดไปให้เส้นทางอื่นในทันที แต่ในทางกลับกันถ้าระบบเน็ตเวิร์คมีความหนาแน่นมากก็จะรีบกระจายโหลดอย่างรวดเร็ว เมื่อนำมาเปรียบเทียบกับ LDM-EXRED ที่มีความสมูธในการกระจายโหลดมากกว่า LDM-EXRED จึงสามารถลดการใช้งานบัฟเฟอร์ของแต่ละเส้นทางได้ดียิ่งขึ้น ในขณะที่การใช้บัฟเฟอร์เฉลี่ยแต่ละเส้นทางมีความใกล้เคียงกันมากขึ้นซึ่งแสดงถึงการจัดการโหลดบาลานซิ่งที่ดี นอกจากนี้ ในแง่ของ load balancing efficiency ที่ดีพอๆกันซึ่งดีกว่ากลไกแบบอื่นๆที่มีมาก่อน รวมทั้ง อัตราการเกิดปัญหา packet reordering ก็มีโอกาสเกิดน้อยพอๆกัน ซึ่ง LDM-EXRED มีโอกาสเกิดปัญหา packet reordering น้อย พอๆกับ LDM-RED แต่น้อยกว่ารูปแบบอื่นที่มีมาก่อนค่อนข้างมาก

3.6 การพัฒนาเทคโนโลยีการสื่อสารผ่านดาวเทียมเพื่อใช้ในสถานการณ์ภัยพิบัติ

การสื่อสารผ่านระบบดาวเทียมในปัจจุบันประสบปัญหาเนื่องจากระยะทางระหว่างโหนดต้นทางและโหนดปลายทางมีมาก ส่งผลให้ดีเลย์ในการติดต่อสื่อสารระหว่างโหนดนั้นสูงขึ้น ซึ่งในกรณีที่เกิดความคับคั่งในระบบเครือข่ายแล้ว จะทำให้การแก้ปัญหาเป็นไปได้อย่างล่าช้า งานวิจัยชิ้นนี้จึงถูกพัฒนาขึ้นเพื่อรับมือกับปัญหาดังกล่าว

งานวิจัยนี้ได้รับการตอบรับจากการประชุมวิชาการระดับนานาชาติ International Symposium on Technology for Sustainability (ISTS 2012) [31] และ IEICE Technical Report [32]

3.6.1 ปัญหาที่ต้องการแก้ไข

ในการติดต่อสื่อสารในระบบเน็ตเวิร์ค เมื่อใดก็ตามที่โหนดต้นทางส่งข้อมูลผ่านตัวกลางการสื่อสาร เช่นเราท์เตอร์ ตัวกลางเหล่านั้นจะมีหน้าที่ตรวจสอบความคับคั่งในระบบเครือข่าย ในกรณีที่เครือข่ายมีความหนาแน่นมาก ตัวกลางเหล่านั้นจะทำการเพิ่มข้อมูลลงไปบนเฮดเดอร์ของแพ็คเกจที่ถูกส่งไปเพื่อเปิดการเชื่อมต่อระหว่างโหนดต้นทางและโหนดปลายทาง และเมื่อแพ็คเกจนั้นถูกส่งกลับมา โหนดต้นทางจะทราบว่ามีความหนาแน่นเกิดขึ้น และจะลดปริมาณการส่งข้อมูลลง แต่ในการสื่อสารระหว่างโหนดต้นทางกับดาวเทียมนั้น มีระยะทางที่ไกลมาก ส่งผลให้ระยะเวลาในการส่งข้อมูลต้องใช้มากขึ้น ทำให้วิธีการตรวจสอบดังกล่าว ไม่สามารถแก้ไขปัญหาได้อย่างมีประสิทธิภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.6.2 ไอเดียที่ถูกนำเสนอ

งานวิจัยชิ้นนี้เมื่อตรวจสอบพบว่ามีความหนาแน่นในระบบเน็ตเวิร์ค ตัวกลางจะเพิ่มข้อมูลลงไปบนเฮดเดอร์ของแพ็คเกตที่ถูกส่งกลับมายังโหนดต้นทางล่าสุด ซึ่งไม่จำเป็นต้องเป็นข้อความตอบกลับของโหนดต้นทางนั้นๆ วิธีการดังกล่าวจะทำให้เกิดการแจ้งเตือนโหนดต้นทางบ่อยขึ้น และลดปริมาณการดรอปแพ็คเกจที่เกิดจากความคับคั่งของเครือข่ายลงได้

3.6.3 ผลการทดลอง

จากการชิมมูเลชั่นพบว่า การแจ้งเตือนให้ลดปริมาณการส่งข้อมูลจากโหนดตัวกลางไปยังโหนดต้นทางเกิดมากขึ้น เมื่อเทียบกับการทำงานในรูปแบบเดิม แต่จำนวนแพ็คเกตที่ถูกดรอปนั้นลดลงอย่างเห็นได้ชัด รวมทั้งปริมาณทรูพุธที่เพิ่มขึ้นด้วยเช่นกัน

3.7 เครือข่ายเฉพาะกิจแบบดีทีเอ็นบนสมาร์ทโฟนสำหรับการสื่อสารในสถานการณ์ภัยพิบัติ

เนื่องจากในปัจจุบันสมาร์ทโฟน (Smartphone) เป็นอุปกรณ์สื่อสารที่ได้รับความนิยมและมีการพัฒนาอย่างต่อเนื่อง การสร้างเครือข่ายเฉพาะกิจด้วยสมาร์ทโฟน เป็นการเชื่อมต่อระหว่างสมาร์ทโฟนเครื่องหนึ่งไปยังสมาร์ทโฟนอีกเครื่องหนึ่ง เพื่อให้สามารถแลกเปลี่ยนข้อมูลข่าวสารเหตุการณ์ภัยพิบัติ หรือกระจายข่าวสารเหตุการณ์ภัยพิบัติไปยังเครื่องอื่นๆได้ เป็นช่องทางการสื่อสารที่ไม่ต้องพึ่งพาสาธารณูปโภคพื้นฐานสำหรับผู้ประสบเหตุหรือผู้ประสบภัย รวมทั้งผู้ให้ความช่วยเหลือ ในการรับแจ้งหรือกระจายข่าวออกไป ซึ่งทำให้การช่วยเหลือเป็นไปอย่างมีประสิทธิภาพ ช่วยลดความสูญเสียจากเหตุการณ์ภัยพิบัติลงได้

งานวิจัยนี้จะศึกษาหลักการ Multi-Hop Routing เพื่อสร้างเครือข่ายที่มีการเชื่อมโยงหลาย Hop และหลักการเชื่อมโยงเครือข่าย DTN เพื่อสร้างเครือข่ายที่ไม่สามารถกำหนดเส้นทางการเชื่อมโยงระหว่างผู้ส่งกับผู้รับล่วงหน้าได้ โดยประยุกต์ใช้หลักการดังกล่าวกับการสร้างเครือข่ายสมาร์ทโฟนด้วยเทคโนโลยี Wi-Fi Direct ด้วยหลักการเบื้องต้นนี้ จึงคาดว่าจะสามารถสร้าง เครือข่ายเฉพาะกิจสมาร์ทโฟนเพื่อเป็นระบบสื่อสารสำรอง สำหรับการแจ้งและรับทราบข่าวสาร ในสถานการณ์ที่เครือข่ายสื่อสารที่เป็นโครงสร้างพื้นฐานไม่สามารถทำงานให้บริการได้ตามปกติได้

งานวิจัยดังกล่าวมีความเป็นไปได้และได้ผ่านการพิจารณาสนับสนุนจากสำนักงานคณะกรรมการวิจัยแห่งชาติ(วช.) และในปัจจุบันผู้วิจัยสามารถพัฒนาชิ้นงานไปได้ระดับหนึ่ง โดยสามารถส่งข้อมูลระหว่างสมาร์ทโฟนสองเครื่องด้วยเทคโนโลยี Wi-Fi direct ได้เป็นผลสำเร็จ ซึ่งผลงานการทดลองส่งข้อมูลระหว่างสมาร์ทโฟน [33]ได้รับการตอบรับให้เผยแพร่ในงานประชุมวิชาการ ECTI-CARD ซึ่งจัดขึ้นในวันที่ 21-23 พฤษภาคม 2557

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.8 การศึกษาการประยุกต์ใช้เครือข่ายเซนเซอร์ในระบบควบคุมปัจจัยการเพาะปลูกอัตโนมัติ

ในปัจจุบัน การเพาะเลี้ยงต้นไม้ และไม้ประดับ เป็นอุตสาหกรรมหนึ่งที่น่าสนใจ เพราะสามารถสร้างรายได้ให้กับประเทศ อย่างไรก็ตาม การเพาะเลี้ยงพืชที่มีถิ่นกำเนิดอยู่ในสภาพแวดล้อมที่ต่างจากประเทศไทย และพืชทั่วไปที่มีความอ่อนไหวต่อการเปลี่ยนของสภาพแวดล้อม รวมถึงสภาวะแวดล้อมที่มีความแปรปรวนมากขึ้นในปัจจุบัน ดังนั้นจึงจำเป็นที่จะต้องมีการดูแลอย่างใกล้ชิด ในงานชิ้นนี้จะเป็นการพัฒนาระบบตรวจวัดสภาพแวดล้อมของพืช โดยการประยุกต์ใช้เซ็นเซอร์ต่างๆ ร่วมกับโมดูลส่งข้อมูลไร้สาย เพื่อเก็บบันทึกข้อมูลปัจจัยแวดล้อมตามช่วงเวลาต่างๆ และสามารถเรียกใช้งานได้ผ่านเว็บแอพพลิเคชัน ซึ่งจะทำให้ผู้ใช้งานสามารถนำข้อมูลเหล่านี้ไปปรับสภาพแวดล้อม และรับมือกับการเปลี่ยนแปลงของสภาพภูมิอากาศได้อย่างเหมาะสม.

ผลงานนี้ใช้ประกอบการสำเร็จการศึกษาของนักศึกษาระดับปริญญาตรีสาขาเทคโนโลยีสารสนเทศ จำนวน 2 คน [34]

3.8.1 ปัญหาที่ต้องการแก้ไข

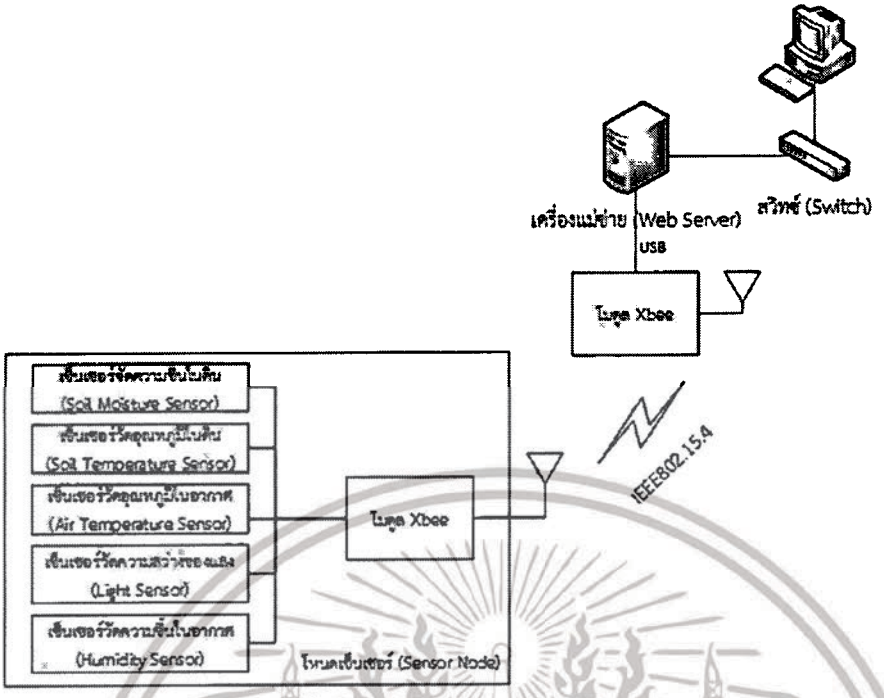
การปลูกพืชในโรงเรือนเพาะปลูก (Greenhouse) เป็นทางเลือกที่น่าสนใจในปัจจุบัน เนื่องจากการที่เป็นระบบปิด ซึ่งป้องกันไม่ให้แมลงเข้าไปทำลายพืชที่เพาะปลูก ป้องกันน้ำฝนลงไปเจือปนในสารละลายธาตุอาหารหรือปุ๋ย และสามารถควบคุมปัจจัยด้านสิ่งแวดล้อมในการเจริญเติบโต รวมถึงพัฒนาการของพืชโดยไม่ต้องอาศัยฤดูกาลตามธรรมชาติ ซึ่งจะช่วยให้สามารถวางแผนการผลิตได้ง่าย และลดความเสี่ยงต่อความแปรปรวนของสิ่งแวดล้อมตามธรรมชาติได้เป็นอย่างดี

จากที่กล่าวมาข้างต้น ผู้วิจัยจึงมีความประสงค์ที่จะพัฒนาระบบเก็บข้อมูลสภาพแวดล้อมในการเพาะปลูกพืชในโรงเรือนเพาะปลูก ซึ่งจะช่วยให้สามารถนำข้อมูลเหล่านี้ไปใช้เพื่อปรับระดับของสภาพแวดล้อมให้เหมาะสม และนำไปวิจัยเพื่อพัฒนาอุปกรณ์ในการปรับระดับสภาพแวดล้อม หรือใช้เป็นข้อมูลในการวิจัยพัฒนาพันธุ์พืชที่เหมาะสมกับสภาพพื้นที่ต่อไปได้

3.8.2 ไอเดียที่ถูกนำเสนอ

ในเครือข่ายเซ็นเซอร์นั้น เซ็นเซอร์จะถูกเชื่อมต่อ และส่งข้อมูลผ่านโมดูล Xbee โดยที่เครื่องแม่ข่ายนั้น จะมีโมดูล Xbee ติดตั้งเช่นกัน โดยทำหน้าที่ในการรอรับข้อมูลเซ็นเซอร์ต่างๆ ที่ส่งมาจากโมดูล Xbee ของโหนดเซ็นเซอร์ในเครือข่ายมาตรฐาน IEEE802.15.4 และรับเฟรมข้อมูลเพื่อนำมาประมวลผลต่อ ระบบสามารถแสดงเป็น Block Diagram ได้ดังรูปที่ 3.11

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 0.11 Block Diagram ของระบบ

เนื่องจากผลงานชิ้นนี้มีการใช้งานเซนเซอร์และอุปกรณ์จำนวนมาก ผู้ใดที่สนใจศึกษาเพิ่มเติมสามารถไปหาอ่านเพิ่มได้จากปริญญานิพนธ์ [34]

3.8.3 ผลการทดลอง

ระบบตรวจวัดสภาพล้อมของพืชที่ได้พัฒนาขึ้นได้นำข้อดีของเทคโนโลยีของเครื่องข่ายเซ็นเซอร์ไร้สายและโครงสร้างแบบตาข่าย ซึ่งติดตั้งง่าย ใช้พลังงานต่ำ เครือข่ายมีความคงทนแม้จะมีบางส่วนเกิดความผิดพลาด รวมถึงเลือกใช้อุปกรณ์ต่างๆ ที่เหมาะสม ลดการใช้อุปกรณ์ที่ไม่จำเป็น ส่งผลให้ต้นทุนในการผลิตโหนดเซ็นเซอร์ต่ำลง โดยที่ยังคงความแม่นยำในการตรวจวัดสภาพแวดล้อมได้เป็นอย่างดีมาทำงานร่วมกับเครื่องแม่ข่าย ซึ่งมีส่วนติดต่อผู้ใช้ที่แสดงข้อมูลสภาพแวดล้อมในรูปของกราฟ ผ่านเว็บแอพพลิเคชั่น และมีการแจ้งเตือนผู้ใช้ถึงความผิดปกติของปัจจัยแวดล้อมที่เปลี่ยนแปลงไป ทำให้การเก็บข้อมูลสภาพแวดล้อมเป็นไปอย่างแม่นยำ ถูกต้องใกล้เคียงกับสภาพความเป็นจริง และทำให้ผู้ใช้ทราบแนวโน้มการเปลี่ยนแปลงของปัจจัยแวดล้อมในช่วงเวลาต่างๆ ซึ่งเป็นข้อมูลที่นำไปสู่การตัดสินใจของผู้ใช้ในการปรับสภาพแวดล้อมให้เหมาะสมกับพืช และสามารถรับมือต่อสภาวะการเปลี่ยนแปลงสภาพภูมิอากาศ โดยที่มีการทำงานทั้งหมดเป็นแบบระบบอัตโนมัติ แสดงให้เห็นว่าเทคโนโลยีสารสนเทศนั้นสามารถนำมาประยุกต์ใช้เพื่อพัฒนาอุตสาหกรรมการเกษตรให้มีความทันสมัยและเพิ่มผลผลิตการเกษตรได้เป็นอย่างดี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.9 การประยุกค์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉินแล้วตำแหน่งที่อยู่เพื่อขอรับบริการรถนำส่งและบริการทางการแพทย์

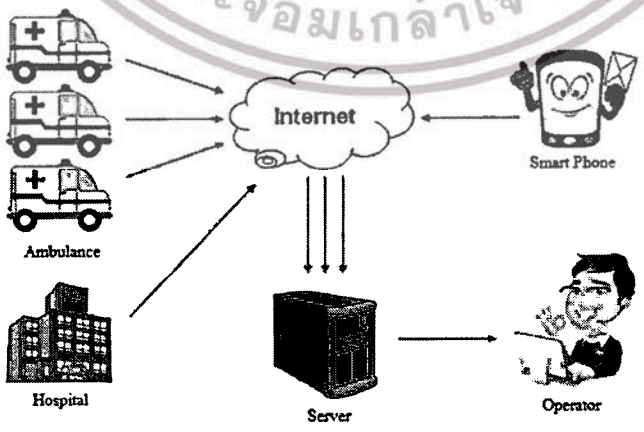
ในปัจจุบันผู้ป่วยฉุกเฉินวิกฤตที่มีสาเหตุมาจากอาการเจ็บป่วยหรืออุบัติเหตุมีมากกว่า 200,000 รายต่อปี โดยระบบที่ใช้ในการรองรับผู้ป่วยดังกล่าวคือระบบสายด่วนฉุกเฉิน 1669 ซึ่งเป็นระบบการแจ้งเหตุผ่านทางโทรศัพท์เพื่อแจ้งที่อยู่ และอาการของผู้ป่วยแก่เจ้าหน้าที่ ก่อนที่เจ้าหน้าที่จะทำการช่วยเหลือต่อไป ซึ่งในบทนี้จะกล่าวถึงการประยุกต์ใช้งานระบบระบุตำแหน่งบนพื้นโลกและสมาร์ทโฟนเพื่อใช้ในการระบุตำแหน่งของผู้ป่วยหรือพื้นที่ที่เกิดอุบัติเหตุ ก่อนที่จะส่งความช่วยเหลือทางการแพทย์ที่เหมาะสมไปยังผู้ป่วย โดยมีระบบช่วยตัดสินใจในการคัดกรองเส้นทาง และเลือกทรัพยากรที่จำเป็นต่อการช่วยเหลือผู้ป่วยเพื่อลดระยะเวลาปฏิบัติการที่ใช้ในการตัดสินใจของเจ้าหน้าที่

งานวิจัยฉบับนี้[35] ได้รับการตอบรับจากการประชุมวิชาการระดับชาติด้านเทคโนโลยีสารสนเทศครั้งที่ 5 (National Conference on Information Technology 2013)

3.9.1 ปัญหาที่ต้องการแก้ไข

ระบบที่ใช้ในการแจ้งเหตุฉุกเฉินในปัจจุบันยังคงใช้วิธีการติดต่อสื่อสารกับผู้ป่วยผ่านทางโทรศัพท์โดยตรง[1] ในการสอบถามอาการและที่อยู่ของผู้ป่วย ซึ่งต้องใช้เวลาและปัจจัยอีกหลายอย่างมาเกี่ยวข้องเพื่อทำให้การสื่อสารในลักษณะนี้ประสบความสำเร็จในสภาวะฉุกเฉิน จึงมีแนวคิดในการประยุกต์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉินเพื่อช่วยเพิ่มช่องทางในการแจ้งเหตุฉุกเฉินและลดระยะเวลาการติดต่อสื่อสารกับเจ้าหน้าที่ในการแจ้งเหตุฉุกเฉิน ประกอบกับระบบช่วยตัดสินใจในส่วนของเจ้าหน้าที่ซึ่งสามารถช่วยลดระยะเวลา และปริมาณข้อมูลที่ใช้ในการตัดสินใจ ส่งผลให้การช่วยเหลือผู้ป่วยมีประสิทธิภาพมากยิ่งขึ้น

3.9.2 ไอเดียที่ถูกนำเสนอ

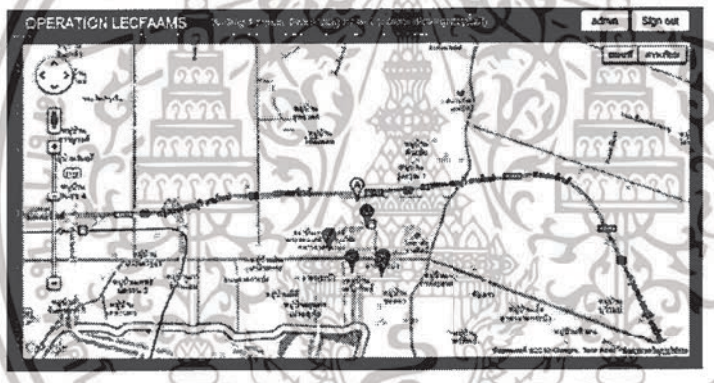


รูปที่ 3.12 ภาพรวมของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากรูปที่ 3.12 หลังจากมีการส่งข้อมูลของผู้ป่วยเข้ามาที่เซิฟเวอร์แล้วระบบจะทำการตรวจสอบพิกัดจีพีเอสที่จุดเกิดเหตุและทำการค้นหาโรงพยาบาลและรถนำส่งที่อยู่ใกล้กับจุดเกิดเหตุ เพื่อสร้างตารางเส้นทางระหว่างโรงพยาบาลและรถนำส่งที่เหมาะสม โดยคำนึงถึงอาการของผู้ป่วยเป็นสำคัญ เพื่อให้สามารถเลือกรถนำส่งที่เหมาะสมไปทำการช่วยเหลือผู้ป่วยได้ ในกรณีที่ไม่สามารถระบุอาการได้ระบบจะนำประวัติส่วนตัวของผู้ป่วยมาประมวลผลแทน จากนั้นเจ้าหน้าที่จะทำการตัดสินใจครั้งสุดท้ายในการเลือกเส้นทางจากตารางที่ระบบสร้างขึ้น และประสานงานไปยังเจ้าหน้าที่ประจำรถนำส่งเพื่อทำการช่วยเหลือผู้ป่วยต่อไป

ในส่วนของระบบช่วยตัดสินใจนั้นแบ่งการทำงานออกเป็น 3 ส่วน คือ ส่วนที่ทำการรับข้อมูล โดยจะรับข้อมูลจากการแจ้งเหตุของผู้ป่วย ข้อมูลเกี่ยวกับรถพยาบาล และข้อมูลของโรงพยาบาลส่วนประมวลผลข้อมูลและเปรียบเทียบข้อมูลเพื่อค้นหาเส้นทางที่เหมาะสม และ ส่วนติดต่อกับเจ้าหน้าที่ในการแสดงผลข้อมูล

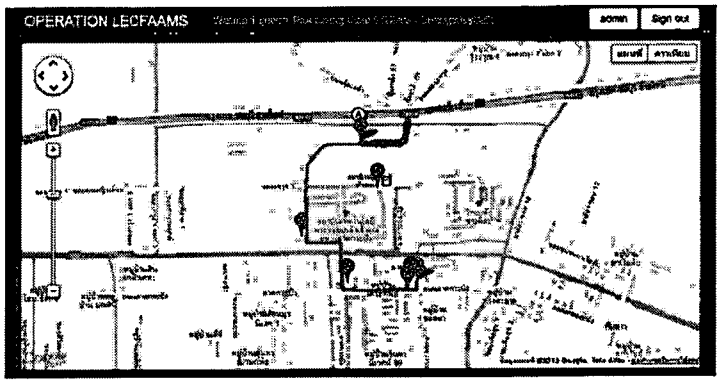


รูปที่ 3.13. หน้าจอปฏิบัติงานของเจ้าหน้าที่สำหรับรับการแจ้งเหตุฉุกเฉินต่างๆ

Path No.	Ambulance	Hospital	Path info	Estimate distance
1	ID:001(B)	LADKRABANG		3.9 KM
2	ID:001(B)	CHULARUT 7		4.1 KM
3	ID:002(A)	CHULARUT7		4.7 KM
4	ID:003(B)	LADKRABANG		5 KM

รูปที่ 3.14 ตารางเปรียบเทียบเส้นทางการนำส่งผู้ป่วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.15 ข้อมูลเส้นทางที่ใช้ในการนำส่งผู้ป่วย

หลังจากระบบรับข้อมูลการแจ้งเหตุจากผู้ป่วยแล้ว ข้อมูลดังกล่าวจะถูกแสดงผลออกมาดังตัวอย่างในรูปที่ 3.13 ซึ่งจะแสดงหน้าจอระบบช่วยตัดสินใจของเจ้าหน้าที่ โดยจะแสดงผลตำแหน่งของจุดเกิดเหตุ รถพยาบาลและโรงพยาบาลที่อยู่ใกล้กับจุดเกิดเหตุลงบนแผนที่ จากนั้นจึงทำการประมวล และแสดงผลออกมาในรูปแบบตารางแนะนำเส้นทางดังรูปที่ 3.14 ซึ่งเรียงลำดับตามระยะทางจากรถพยาบาลไปยังจุดเกิดเหตุรวมกับระยะทางจากจุดเกิดเหตุไปยังโรงพยาบาลที่ใกล้ที่สุด และจะแสดงผลข้อมูลระดับของรถพยาบาลซึ่งมีอยู่ทั้งหมด 4 ระดับ[1] แบ่งตามความพร้อมของอุปกรณ์ช่วยเหลือที่มีอยู่บนรถพยาบาลนั้นๆ (ในรูปที่ 3.13 สมมุติว่ามีรถพยาบาลระดับ A และ B อยู่ในบริเวณที่มีการแจ้งเหตุ) โดยเจ้าหน้าที่จะทำการเลือกเส้นทางและรถพยาบาลที่เหมาะสมกับผู้ป่วย และส่งข้อมูลเส้นทางดังรูปที่ 3.15 ไปยังเจ้าหน้าที่ประจำรถพยาบาลผ่านทางเว็บไซต์ โดยจะนำเส้นทางที่ได้ไปแสดงผลบนอุปกรณ์ระบุพิกัดจีพีเอสที่ติดตั้งอยู่บนรถพยาบาล เพื่อให้เจ้าหน้าที่ประจำรถพยาบาลสามารถทำการช่วยเหลือผู้ป่วยได้อย่างรวดเร็ว

3.9.3 ผลการทดลอง

ระบบที่นำเสนอจะสามารถแจ้งเหตุฉุกเฉินได้รวดเร็วกว่าเมื่อเปรียบเทียบการแจ้งเหตุผ่านโทรศัพท์ซึ่งต้องระบุทั้งที่อยู่ และอาการของผู้ป่วย ในขณะที่การใช้พิกัดจีพีเอสสามารถระบุตำแหน่งได้แม่นยำและใช้เวลาน้อยกว่าเพียงกดปุ่มบนสมาร์ทโฟนซึ่งใช้เวลาเพียงไม่กี่วินาที รวมทั้งสามารถระบุอาการของผู้ป่วยได้พร้อมกัน แต่อาจมีข้อเสียในเรื่องความละเอียดของอาการที่สามารถระบุได้ แต่ถ้าคำนึงถึงสภาวะของผู้ป่วยที่แตกต่างกันในกรณีที่ผู้ป่วยมีสติไม่มากพอที่จะสื่อสารได้ ระบบเก่าจะไม่สามารถทำงานได้เลย ในขณะที่ระบบใหม่ใช้ปริมาณการตัดสินใจน้อยกว่าการโทรศัพท์มาก ในส่วนปัญหาด้านความคลาดเคลื่อนของการระบุตำแหน่งจีพีเอส อาจส่งผลต่อความแม่นยำในการคำนวณเส้นทางในการนำส่งผู้ป่วยได้ แต่ปัญหานี้สามารถถูกแก้ไขได้ด้วยการอัพเดทพิกัดจีพีเอสใหม่ โดยระบบจะมีการอัพเดทพิกัดจีพีเอสของผู้ป่วยอยู่เป็นระยะ ดังนั้นปัญหานี้จึงได้รับการแก้ไขอย่างอัตโนมัติ ในด้านการจัดการทรัพยากรระบบเก่าไม่มีการแสดงข้อมูลรถนำส่งทั้งหมดที่สามารถปฏิบัติการได้ในขณะนั้น จึงทำให้การตัดสินใจของเจ้าหน้าที่อาจผิดพลาดได้ ในส่วนของระบบช่วยตัดสินใจที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพิ่มเข้ามาจะทำให้เจ้าหน้าที่สามารถทำงานได้ง่ายและรวดเร็วขึ้น แต่อย่างไรก็ตามระบบใหม่ก็ยังไม่สามารถป้องกันปัญหาการแจ้งข้อมูลเท็จได้

3.9.4 แนวทางการพัฒนาต่อยอด

ผลงานที่กล่าวถึงในบทนี้ได้ถูกส่งเข้าประกวดในงาน National software Contest ประจำปี 2013 และได้ผ่านเข้าสู่รอบก่อนรองชนะเลิศ

3.10 การประยุกต์ใช้สมาร์ทโฟนเพื่อการพิสูจน์ตัวตนด้วยข้อมูลพิกัดจีพีเอส

เนื่องด้วยความสามารถของโทรศัพท์สมาร์ทโฟนที่เหนือกว่าโทรศัพท์มือถือพื้นฐานทั่วไป ทำให้ปัจจุบันโทรศัพท์สมาร์ทโฟนกลายเป็นอุปกรณ์สื่อสารที่มีผู้คนนิยมใช้มากขึ้นเรื่อยๆ โดยภายในโทรศัพท์สมาร์ทโฟนจะมีเครื่องรับสัญญาณตำแหน่งดาวเทียมหรือจีพีเอส ซึ่งสามารถนำมาประยุกต์ใช้ประโยชน์ได้มากมาย หนึ่งในนั้นคือการระบุตำแหน่งเพื่อยืนยันตัวตนของผู้ใช้โดยจีพีเอส เพื่อช่วยในการระบุตำแหน่ง โดยจะใช้ประกอบกับการทำธุรกรรมทางการเงินผ่านบัตรเครดิต ทำให้ผู้ใช้มีความปลอยภัยจากผู้ไม่ประสงค์ดีที่จะทำการบิดเบือนข้อมูลที่มีความสำคัญไปหรือโจรกรรมบัตรเครดิตเพื่อนำไปใช้โดยผิดกฎหมาย

งานวิจัยฉบับนี้[36] ได้รับการตอบรับจากการประชุมวิชาการระดับชาติด้านเทคโนโลยีสารสนเทศครั้งที่ 5 (National Conference on Information Technology 2013)

3.10.1 ปัญหาที่ต้องการแก้ไข

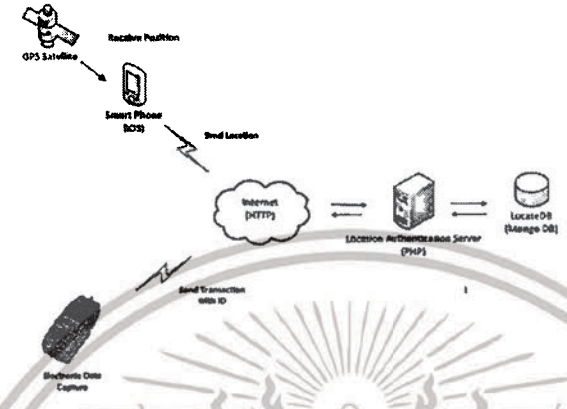
จากการที่เทคโนโลยีของการซื้อขายแลกเปลี่ยนสินค้าและเทคโนโลยีของโทรศัพท์สมาร์ทโฟนมีการพัฒนาไปอย่างต่อเนื่อง แต่ความปลอดภัยในการซื้อขายนั้นยังไม่มีการเพิ่มประสิทธิภาพมากนัก โครงการนี้จึงจะทำการเพิ่มความปลอดภัยในการซื้อสินค้าผ่านบัตรเครดิต โดยมีการนำ GPS ของสมาร์ทโฟน มาประยุกต์ใช้ในการยืนยันระบุตัวตนว่าบุคคลผู้เป็นเจ้าของบัตรเครดิตนั้นอยู่ในสถานที่ที่มีการทำธุรกรรมทางการเงินนั้นจริงหรือไม่ ซึ่งถือเป็นการเพิ่มความปลอดภัยต่อการทำธุรกรรมทางการเงินของลูกค้าบัตรเครดิตได้เป็นอย่างดี

3.10.2 ไอเดียที่ถูกนำเสนอ

การทำงานโดยรวมนั้นสามารถสรุปเป็นใจความสำคัญได้คือ “ไม่มีสมาร์ทโฟน ไม่มีการซื้อขาย” โดยจะใช้โทรศัพท์สมาร์ทโฟนเป็นเครื่องมือช่วยในการระบุตำแหน่งของผู้ใช้งานที่จะไปซื้อของในห้างสรรพสินค้าหรือร้านค้าต่างๆ ที่มีเครื่องรูดบัตรเครดิต แต่เครื่องรูดบัตรเครดิตไม่สามารถที่จะส่งข้อมูลพิกกัดบนแผนที่ไปยังเครื่องเซิฟร์เวอร์ได้โดยตรง ซึ่งจะใช้วิธีการเก็บข้อมูลพิกัดของเครื่องรูดบัตรไว้ภายในฐานข้อมูลก่อน เมื่อมีการรูดบัตรเกิดขึ้นตัวเครื่องจะส่งหมายเลขบัตรเครดิต จำนวนเงินที่ซื้อ และรหัสเครื่องซึ่งจะข้อมูลรหัสเครื่องนี้ใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การตรวจสอบว่าเครื่องนี้อยู่ที่ใดบนแผนที่ และนำไปเทียบกับพิกัดของผู้ใช้ว่ามีควสใกล้เคียงกันหรือไม่ ถ้าหากอยู่ไกลมากต้องทำอย่างไร โดยต้องมีเครื่องเซิร์ฟเวอร์เพิ่มขึ้นมากจากเดิมหนึ่งเครื่องและฐานข้อมูลเพื่อเก็บข้อมูลต่างๆ



รูปที่ 3.16. ภาพจำลองระบบการทำงาน

3.10.3 ผลการทดลอง

แอพพลิชันนี้สามารถเพิ่มความปลอดภัยให้กับบัตรเครดิตให้ไม่สามารถที่จะรูดซื้อของโดยที่เจ้าของบัตรนั้นไม่ยินยอม และการที่จะใช้แอพพลิเคชันนั้นไม่ใช่เรื่องยาก เพียงแต่เข้าไปในแอพพลิเคชันและกดส่งข้อมูลเท่านั้น โดยยอมเสียเวลาไม่มากเพื่อความปลอดภัยที่เพิ่มเข้ามาอย่างมาก ซึ่งระบบการจ่ายเงินด้วยบัตรเครดิตแบบเดิมไม่มีสิ่งใดระบุตัวตนนอกจากลายเซ็นต์หลังบัตรเท่านั้น แต่หากพื้นที่ของห้างสรรพสินค้าอยู่ในพื้นที่ที่ไม่มีสัญญาณดาวเทียมหรือไม่สามารถรับสัญญาณจากดาวเทียมได้ การกดส่งข้อมูลพิกัดไปจะไม่ตรงตามตำแหน่งที่อยู่ปัจจุบัน การตรจสอบจากเซิร์ฟเวอร์จะไม่อนุมัติ แต่ปัญหานี้ได้สามารถแก้โดย หากข้อมูลพิกัดที่ส่งมานั้นอยู่ห่างกับตำแหน่งของเครื่องรูดบัตรมากๆ หรือไม่ได้อยู่ในบริเวณนั้นเลย เซิรฟเวอร์จะส่ง Push Notification เข้ามาให้ลูกค้าเพื่อให้กดปุ่ม บังคับซื้อแทน โดยวิธีนี้อาจเป็นข้อจำกัดที่อาจมีคนแอบนำโทรศัพท์สมาร์ทโฟนและบัตรเครดิตของเจ้าของไปใช้พร้อมกันได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

บทสรุป

ห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายโมบายล์และเซนเซอร์เน็ตเวิร์ค (Mobile Computing and Sensor Networks) ได้มีการศึกษางานวิจัยที่เกี่ยวข้องเพื่อรวบรวมองค์ความรู้ใหม่ และนำมาพัฒนาต่อยอดเพื่อนำไปสู่เทคโนโลยีใหม่ที่จะเกิดขึ้นในอนาคต โดยอาจารย์ประจำห้องวิจัยมีเป้าหมายที่จะพัฒนาองค์ความรู้ด้านเทคโนโลยีเครือข่ายให้แก่นักศึกษาที่เข้ามาเป็นผู้ช่วยวิจัย ซึ่งผลงานบางส่วนก็ถูกพัฒนาขึ้นร่วมกับนักศึกษา และบุคลากรจากต่างประเทศ

ในด้านการวิจัย ห้องวิจัยฯมี 11 ผลงานที่ได้รับการเผยแพร่ในงานประชุมวิชาการ โดยมี 3 ผลงานซึ่งวิจัยร่วมกับต่างประเทศ ได้รับการเผยแพร่ในงานประชุมวิชาการระดับนานาชาติ และมี 8 ผลงานที่ได้รับการเผยแพร่ในงานประชุมวิชาการระดับชาติ หนึ่งในผลงานนี้ได้ผ่านเข้ารอบก่อนรองชนะเลิศในงาน National Software Contest (NSC) 2013

ในด้านการเรียนการสอน ห้องวิจัยฯสนับสนุนการผลิตบัณฑิตทั้งในระดับปริญญาตรีและบัณฑิตศึกษา มีนักศึกษาที่เข้ามาร่วมทำงานในห้องวิจัยฯรวมทั้งสิ้น 14 คน ในปีการศึกษา 2555 สำเร็จการศึกษาระดับปริญญาตรีไปแล้วทั้งสิ้น 5 คน และในปีการศึกษา 2556 กำลังจะสำเร็จการศึกษาระดับปริญญาตรี 7 คน และระดับปริญญาโท 2 คน นอกจากนี้ห้องวิจัยฯ ยังให้บริการยืมอุปกรณ์โมบายล์เพื่อการทดลอง หรือการพัฒนาแอพพลิเคชั่นต่างๆแก่นักศึกษาหรือคณาจารย์

จากผลงานที่กล่าวมาทั้งหมดนั้นสามารถแสดงถึงประสิทธิภาพ และศักยภาพของห้องปฏิบัติการวิจัยและพัฒนาระบบเครือข่ายอุปกรณ์โมบายล์และเซนเซอร์เน็ตเวิร์ค ซึ่งมีผลงานบรรลุวัตถุประสงค์ของโครงการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

[1] M. K. Jeya Kumar, R. S. Rajesh., "A Survey of MANET Routing Protocols in Mobility Models." Medwell Journals, 2009. [Available Online]: http://www.medwelljournals.com/fulltext/?doi=ijscomp.2009.136.141

[2] Sunil Taneja, Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks." Reading: International Association of Computer Science and Information Technology, Aug. 2010.

[3] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)." Internet Engineering Task Force (IETF) draft, Feb. 2007. [Available Online] :http://datatracker.ietf.org/doc/rfc4728/

[4] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. "Ad hoc On-Demand Distance Vector(AODV) Routing." Internet Engineering Task Force (IETF) draft, Jul. 2003, [Available Online]: http://datatracker.ietf.org/doc/rfc3561/

[5] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot. ,"Optimized Link State Routing Protocol (OLSR)." Internet Engineering Task Force (IETF) draft, Oct. 2003. [Available Online]: https://datatracker.ietf.org/doc/ rfc3626/

[6] Y. KO and N.H. Vaidya. "Location-Aided Routing (LAR) in mobile Ad Hoc Networks", Journal Wireless network, vol. 6, pp. 307–321, Jul. 2000.

[7] R. Bajaj, S. L. Ranaweera and D. P. Agrawal, "GPS: Location-Tracking Technology", IEEE Computer, Vol. 35, No. 4, 2002, pp. 92–94. Apr. 2012

[8] S. Basagni et al., "A Distance Routing Effect Algorithm for Mobility (DREAM)" ACM/IEEE Int'l. Conf. Mobile Comp. Net., 1998, pp. 76–84.

[9] Scott Burleigh, Adrian Hooke, Leigh Torgerson. Delay-Tolerant Network (DTNs) A Tutorial. Reading: DTN Research Group Internet Draft, Mar. 2013.

[10] Jones, Evan PC, et al. "Practical routing in delay-tolerant networks." Mobile Computing, IEEE Transactions on 6.8 (2007): 943–959.

[11] Jones, Evan PC, and Paul AS Ward, "Routing strategies for delay-tolerant networks." Submitted to ACM Computer Communication Review (CCR) (2006).

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[12] Vahdat, Amin, and David Becker. Epidemic routing for partially connected ad hoc networks. Technical Report CS-200006, Duke University, 2000.

[13] Lu, Xiaofeng, and Pan Hui, "An energy-efficient n-epidemic routing protocol for delay tolerant networks." Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on. IEEE, 2010.

[14] De Rango, and Amelio S. ,"Performance evaluation of scalable and energy efficient dynamic n-epidemic routing in Delay Tolerant Networks" Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2013 International Symposium on. IEEE, 2013.

[15] Wi-Fi CERTIFIED Wi-Fi Direct™ Consumer. Reading: Wi-Fi Alliance®, Oct. 2010.

[16] Wi-Fi CERTIFIED Wi-Fi Direct™ Industry. Reading: Wi-Fi Alliance®, Oct. 2010.

[17] S-C. Yeh, W-H. Hsu, M-Y. Su, C-H. Chen, and K-H. Liu, "A Study on Outdoor Positioning Technology Using GPS and WiFi Networks," in *Proc. of the 2009 IEEE International Conference on Networking, Sensing and Control*, Okayama, Japan, Mar. 26–29, 2009.

[18] A. Chandra, S. Jain, and M. A. Qadeer, "GPS Locator: An Application for Location Tracking and Sharing Using GPS for Java Enabled Handhelds," in Proc. of the International Conference on Computational Intelligence and Communication Networks (CICN) 2011, Gwalior, India, pp. 406–410, Oct. 7–9, 2011.

[19] G. B. Al-Suwaidi and M. J. Zemerly, "Locating friends and family using mobile phones with global positioning system (GPS)," in Proc. of the IEEE/ACS International Conference on Computer Systems and Applications 2009 (AICCSA 2009), Rabat, Morocco, pp. 555–558, May 10–13, 2009.

[20] ศุภโชค พงษ์ขวัญ, วรวัชร ณรงคะชวนะ, และ สุเมธ ประภาวัต, "การปรับปรุงการแบ่งโหลดเพื่อกระจายข้อมูลหลายทางบนเครือข่ายเฉพาะกิจเคลื่อนที่," งานประชุมวิชาการระดับประเทศด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ (National Conference on Computing and Information Technology: NCCIT) ครั้งที่ 10, ภูเก็ต, ประเทศไทย, พ.ค. 2557.

[21] ธนานพ ทองถาวร, วรวัชร ณรงคะชวนะ, และ สุเมธ ประภาวัต, "การศึกษาความเป็นไปได้ในการลดโอเวอร์เฮดบนระบบเครือข่ายไร้สายเฉพาะกิจ โดยการสร้างเงื่อนไขในการจำกัดการกระจายข้อมูลในขั้นตอนการค้นหาเส้นทาง," รายงานการประชุมวิชาการระดับประเทศด้านเทคโนโลยีสารสนเทศ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

(National Conference on Information Technology: NCIT) ครั้งที่ 6, นครราชสีมา,ประเทศไทย, ก.พ. 2557, หน้า 125–129.

[22] ธีรพงษ์ โชคสถิตย์, เบญจพร ปาวะรีย์, วรวัชร ณรงคะชวนะ, และ สุเมธ ประภาวัต, "การปรับปรุงกลไกการแพร่กระจายข้อความเพื่อลดการแลกเปลี่ยนข้อมูลบนเครือข่ายดีทีเอ็น," รายงานการประชุมวิชาการระดับประเทศด้านเทคโนโลยีสารสนเทศ (National Conference on Information Technology: NCIT) ครั้งที่ 6, นครราชสีมา, ประเทศไทย, ก.พ. 2557, หน้า 212–217.

[23] สุเมธ ประภาวัต, ทะนง ชูวณิชชานนท์, สารัช ศรีสวัสดิ์พงษ์ และ วรวัชร ณรงคะชวนะ, "การปรับปรุงกลไกค้นหาเกตเวย์เพื่อลดโอเวอร์เฮดจากการแลกเปลี่ยนข้อมูลในเครือข่ายเฉพาะกิจ," รายงานการประชุมวิชาการระดับประเทศด้านเทคโนโลยีสารสนเทศ (National Conference on Information Technology: NCIT) ครั้งที่ 6, นครราชสีมา, ประเทศไทย, ก.พ. 2557, หน้า 119–124.

[24] M. Rosenschon, T. Manz, J. Habermann, and V. Rakocevic, "Gateway Discovery Algorithm for Ad-Hoc Networks using HELLO Messages," in Proc. International Workshop on Wireless Ad Hoc Networks (IWWAN 2005), London, UK, May 2005.

[25] สุเมธ ประภาวัต, สารัช ศรีสวัสดิ์พงษ์, ทะนง ชูวณิชชานนท์, และ วรวัชร ณรงคะชวนะ, "กลไกค้นหาเกตเวย์ที่มีโอเวอร์เฮดจากการแลกเปลี่ยนข้อความต่ำสำหรับเครือข่ายเคลื่อนที่เฉพาะกิจ," งานประชุมวิชาการระดับประเทศด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ (National Conference on Computing and Information Technology: NCCIT) ครั้งที่ 10, ภูเก็ต, ประเทศไทย, พ.ค. 2557.

[26] S. Prabhavat, R. Varakulsiripunth, S. Utsumi, and Yasushi Kato, "Load Distribution using Modified RED for Multipath TCP Communication," in Proc. IEEE International Conference on Information Technology and Electrical Engineering (ICITEE 2013), Yogyakarta, Indonesia, Oct. 2013, pp. 287–290.

[27] S. Prabhavat and R. Varakulsiripunth, "Performance Improvement on RED Based Gateway in TCP Communication Network," in Proc. International Conference on Control, Automation and Systems (ICCAS2004), Bangkok, Thailand, Aug. 2004, pp. 782–787.

[28] S. Prabhavat, N. Kato, and R. Varakulsiripunth, "Load Distribution Mechanism for Multipath TCP Communication," in Proc. International Symposium on Technology for Sustainability (ISTS 2011) , Bangkok, Thailand, Jan. 2012, pp. 321–324.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[29] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "Effective Delay-Controlled Load Distribution over Multipath Networks," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 10, pp.1730– 1741, Oct. 2011.

[30] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "On Load Distribution over Multipath Networks," IEEE Communications Surveys and Tutorials, vol. 14, no. 3, pp. 662–680, Jul. 2012.

[31] M. Inoue, P. Tangdumrongrat, S. Prabhavat, S. Utsumi, S. Zabir, and N. Shiratori, "Mark-Reverse Explicit Congestion Notification for Satellite IP Networks: Simulation and Analysis Results," in Proc. International Symposium on Technology for Sustainability (ISTS 2012), Bangkok, Thailand, Nov. 2012, pp. 127–130.

[32] M. Inoue, P. Tangdumrongrat, S. Prabhavat, S. Utsumi, S. M. S. Zabir, N. Shiratori, "Mark-Reverse Explicit Congestion Notification: Concept, Analysis and Evaluation," IEICE Technical Report, vol. 112, no. 208, NS2012-79, Sep. 2012, pp. 153–158.

[33] ธีรพงษ์ โชคสถิตย์, เบญจพร ปาวะรีย์, และ สุเมธ ประภาวัต, "การพัฒนาระบบสื่อสารสมาร์ทโฟนด้วยเทคโนโลยี WiFi-Direct," การประชุมวิชาการงานวิจัยและพัฒนาเชิงประยุกต์ครั้งที่ 6 การพัฒนาเทคโนโลยีเพื่อให้โลกมีสันติสุข (ECTI-CARD Proceedings 2014), เชียงใหม่, ประเทศไทย, พ.ค. 2557.

[34] วรวัชร ณรงคะชวนะ, สรัล วีรกุล, ปานวิทย์ ธุวะนุติ, และ สุเมธ ประภาวัต, "การศึกษาการประยุกต์ใช้เครือข่ายเซ็นเซอร์ในระบบควบคุมปัจจัยการเพาะปลูกอัตโนมัติ," ปริญญานิพนธ์วิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง, 2557.

[35] สุเมธ ประภาวัต, ธนานพ ทองถาวร, และ ณัชชา วัฒนอรุณกิจ, "การประยุกต์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉิน และตำแหน่งที่อยู่ เพื่อขอรับบริการรถนำส่ง และบริการทางการแพทย์," รายงานการประชุมวิชาการระดับประเทศด้านเทคโนโลยีสารสนเทศ (National Conference on Information Technology: NCIT) ครั้งที่ 5, เพชรบุรี, ประเทศไทย, ก.พ. 2556, หน้า 137–140.

[36] สุเมธ ประภาวัต, นิติ ชัยกะเสวี, และ ภรภัทร นนทะบรรหาญ, "การประยุกต์ใช้สมาร์ทโฟนเพื่อการพิสูจน์ตัวตนด้วยข้อมูลพิกัดจีพีเอส," รายงานการประชุมวิชาการระดับประเทศด้านเทคโนโลยีสารสนเทศ (National Conference on Information Technology: NCIT) ครั้งที่ 5, เพชรบุรี, ประเทศไทย, ก.พ. 2556, หน้า 141–144.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารแนบ

ผลงานที่ได้รับการเผยแพร่



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การปรับปรุงการแบ่งโหลดเพื่อกระจายข้อมูลหลายทางบนเครือข่ายเฉพาะกิจเคลื่อนที่
Multipath Load-balancing Improvement on Mobile Ad-hoc Network

ศุภโชค พงษ์ขวัญ (Supachoke Pongquan) วรวัชร ณรงคะชวนะ (Worrawat Narongkhachavana)
และ สุเมธ ประภาวัต (Sumet Prabhavat)
คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ
aquarix38425@gmail.com, worrawat@gmail.com, sumet@it.kmitl.ac.th

บทคัดย่อ

ความล้มเหลวของการสื่อสารบนเครือข่ายเฉพาะกิจ มักมีสาเหตุมาจากเส้นทางที่ใช้งานอยู่ถูกตัดขาด อันเนื่องมาจากการสูญหายของโมบายล์โหนด เช่น การเคลื่อนที่ของโมบายล์โหนด พลังงานที่จำกัดของโมบายล์โหนด เป็นต้น งานวิจัยนี้จึงพัฒนารูปแบบวิธีการส่งข้อมูลโดยใช้การส่งข้อมูลหลายเส้นทาง และวิธีการเลือกเส้นทางของโปรโตคอลซึ่งส่งผลให้สามารถใช้งานเส้นทางที่ถูกเลือกได้อย่างมีประสิทธิภาพ จากผลการจำลองการส่งข้อมูลระหว่างโมบายล์โหนด แสดงให้เห็นถึงการเพิ่มขึ้นของอัตราสำเร็จในการส่งข้อมูล และเวลาที่ใช้ในการทำงานลดลง

คำสำคัญ: เครือข่ายสื่อสารเฉพาะกิจ การส่งข้อมูลหลายเส้นทาง การกระจายโหลดของเครือข่าย

Abstract

Mobile Ad-hoc network has been popularly focused in recent years. Major problem of Mobile Ad-hoc network is the mobility of mobile nodes which could bring packet delivery failure into the network. This paper aims to develop multipath load-balancing algorithm into multipath routing protocol based on Dynamic Source Routing Protocol (DSR). The algorithm use multiple routes found from route discovery process and utilize that routes by using per-packet allocation scheme. We use extensive simulation to show the result which increase success ratio and reduce overall worktime.

Keyword: Mobile Ad-hoc Network, Dynamic Source Routing Load Balancing, Multipath Routing.

1. บทนำ

เทคโนโลยีการสื่อสารคือหัวใจสำคัญของระบบเครือข่าย ซึ่งมีทั้งระบบเครือข่ายแบบ Infrastructure ที่จำเป็นต้องพึ่งพาอุปกรณ์ที่ทำหน้าที่รับ-ส่ง ข้อมูล โดยหากเกิดเหตุไม่คาดฝันที่ทำให้ระบบ Infrastructure ไม่สามารถทำงานได้ ก็จะทำให้การสื่อสารขัดข้อง เป็นที่มาของระบบเครือข่ายไร้สายเฉพาะกิจ (Ad Hoc Network) ซึ่งเป็นระบบเครือข่ายแบบที่ไม่จำเป็นต้องมีอุปกรณ์ที่ทำหน้าที่รับ-ส่งข้อมูล เป็นตัวกลาง (Infrastructureless) เพื่อที่จะให้การติดต่อสื่อสารเป็นไปได้ในเวลาที่เกิดเหตุขัดข้องจนระบบ Infrastructure ไม่สามารถทำงานได้

Mobile Ad Hoc Network (MANET) [1] เป็นระบบเครือข่ายแบบ Infrastructureless ที่ทำงานด้วยเทคโนโลยีเครือข่ายไร้สาย โดยเทคโนโลยีที่แพร่หลายที่สุดก็คือเทคโนโลยี IEEE 802.11 หรือ Wi-Fi ซึ่งมีอยู่ในสมาร์ทโฟนทั่วไป ดังนั้นการนำเทคโนโลยี Wi-Fi มาใช้สำหรับสร้างเครือข่ายเฉพาะกิจของสมาร์ทโฟนจึงเป็นทางเลือกที่ดีในการทำให้เกิดเครือข่ายสื่อสารในสถานการณ์วิกฤตดังกล่าวได้

แต่ปัญหาของการสร้างเครือข่าย MANET ด้วยเทคโนโลยี Wi-Fi ก็คือ โมบายล์โหนดในเครือข่าย MANET มีโอกาสสูงที่จะขาดการเชื่อมต่อจากกัน เพราะเทคโนโลยี Wi-Fi ไม่เหมาะสมกับการใช้งานกับเครือข่ายที่โมบายล์โหนดมีการเคลื่อนที่ เนื่องจากเทคโนโลยีดังกล่าวมีระยะการเชื่อมต่อค่อนข้างสั้น ทำให้มีโอกาสที่โมบายล์โหนดจะเคลื่อนที่ออกนอกจากระยะการเชื่อมต่อ ส่งผลให้มีโอกาสเกิดการขาดการเชื่อมต่อระหว่างโมบายล์โหนดต้นทางและปลายทาง ซึ่งนำไปสู่ปัญหาความยั่งยืนทนทานของเครือข่าย ดังนั้นการมีการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หาเส้นทางหลายเส้นในเครือข่าย MANET สามารถลดโอกาสเกิดการขาดการเชื่อมต่อระหว่างโมบายล์โหนดต้นทางและปลายทางได้ จึงเป็นทางเลือกที่เป็นไปได้ในการแก้ปัญหาดังกล่าว

ในส่วนที่ 2 จะกล่าวถึงทฤษฎีพื้นฐานที่เกี่ยวข้องและนำมาพัฒนา, ส่วนที่ 3 มีการอธิบายรายละเอียดอัลกอริทึมที่นำมาใช้พัฒนาระบบเครือข่าย, ส่วนที่ 4 เป็นการประเมินผลการทดลองของอัลกอริทึมที่พัฒนาขึ้นมา โดยเปรียบเทียบกับโปรโตคอลหลักที่นำมาพัฒนา และส่วนที่ 5 เป็นการสรุปผลการทดลองของงานวิจัยนี้

2. วิจารณ์วรรณกรรม

2.1 Mobile Ad-hoc Network

ระบบเครือข่ายเฉพาะกิจไร้สาย (MANET) เป็นระบบที่ถูกออกแบบมาเพื่อรองรับการเชื่อมต่อระหว่างโมบายล์โหนดโดยไม่จำเป็นต้องพึ่งพาอุปกรณ์เชื่อมต่อพื้นฐาน เช่น แอคเซสพอยท์ สวิทช์ หรือ เราท์เตอร์ โดยตัวอุปกรณ์ (End-device) สามารถสร้างเครือข่ายขึ้นมาได้เอง และทำการติดต่อกันระหว่างโมบายล์โหนดด้วยกันเอง เพื่อให้ข้อมูลส่งไปถึงปลายทาง โดยที่จุดเด่นของ MANET คือ สามารถจัดการกับอุปกรณ์ต่างๆ ที่มีการเคลื่อนที่อยู่ได้อย่างอิสระ (Node Mobility)

โปรโตคอลการค้นหาเส้นทางของระบบเครือข่ายเฉพาะกิจไร้สาย หากจัดแบ่งตามลักษณะการทำงานของโปรโตคอล [2], [3] จะแบ่งเป็น 2 กลุ่ม ได้แก่ 1) โปรโตคอลค้นหาเส้นทางแบบโปรแอคทีฟ ซึ่งในโปรโตคอลประเภทนี้โมบายล์โหนดทุกๆ ตัวในเครือข่ายจะมีตารางข้อมูลของโมบายล์โหนดต่างๆ (Routing Information) ภายในระบบ และมีการอัพเดทข้อมูลนั้นทุกๆ ช่วงเวลาที่กำหนด 2) โปรโตคอลค้นหาเส้นทางแบบรีแอคทีฟ จะไม่มีการกำหนดเวลาในการอัพเดทข้อมูลภายในช่วงเวลาที่กำหนด แต่จะทำการหาเส้นทางของทั้งระบบเฉพาะเวลาที่จะมีการส่งข้อมูลระหว่างโมบายล์โหนดตั้งแต่ต้นทางจนถึงปลายทาง

2.2 Dynamic Source Routing Protocol (DSR)

DSR [4] เป็นโปรโตคอลในการหาเส้นทางการส่งข้อมูลแบบรีแอคทีฟ โดยเมื่อโมบายล์โหนดต้องการที่จะส่งข้อมูล โมบายล์โหนดต้นทางจะมีการบรอดแคสท์แพ็คเก็ตชนิดพิเศษที่เพิ่ม DSR Header เข้าไปในแพ็คเก็ตแบบปกติ เพื่อทำการเก็บข้อมูลของโมบายล์โหนดต่างๆ ภายในเครือข่าย ซึ่งตัวแพ็คเก็ตที่มี DSR Header จะเก็บข้อมูลไอพีแอดเดรส ของโมบายล์โหนดที่ส่งผ่านเข้าไปในส่วนหัวของแพ็คเก็ต และเมื่อพบโมบายล์โหนดปลายทางแล้วก็จะส่งข้อความตอบกลับมายังต้นทาง จากนั้นก็จะเริ่มทำการสร้างเส้นทางเพื่อทำการส่งแพ็คเก็ตปกติตามเส้นทางที่ได้ทำการบันทึกไว้

โปรโตคอล DSR มีกลไกการทำงานหลักสองกลไก คือ 1) กลไกการค้นหาเส้นทาง (Route Discovery) จะเริ่มต้นทำงานเมื่อโมบายล์โหนดต้องการส่งแพ็คเก็ตไปยังปลายทางแต่ไม่มีข้อมูลเส้นทางที่จะทำการส่งแพ็คเก็ตนั้นๆ ไปยังปลายทาง จึงเริ่มทำการค้นหาเส้นทาง โดยโหนดต้นทางจะทำการบรอดแคสต์แพ็คเก็ตร้องขอเส้นทาง (Route Request: RREQ) ออกไป โดยมีหมายเลข RREQ ID กำหนดไว้และเมื่อโมบายล์โหนดภายในเครือข่ายได้รับก็จะทำการตรวจสอบแพ็คเก็ตว่ามีปลายทางเป็นของตนหรือไม่ หากไม่ใช่ก็จะทำการบรอดแคสต์แพ็คเก็ตนั้นต่อออกไป และหากมีปลายทางเป็นตนเองก็จะทำการส่งแพ็คเก็ตตอบรับ (Route Reply: RREP) กลับมายังโหนดต้นทาง 2) กลไกการปรับปรุงเส้นทาง (Route Maintenance) จะถูกเรียกใช้เมื่อโมบายล์โหนดภายในเครือข่ายทำการส่งข้อมูลอยู่และเส้นทางที่ถูกใช้มีโมบายล์โหนดขาดหายออกไปจากเส้นทาง ทำให้การส่งข้อมูลหยุดชะงักลง โมบายล์โหนดระหว่างทางที่เชื่อมต่อกับโหนดที่หายไปจะทำการส่งแพ็คเกตแจ้งกลับมายังต้นทาง (Route Error: RERR) ว่าเส้นทางที่ใช้อยู่ได้ขาดลงไป และโมบายล์โหนดต้นทางก็จะทำการเรียกใช้เส้นทางอื่นๆ ที่อยู่ภายในแคชของตน หรืออาจเรียกกลไก Route Discovery เพื่อทำการหาเส้นทางใหม่

2.3 Multiple Source Routing Protocol (MSR)

โปรโตคอล MSR [5] พัฒนาขึ้นโดยใช้หลักการของ Dynamic Source Routing Protocol และนำหลักการของการส่งแบบหลายเส้นทางมาประยุกต์ใช้ได้ง่าย เนื่องจากในการทำงานปกติของ DSR เป็นแบบ Source Routing ซึ่งมีกลไกในการหา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เส้นทางก่อนส่งข้อมูลและมีการเก็บข้อมูลเส้นทางที่หามาได้ไว้กับโมบายล์โหนดที่ทำการส่งข้อมูล ทำให้การประมวลผลการส่งแบบหลายเส้นทางมีความเป็นไปได้ที่จะนำมาใช้กับโปรโตคอล DSR

กลไกการค้นหาเส้นทางในโปรโตคอล MSR มีการทำงานเหมือนในโปรโตคอล DSR แต่จะมีการนำข้อมูลเส้นทางที่ได้รับกลับมาจากโหนดปลายทางมาเก็บไว้ในแคชของตน และนำข้อมูลเส้นทางต่างๆ ที่ได้รับออกมาใช้ในการส่งแพ็คเก็ตโดยใช้รูปแบบการส่งแพ็คเก็ตแบบ Round Robin [6] ซึ่งจะมีการวนใช้งานแต่ละเส้นทางไปเรื่อยๆ

3. ขั้นตอนการดำเนินงานวิจัย

จากการศึกษาทบทวนวรรณกรรมในส่วนที่ 2 เกี่ยวกับเครือข่ายเฉพาะกิจเคลื่อนที่, โปรโตคอล DSR และโปรโตคอล MSR ผู้วิจัยได้เล็งเห็นว่าโปรโตคอล DSR ที่มีการใช้เส้นทางเพียงเส้นทางเดียวที่ได้รับจากกระบวนการ Route Discovery นั้นมีโอกาสทำให้เกิดปัญหา Single-point-of-failure ซึ่งมีผลต่อความน่าเชื่อถือของโปรโตคอล โดยชี้วัดได้จากอัตราสำเร็จในการส่งแพ็ตเก็ต นอกจากนี้การเลือกใช้เส้นทางเพียงเส้นทางเดียว ยังมีโอกาสทำให้เกิดความคับคั่งภายในเส้นทางนั้น ในขณะที่ยังมีเส้นทางอื่นที่ได้รับมาสามารถใช้ในการส่งข้อมูลได้อีก ส่งผลให้ใช้เวลานานในการส่งข้อมูลสำเร็จ

ผู้วิจัยจึงทำการนำเสนอแนวคิดการพัฒนาโปรโตคอล MSR ที่มีอยู่เดิมโดยจะปรับปรุงรูปแบบการส่งแพ็คเก็ตเดิมที่ใช้แบบ Round Robin ผู้วิจัยนำเสนอรูปแบบการส่งแพ็คเก็ตแบบ Weight-Round Robin (WRR) แทนการใช้รูปแบบการส่งแบบเดิม เนื่องจากในการส่งแพ็คเก็ตแบบ Round Robin นั้นมีการกระจายโหลดของเส้นทางเท่าๆ กัน จึงมีโอกาสที่เส้นทางที่มีดีเลย์สูงจะถูกเรียกใช้งานเท่ากับเส้นทางที่มีดีเลย์ต่ำ ซึ่งค่าดีเลย์วัดได้จากกการจับเวลาตั้งแต่ส่งแพ็คเก็ต Route Request ออกไปและได้รับ Route Reply กลับมาผ่านเส้นทางนั้นๆ

ผู้วิจัยได้ทำการนำค่าบิทเรทจากดาต้าลิงค์เลเยอร์ ขึ้นมาเป็นตัวแปรในการกำหนดน้ำหนักให้กับเส้นทางบนเน็ตเวิร์คเลเยอร์ ทั้งนี้ ผู้วิจัยคาดว่าค่าบิทเรทดังกล่าวสามารถประเมินคุณภาพของเส้นทางได้โดยประมาณ และมีการใช้จำนวนฮอปของเส้นทางเป็นตัวกำหนดน้ำหนักรองในกรณีที่ค่าบิทเรทของเส้นทางเท่ากันดังที่แสดงให้เห็นจากโค้ดเทียมในภาพที่ 1

```
1  struct route
2  {
3      path
4      bitrate
5      num_hop
6  };
7  new vector srt_vector
8  new vector weight_vector
9  if (srt_vector.size() = 0)
10 {
11     srt_vector.pushback(route);
12 }
13 else
14 {
15     for(int i=0; i<srt_vector.size();i++)
16     {
17         if (srt_vector.at(i).bitrate < route.getBitrate()
18             OR srt_vector.at(i).num_hop < route.num_hop)
19         {
20             srt_vector.insert(srt_vector.at(i-1), route);
21             weight_vector.insert(weight_vector.at(i-1), i);
22         }
23     if(n==srt_vector.size())
24     {
25         srt_vector.pushback(route);
26         weight_vector.pushback(srt_vector.size());
27     }
28 }
29 return srt_vector;
```

ภาพที่ 1: แสดงโค้ดเทียมของกระบวนการหาเส้นทาง

การกำหนดค่าตัวแปรต่างๆ ดังนี้

route = โครงสร้างของเส้นทาง ประกอบไปด้วย

- *path* = เส้นทาง
- *bitrate* = บิทเรทของดาต้าลิงค์เลเยอร์
- *num_hop* = จำนวนฮอป

srt_vector = เวกเตอร์ที่เก็บเส้นทางต่างๆ ไว้

weight_vector = เวกเตอร์ที่เก็บน้ำหนักของเส้นทาง

n = ขนาดของเวกเตอร์

การทำงานของโค้ดข้างต้นจะเริ่มทำงานเมื่อเริ่มกระบวนการค้นหาเส้นทางโดย กำหนดค่าจำนวนเต็ม *n* ให้เท่ากับขนาดของเวกเตอร์เส้นทาง เมื่อเริ่มต้นค้นหาเส้นทางหากพบเส้นทางที่ใช้ได้ก็จะทำการเพิ่ม *route* เข้าไปในเวกเตอร์ และหากพบเส้นทางต่อมาก็จะทำการเปรียบเทียบค่าบิทเรท (*bitrate*) และจำนวนฮอป (*num_hop*) ของเส้นทางภายในเวกเตอร์ โดยจะกำหนดให้เส้นทางที่มีค่าบิทเรทสูงกว่าอยู่ด้านหน้าของเวกเตอร์ และหากมีค่าบิทเรทเท่ากันก็จะทำการเปรียบเทียบจำนวนฮอป โดยให้เส้นทางที่ใช้จำนวนฮอปน้อยกว่าอยู่ด้านหน้า พร้อมกับเพิ่มน้ำหนักให้กับเส้นทางเข้าไปยัง *weight_vector* ที่ตำแหน่งเดียวกับเส้นทางนั้นๆ เมื่อทำงานเสร็จสิ้นก็จะทำการส่งค่า *srt_vector* ที่เก็บเส้นทางต่างๆ ออกไปใช้งานต่อ

ในงานวิจัยนี้ ผู้วิจัยทำการคำนวณน้ำหนักของเส้นทางโดยกำหนดน้ำหนักสูงสุดตามจำนวนเส้นทางที่สามารถใช้ได้ ลดลง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มาจนถึงเส้นทางที่มีน้ำหนักต่ำสุดคือ 1 และมีการกระจายโหลดโดยใช้การกระจายตามแต่ละแพ็คเก็ต โดยจะส่งแพ็คเก็ตออกไปยังเส้นทางที่มีน้ำหนักสูงสุดเป็นจำนวนตามค่าน้ำหนักของเส้นทางนั้นๆ จากนั้นจึงส่งแพ็คเก็ตออกไปยังเส้นทางถัดไปตามค่าน้ำหนักของเส้นทางเช่นกัน

ผู้วิจัยเล็งเห็นว่าการส่งแพ็คเก็ตแบบ WRR สามารถแก้ปัญหาดังกล่าวได้โดยใช้ค่าดีเลย์ของเส้นทางเป็นตัวกำหนดอัตราการถ่วงน้ำหนักของการส่งแพ็คเก็ตทำให้สามารถแบ่งโหลดของการส่งแพ็คเก็ตไปยังเส้นทางที่มีดีเลย์น้อยกว่าได้ดี ทั้งนี้เพื่อลดเวลาการทำงานโดยรวมของระบบตั้งแต่เริ่มส่งแพ็คเก็ตจนกระทั่งส่งแพ็คเก็ตทั้งหมดสำเร็จโดยจะมีการนำเสนอผลของการทดลองในส่วนถัดไป

4. ผลการทดลอง

จากการนำเสนอการปรับปรุงโปรโตคอลในส่วนที่ 3 ผู้วิจัยได้ทำการทดลองโดยใช้โปรแกรมจำลองระบบเครือข่าย และนำผลการจำลองเครือข่ายมาเปรียบเทียบกับอัลกอริทึม DSR และ MSR โดยมีข้อกำหนดควบคุม และผลการทดลองดังนี้

4.1 การควบคุมข้อกำหนดระบบเครือข่ายของแต่ละโปรโตคอล

การทดลองมีการกำหนดการควบคุมโดยมีการกำหนดให้โมบายล์โหนดมีการเคลื่อนที่อยู่เสมอด้วยความเร็วคงที่ โดยที่ความเร็วของแต่ละโหนดมีการสุ่มแบบยูนิฟอร์ม มีกระจายตัวของโหนดแบบสุ่มภายในพื้นที่กว้าง 1500 เมตร ยาว 1000 เมตร กำหนดให้โหนดต้นทางส่งข้อมูลไปยังโหนดปลายทางด้วยโปรโตคอล UDP และให้ระบบหยุดทำงานเมื่อโหนดปลายทางได้รับข้อมูลจำนวน 1000 แพ็คเก็ต โดยมีการแสดงข้อมูลจำเพาะอื่นๆ ภายในตารางที่1 ต่อจากนี้

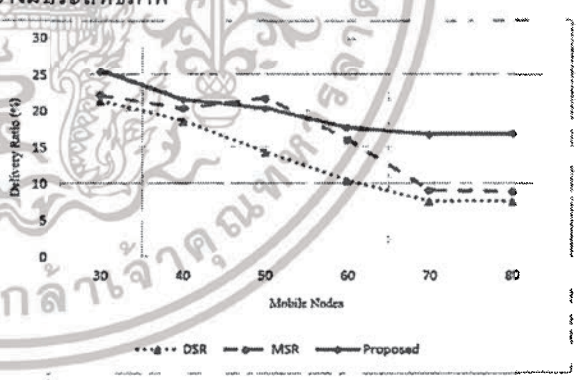
ตารางที่ 1: แสดงข้อมูลจำเพาะของการจำลองการทำงาน

พื้นที่จำลอง	1500 เมตร × 1000 เมตร
รัศมีการทำงานของโหนด	250 เมตร
จำนวนแพ็คเก็ตที่ปลายทางได้รับ	1000 แพ็คเก็ต
จำนวนโหนดในเครือข่าย	30, 40, 50, 60, 70, 80
อัตราการส่งแพ็ตเก็ต	4 แพ็คเก็ต/วินาที
โปรโตคอลที่ใช้ส่งข้อมูล	UDP
ความเร็วในการเคลื่อนที่เฉลี่ย	2.5, 5, 7.5, 10 เมตร/วินาที
จำนวนรอบที่ใช้ในการทดลอง (ต่อหนึ่งรูปแบบจำลอง)	40 รอบ

4.2 ตัวชี้วัดและผลการทดลอง

จากการควบคุมข้อกำหนดต่างๆ ในส่วนที่ 4.1 และทำการทดลองจำลองการทำงานของอัลกอริทึมการค้นหาเส้นทางของโปรโตคอล DSR โปรโตคอล MSR และอัลกอริทึมที่ผู้วิจัยนำเสนอ ผู้วิจัยได้เสนอผลการจำลองระบบออกมาในรูปแบบกราฟโดยมีตัวชี้วัดต่างๆ ที่ใช้ในการเปรียบเทียบผลการทำงาน คือ ผลสำเร็จของการส่งแพ็คเก็ต และเวลาการทำงานตั้งแต่เริ่มส่งแพ็ตเก็ตจนโมบายล์โหนดปลายทางได้รับแพ็คเก็ตเป็นจำนวน 1,000 แพ็คเก็ต

การทดลองควบคุมการทำงานโดยกำหนดความเร็วในการเคลื่อนที่เฉลี่ยเป็น 7.5 และ 10 เมตร/วินาที พบว่าอัตราสำเร็จในการส่งแพ็คเก็ตของระบบที่มีจำนวนโมบายล์โหนดที่เพิ่มขึ้นจะส่งผลให้อัตราสำเร็จในการส่งแพ็ตเก็ตลดลง โดยในอัลกอริทึมของ MSR และอัลกอริทึมที่ผู้วิจัยนำเสนอ สามารถทำงานได้ดีกว่าอัลกอริทึมการค้นหาเส้นทางของ DSR ตามภาพที่ 1 และภาพที่ 2 ซึ่งจะเห็นได้ว่าเมื่อมีจำนวนโมบายล์โหนดเยอะ อัลกอริทึมที่นักวิจัยได้นำเสนอจะสามารถทำงานได้ดีกว่าอัลกอริทึม MSR และ DSR ที่ยังมีค่าใกล้เคียงกัน ทั้งนี้เนื่องจากกลไกการกระจายโหลดที่ทำให้สามารถใช้งานเส้นทางที่มีอยู่ได้อย่างมีประสิทธิภาพ

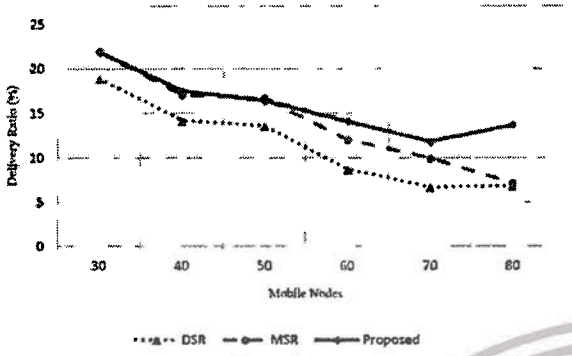


ภาพที่ 1: แสดงผลการทดลองอัตราสำเร็จต่อจำนวนโมบายล์โหนดที่ความเร็ว 7.5 เมตร/วินาที

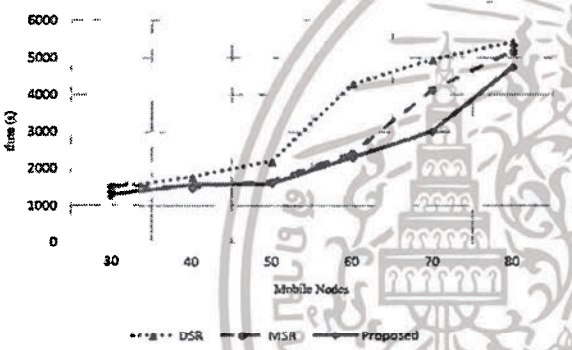
ในการทดลองเพื่อหาเวลาการทำงานด้วยการกำหนดความเร็วในการเคลื่อนที่เฉลี่ยเป็น 7.5 และ 10 เมตร/วินาที ตามภาพที่ 3 และภาพที่ 4 แสดงให้เห็นว่าที่จำนวนโหนดตั้งแต่ 30 – 50 โหนด แต่ละอัลกอริทึมจะใช้เวลาในการทำงานใกล้เคียงกัน แต่เมื่อจำนวนโหนดเพิ่มขึ้น อัลกอริทึมที่นักวิจัยนำเสนอมาสามารถทำงานได้ดีกว่าโปรโตคอล MSR และ DSR อย่างเห็นได้ชัด ทั้งนี้เพราะว่ามีการกำหนดน้ำหนักให้กับเส้นทาง ทำให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

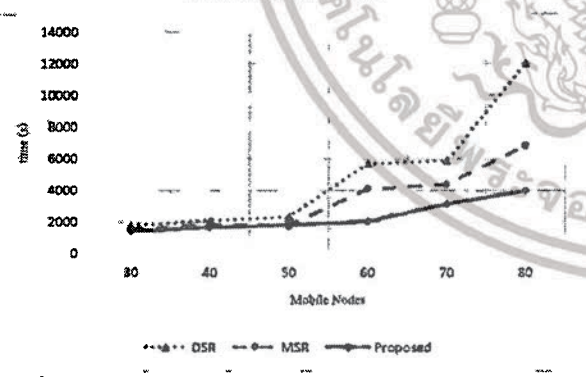
สามารถกระจายโหลดออกไปยังเส้นทางที่มีบิทเรทสูงกว่า สามารถระบายการไหลของแพ็ตเก็ตได้และไม่เกิดความคับคั่งภายในเส้นทางที่มีบิทเรทต่ำ



ภาพที่ 2: แสดงผลการทดลองอัตราสำเร็จต่อจำนวนโมบายล์โหนดที่ความเร็ว 10 เมตร/วินาที

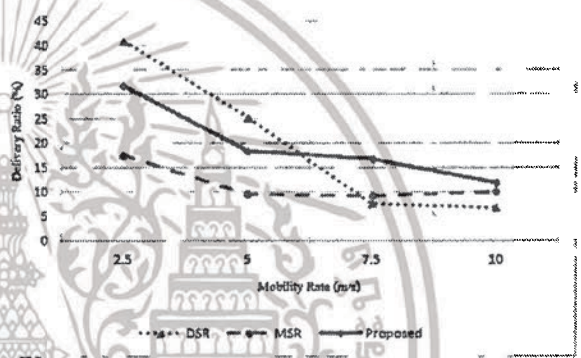


ภาพที่ 3: แสดงผลการทดลองเวลาการทำงานต่อจำนวนโมบายล์โหนดที่ความเร็ว 7.5 เมตร/วินาที

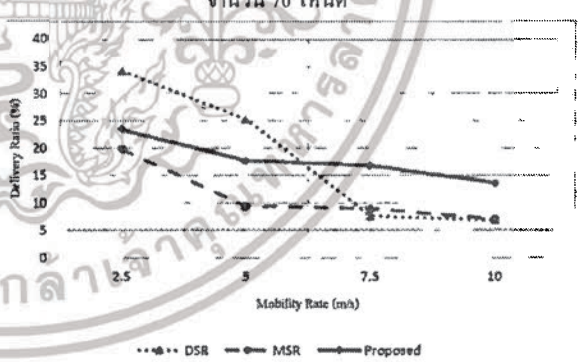


ภาพที่ 4: แสดงผลการทดลองเวลาการทำงานต่อจำนวนโมบายล์โหนดที่ความเร็ว 10 เมตร/วินาที

ภาพที่ 5 และภาพที่ 6 แสดงการเปรียบเทียบการทำงานที่มีจำนวนโมบายล์โหนดภายในเครือข่ายสูง เช่น 70 และ 80 โหนด ระหว่างความเร็วเฉลี่ยในการเคลื่อนที่ของโมบายล์โหนด ต่ออัตราสำเร็จในการส่งแพ็ตเก็ตของโหนด จะเห็นได้ว่าเมื่อโหนดมีการเคลื่อนที่ด้วยความเร็วต่ำ ประสิทธิภาพการทำงานของอัลกอริทึม DSR จะทำงานได้ดีกว่าอัลกอริทึม MSR และอัลกอริทึมที่นักวิจัยนำเสนอ แต่เมื่อโมบายล์โหนดเคลื่อนที่ด้วยความเร็วสูงขึ้น อัตราสำเร็จในการส่งแพ็คเก็ตของ DSR จะลดลงอย่างมาก ในขณะที่อัลกอริทึมของผู้วิจัยมีการลดลงค่อนข้างน้อย ทำให้สามารถทำงานได้ดีกว่าอัลกอริทึม DSR และ MSR ที่ความเร็ว 7.5 และ 10 เมตร/วินาที ทั้งนี้เป็นผลมาจากการเคลื่อนที่ของโมบายล์ด้วยความเร็วสูง ทำให้มีโอกาสสูงที่เส้นทางแพ็คเก็ตจะถูกตัดขาด ทำให้การแพ็คเก็ตในเครือข่ายที่ใช้อัลกอริทึม DSR หยุดชะงักลง ในขณะที่ MSR และอัลกอริทึมที่นำเสนอยังสามารถส่งแพ็คเก็ตได้อยู่เนื่องจากมีการใช้เส้นทางการส่งแพ็คเก็ตหลายเส้นทาง



ภาพที่ 5: แสดงผลการทดลองอัตราสำเร็จต่อความเร็วเฉลี่ยสำหรับโหนดจำนวน 70 โหนด

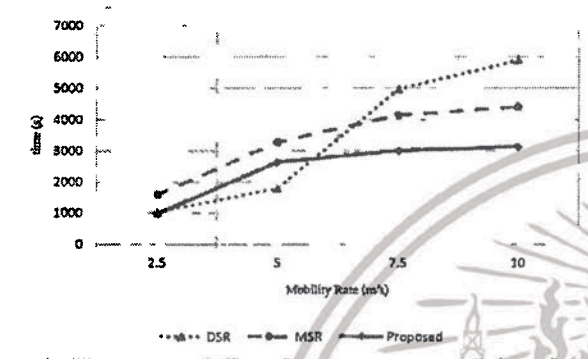


ภาพที่ 6: แสดงผลการทดลองอัตราสำเร็จต่อความเร็วเฉลี่ยสำหรับโหนดจำนวน 80 โหนด

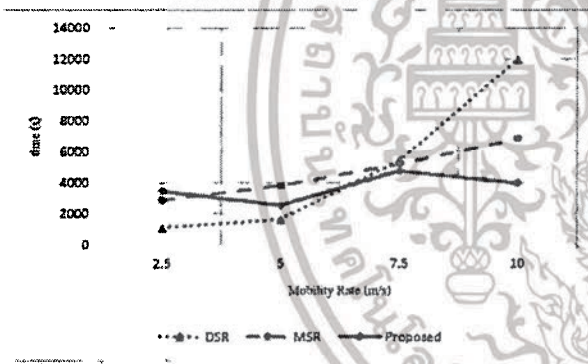
ภาพที่ 7 และภาพที่ 8 เป็นการเปรียบเทียบเวลาการทำงานต่อความเร็วในการเคลื่อนที่ของโมบายล์โหนด ของเครือข่ายที่มีโมบายล์โหนดจำนวน 70 และ 80 โหนดตามลำดับ อัลกอริทึมของ DSR สามารถทำงานได้ดีกว่าในความเร็ว 2.5 และ 5 เมตร/วินาที แต่เมื่อความเร็วเพิ่มขึ้นเป็น 7.5 และ 10 เมตร/วินาที อัลกอริทึม DSR จะใช้เวลาทำงานเพิ่มขึ้นอย่างมาก ส่วนอัลกอริทึม MSR และอัลกอริทึมที่นำเสนอมีการใช้เวลา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพิ่มขึ้นน้อยกว่าอัลกอริทึม DSR เป็นผลมาจากการที่เส้นทางที่ส่งแพ็คเก็ตอยู่ถูกตัดขาด ทำให้อัลกอริทึม DSR ที่ทำงานโดยการส่งแพ็คเก็ตเส้นทางเดียว ต้องเริ่มกระบวนการค้นหาเส้นทางใหม่ จึงใช้เวลาเพิ่มขึ้นเป็นอย่างมาก ในขณะที่อัลกอริทึม MSR และอัลกอริทึมที่นำเสนอยังมีเส้นทางอื่นๆ ที่สามารถใช้ได้มารองรับการส่งแพ็คเก็ตไปยังโมบายล์โหนดปลายทาง



ภาพที่ 7: แสดงผลการทดลองเวลาการทำงานต่อความเร็วเฉลี่ยของโมบายล์โหนดจำนวน 70 โหนด



ภาพที่ 8: แสดงผลการทดลองเวลาการทำงานต่อความเร็วเฉลี่ยของโมบายล์โหนดจำนวน 80 โหนด

5. สรุปผลการทำงานของระบบ

นักวิจัยได้นำเสนอการพัฒนาอัลกอริทึมในการค้นหาเส้นทางของเครือข่ายเฉพาะกิจเคลื่อนที่ โดยมีโปรโตคอล DSR เป็นหลัก และนำโปรโตคอล MSR ที่พัฒนาต่อมาจาก DSR มาเป็นพื้นฐานในการพัฒนาอัลกอริทึม ซึ่งได้ทำการเพิ่มอัลกอริทึมการค้นหาเส้นทางโดยใช้ค่าบิทเรทจากดาต้าลิงค์เลเยอร์ และจำนวนฮอปของเส้นทางมาเป็นตัวกำหนดน้ำหนักให้กับเส้นทาง

จากผลการทดลองในส่วนที่ 4 สามารถบอกได้ว่าอัลกอริทึมที่นักวิจัยนำเสนอนั้น สามารถทำงานได้ดีกว่าอัลกอริทึม DSR และ MSR ในสถานการณ์ที่มีจำนวนโมบายล์โหนดสูง หรือมีการเคลื่อนที่ด้วยความเร็วมาก เป็นผลมาจากการเพิ่มอัลกอริทึมค้นหาเส้นทางให้มีการกำหนดน้ำหนักให้กับเส้นทาง ทำให้ไม่เกิดความคับคั่งในเส้นทางใดเส้นทางหนึ่ง และสามารถดึงประสิทธิภาพของโมบายล์โหนดออกมาใช้งานได้อย่างเต็มที่

เอกสารอ้างอิง

[1] T. S. Rappaport. **"Wireless Communications Principles & Practice."** Upper Saddle River, New Jersey: Prentice-Hall, Inc.1996

[2] T. Lin. **"Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications."** Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the Ph.D. in Computer Engineering. 2004

[3] K.Gorantala. **"Routing Protocols in Mobile Ad-hoc Networks"** Master's Thesis in Computing Science at Ume°a University. June 15, 2006

[4] D. B. Johnson and D. A. Maltz, **"Dynamic Source Routing in Ad Hoc Wireless Networks."** Computer Science Department, Carnegie Mellon University. 1996

[5] L. Wang, Y. Shu, M. Dong and L. Zhang, **"Adaptive Multipath Source Routing in Ad Hoc Networks."** Department of Computer Science, Tianjin University, Tianjin, China

[6] S. Prabhavat, H. Nishiyama, N. Ansari and N. Kato **"On Load Distribution over Multipath Networks."** *IEEE Communications Survey & Tutorials*, vol. 14, no. 3, pp. 662-680, 2012.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การศึกษาความเป็นไปได้ในการลดโอเวอร์เฮดบนระบบเครือข่ายไร้สายเฉพาะกิจ โดยการสร้างเงื่อนไขในการจำกัดการกระจายของข้อมูล ในขั้นตอนการค้นหาเส้นทาง

ธนานพ ทองถาวร วรวัชร ณรงคะชวนะ และ สุเมธ ประภาวัต

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: St_freedom2@hotmail.com, worravat@gamil.com, sumet@it.kmitl.ac.th

บทคัดย่อ

ในปัจจุบันระบบเครือข่ายไร้สายเฉพาะกิจ(Mobile Ad-hoc network) ได้มีการศึกษาอย่างแพร่หลาย โดยมีจุดประสงค์ที่จะผลักดันแนวคิดการทำงานของระบบเน็ตเวิร์คเฉพาะกิจให้สามารถนำมาใช้งานได้ในเชิงปฏิบัติ เพื่อที่จะให้บรรลุวัตถุประสงค์ดังกล่าว นักวิจัยจำเป็นต้องแก้ไขปัญหาหลักสองข้อซึ่งมีผลต่อประสิทธิภาพในการทำงานของระบบอย่างมาก ได้แก่ โอเวอร์เฮด หรือแพ็คเกตที่ไม่มีประโยชน์ต่อการสื่อสารระหว่างโหนดบนระบบเน็ตเวิร์ค และ ปัญหาเรื่องข้อจำกัดของพลังงานในระบบ ในบทความฉบับนี้ได้นำเสนอวิธีการจำกัดการกระจายของข้อมูลในระบบเน็ตเวิร์คเฉพาะกิจเพื่อลดจำนวนโอเวอร์เฮดในระบบ จากการศึกษาพบว่าแนวคิดที่นำเสนอขึ้นใหม่นั้น สามารถลดจำนวนโอเวอร์เฮดลง ในขณะที่ยังคงรักษาอัตราความสำเร็จในการสร้างช่องทางการติดต่อสื่อสารกันระหว่างโหนดได้

คำสำคัญ— เครือข่ายไร้สายเฉพาะกิจ; โอเวอร์เฮด; จำกัดการกระจายข้อมูล

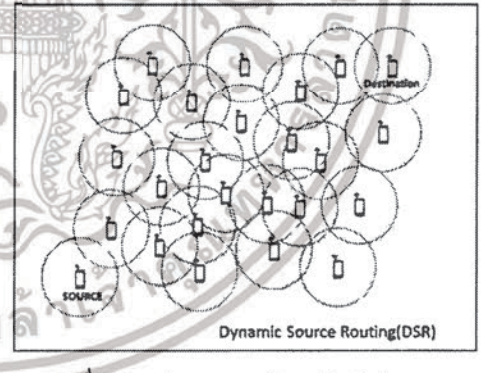
1. บทนำ

ระบบเครือข่ายไร้สายเฉพาะกิจ(Mobile Ad-hoc network) เป็นระบบเครือข่ายแบบไม่มีโครงสร้างโดยอาศัยสมาชิกในระบบเครือข่ายหรือโหนดเป็นสื่อกลางในการติดต่อสื่อสาร ซึ่งการใช้เครือข่ายไร้สายเฉพาะกิจนั้นจะมีประโยชน์มากเมื่อระบบเครือข่ายปกติไม่สามารถใช้งานได้ ยกตัวอย่างเช่น เมื่อเกิดเหตุภัยพิบัติทางธรรมชาติเป็นต้น โดยกระบวนการติดต่อสื่อสารภายในระบบเครือข่ายไร้สายเฉพาะกิจจำเป็นต้องมีโปรโตคอล[1] ที่ใช้ในการควบคุมการทำงานของระบบโดยเฉพาะ โดยใช้แนวคิดพื้นฐานจากสถาปัตยกรรมแบบเพียร์ทูเพียร์ [2] ในการกระจายแพ็คเกตออกไปรอบตัวเพื่อค้นหาและสร้างเส้นทางการติดต่อสื่อสารระหว่างโหนดปลายทาง ในขั้นตอนดังกล่าวจะมีแพ็คเกตอีกจำนวนหนึ่งที่ส่งไปไม่ถึงปลายทางหรือเรียกว่าโอเวอร์เฮด แพ็คเกตเหล่านี้จะส่งผลให้เกิดความแออัดให้แก่ระบบเน็ตเวิร์คเป็นอย่างมาก ซึ่งทำให้ระบบเน็ตเวิร์คประสบกับปัญหา NETWORK COLLISION[3] ที่ส่งผลเสียโดยตรงต่ออัตราความสำเร็จในการสร้างเส้นทางการติดต่อสื่อสารในระบบ

ในบทที่สองจะกล่าวถึงโปรโตคอลต่างๆที่ใช้ในการควบคุมการกระจายแพ็คเกตในระบบเครือข่ายไร้สายเฉพาะกิจ บทที่สามจะกล่าวถึงแนวคิดในการออกแบบโปรโตคอลใหม่ที่มีวัตถุประสงค์ในการลดโอเวอร์เฮดโดยที่ไม่ส่งผลกระทบต่อค่าความสำเร็จในการสร้างเส้นทางการติดต่อสื่อสาร และทำการทดสอบโปรโตคอลด้วยระบบซิมูเลชั่นในบทที่ 4 และสรุปผลการทดลองในบทที่ 5

2. ทฤษฎีและงานที่เกี่ยวข้อง

2.1. Dynamic Source Routing (DSR)



รูปที่ 1. Dynamic source routing protocol scheme

Dynamic Source Routing หรือ DSR [4] เป็นโปรโตคอลพื้นฐานที่ใช้ในการสื่อสารกันระหว่างโหนดในระบบเครือข่ายไร้สายเฉพาะกิจ โดยกระบวนการติดต่อสื่อสารนั้นจะเกิดขึ้นเมื่อโหนดต้นทางต้องการส่งข้อมูลไปยังโหนดปลายทาง โหนดต้นทางจะเริ่มขบวนการค้นหาเส้นทาง(Route discovery) โดยการกระจายแพ็คเกต Route request (RREQ) ออกไป ในกรณีที่โหนดที่ได้รับแพ็คเกต RREQ ไม่ใช่โหนดปลายทางก็จะทำการกระจายแพ็คเกตนั้นต่อไปและเพิ่มตำแหน่งของตัวเองลงไปบนเฮดเดอร์ของแพ็คเกตนั้น เมื่อแพ็คเกตถูกส่งไปจนถึงปลายทาง โหนดปลายทางจะใช้ตำแหน่งของโหนดที่ถูกบันทึกเอาไว้บนเฮดเดอร์มาใช้ในการสร้างเส้นทางการเชื่อมต่อสื่อสารกับโหนดต้นทาง

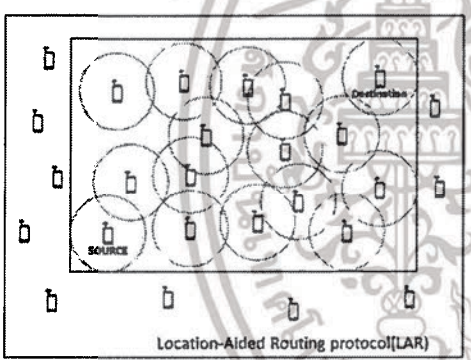
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยการส่งแพ็คเกต Route reply ที่บันทึกข้อมูลเส้นทางที่สามารถส่งข้อมูลมายังโหนดปลายทางได้กลับไปที่โหนดต้นทาง

เนื่องจากโหนดในระบบเครือข่ายไร้สายเฉพาะกิจมีการเคลื่อนที่ตลอดเวลา จึงมีความเป็นไปได้มากที่เส้นทางที่ถูกสร้างไว้ในขั้นตอน Route Discovery จะไม่สามารถใช้งานได้เมื่อระยะเวลาผ่านไป เมื่อโหนดใดๆไม่สามารถส่งข้อมูลตามเส้นทางที่กำหนดไว้โดยโหนดต้นทาง โหนดนั้นๆจะส่ง Route error message กลับมาที่โหนดต้นทาง จากนั้นโหนดต้นทางจะเริ่มกระบวนการ Route maintenance โดยการเลือกใช้เส้นทางอื่นที่ถูกเก็บอยู่ใน catch ของโหนดต้นทาง หรือเริ่มกระบวนการ Route discovery ใหม่อีกครั้ง

การจำกัดการกระจายแพ็คเกตบนโปรโตคอล DSR จะใช้ Route cache เข้ามาช่วยลดโอเวอร์เฮดในระบบ เมื่อโหนดปลายทางส่ง Route reply message กลับมายังโหนดต้นทาง โหนดที่อยู่ระหว่างทางจะทำการสำรองเส้นทางเอาไว้ใน Route cache เมื่อโหนดได้รับ RREQ แพ็คเกต ก็จะทำการตรวจสอบใน route cache ว่ามีเส้นทางที่จะสามารถส่งข้อมูลไปยังปลายทางที่ระบุไว้บน RREQ หรือไม่ ถ้ามีก็จะทำการส่ง Route reply กลับไปยังโหนดต้นทางทันที

2.2. Location-Aided Routing Protocol (LAR)



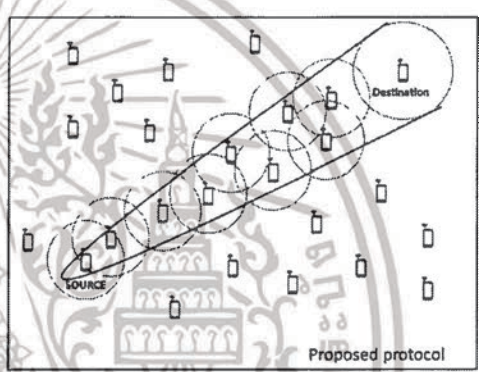
รูปที่ 2. Location-Aided routing protocol scheme

Location-Aided Routing protocol หรือ LAR [5] เป็นโปรโตคอลที่มีการพัฒนาต่อยอดมาจาก DSR โดยการใช้ระบบพิกัด GPS [6] เข้ามาช่วยในการคาดเดาตำแหน่งของปลายทาง ทำให้สามารถสร้างเงื่อนไขในการจำกัดการกระจายของข้อมูลได้ ในกระบวนการทำงานของโปรโตคอล LAR จำเป็นต้องรู้พิกัด GPS ของโหนดปลายทาง และความเร็วเฉลี่ยของโหนดปลายทางเพื่อที่จะคำนวณความเป็นไปได้ที่โหนดปลายทางจะเคลื่อนที่จากจุดเดิมเป็นระยะเท่าไหร่ หรือเรียกว่า expected zone จากนั้นจึงสร้างเงื่อนไขในการกระจายของข้อมูลให้อยู่ในพื้นที่ที่กำหนด ซึ่งจะถูกเรียกว่า forwarding zone จากรูปที่ 2 จะสังเกตได้ว่า expected zone คือพื้นที่วงกลมที่ล้อมรอบโหนดปลายทาง และ forwarding zone คือกรอบสี่เหลี่ยมที่มีโหนดต้นทางอยู่ที่ปลายของเส้นทแยงมุมที่ทำกับโหนดปลายทาง จากนั้นโปรโตคอล LAR จะเริ่มขั้นตอนการทำ Route Discovery เช่นเดียวกับโปรโตคอล DSR เพื่อค้นหาเส้นทางในการติดต่อสื่อสารต่อไป โดยที่โปรโตคอล LAR ยังคงมีการใช้ Route Cache เช่นเดียวกัน

3. แนวคิดการออกแบบโปรโตคอล

จากการศึกษาลักษณะการทำงานบนโปรโตคอล DSR และ LAR แล้ว ผู้วิจัยเล็งเห็นถึงประโยชน์ของการจำกัดการกระจายข้อมูลในขั้นตอน Route discovery ว่าสามารถช่วยลดปัญหาการเกิดโอเวอร์เฮดได้ แต่เนื่องจากเงื่อนไขการจำกัดการกระจายข้อมูลยังไม่รัดกุมมากพอ จึงทำให้มีแนวคิดในการเพิ่มประสิทธิภาพในการทำงานของโปรโตคอลให้สามารถช่วยลดโอเวอร์เฮดได้มากยิ่งขึ้น

การนำพิกัด GPS เข้ามาช่วยในการติดต่อสื่อสารในระบบเครือข่ายเฉพาะกิจ ทำให้โหนดต้นทางสามารถกำหนดทิศทางการกระจายข้อมูลไปยังโหนดปลายทางในขั้นตอน Route discovery ได้ ดังนั้นผู้วิจัยจึงได้มีแนวคิดในการปรับเปลี่ยนเงื่อนไขในขั้นตอน Route discovery รูปภาพที่ 3 แสดงถึงรูปแบบการจำกัดพื้นที่ของโปรโตคอลใหม่



รูปที่ 3. Proposed protocol scheme

ขั้นตอนการทำงานของโปรโตคอลใหม่นั้นโหนดต้นทางจะต้องทราบถึงพิกัด GPS และความเร็วเฉลี่ยของโหนดปลายทางก่อน โดยจะนำข้อมูลดังกล่าวบรรจุลงไปใน RREQ message เพื่อใช้ในการกำหนดบทบาทให้กับโหนดทุกโหนดในระบบเน็ตเวิร์ค ซึ่งในขั้นแรกจะต้องคำนวณพื้นที่ของ expected zone ก่อน ซึ่งสามารถหาได้จากสมการที่ 1

$$expected\ zone = V_{avg}(t_1 - t_0) \qquad (1)$$

โดยกำหนดให้ V_{avg} คือความเร็วเฉลี่ยของโหนดในระบบเครือข่าย และ $t_1 - t_0$ คือระยะเวลาที่โหนดปลายทางใช้ในการเปลี่ยนตำแหน่ง หลังจากคำนวณ expected zone แล้ว จะนำรัศมีของ *expected zone* มาใช้ในการกำหนดบทบาทให้กับโหนดที่จะทำหน้าที่เป็นตัวกลางในการกระจายข้อมูลหรือเรียกว่า forwarding node ร่วมกับสมการที่ 2 และตรวจสอบว่า forwarding node ใดที่อยู่ในรัศมีของ expected zone จากสมการที่ 3

$$f(x,y) = \left(\frac{y_d}{(x_d+\mathrm{r})^2}\right)x^2 - y$$

เมื่อ (2)

$$f(x,y) \neq 0$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$g(x,y) = (x - x_d^2) + (y - y_d^2) - r^2$$

เมื่อ (3)

$$g(x,y) \neq 0$$

โดยกำหนดให้ x_d, y_d เป็นพิกัดของโหนดปลายทาง x, y เป็นพิกัดของโหนดใดๆบนเน็ตเวิร์ค และ r เป็นรัศมีของ expected zone โดยก่อนการคำนวณ ต้องทำการหมุนและย้ายแกน X และ แกน Y ของโหนดต้นทางให้ตั้งฉากกับโหนดปลายทางก่อน จากนั้นโหนดต้นทางจะเริ่มกระบวนการ Route discovery ซึ่งโหนดทุกตัวในระบบเครือข่ายจะทำการตรวจสอบว่าตัวเองนั้นเป็น Forwarding node หรือไม่ ถ้าใช่จะทำการกระจายข้อมูลต่อ แต่ถ้าไม่ใช่ก็จะทำการดร็อปแพ็คเกตทิ้งไป จนกว่าแพ็คเกตจะไปถึงโหนดปลายทาง จากนั้นโหนดปลายทางจะส่งแพ็คเกต *Route reply* ที่บันทึกข้อมูลของ *forwarding node* ทั้งหมดที่จำเป็นต้องใช้ในการติดต่อตามลำดับกลับมาที่โหนดต้นทางเพื่อสร้างช่องทางการติดต่อสื่อสารกันต่อไป

4. การทดสอบและวิเคราะห์ผล

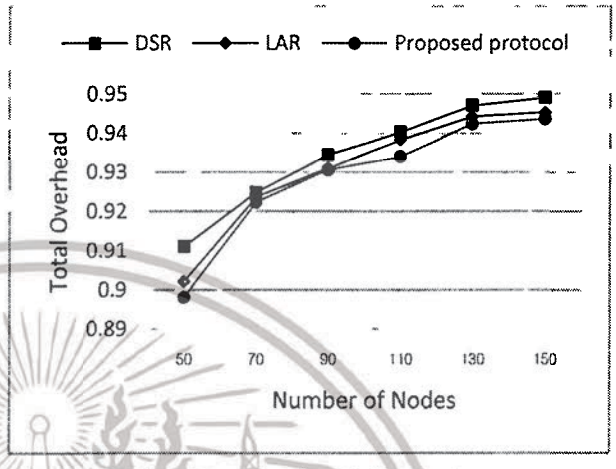
จากที่ได้กล่าวไว้ในบทที่ 3 ผู้วิจัยได้ทำการทดสอบโปรโตคอลที่นำเสนอด้วยโปรแกรมซิมูเลชั่นระบบเครือข่าย OMNET++ โดยเปรียบเทียบผลลัพธ์การทำงานร่วมกับโปรโตคอล DSR และ LAR โดยมีการใช้พารามิเตอร์ในการทดสอบดังตารางที่ 1

ตารางที่ 1 พารามิเตอร์ที่ใช้ในการจำลองเหตุการณ์

พารามิเตอร์	ค่าพารามิเตอร์
ระยะเวลาในการจำลองเหตุการณ์	1000 วินาที
ขอบเขตการกระจายข้อมูลของโหนด	250 เมตร
ความกว้างของพื้นที่ทดสอบ	1000 ตารางเมตร
ระยะเวลาที่ใช้ในการเปลี่ยนองศาการเคลื่อนที่ของโหนด	ใช้การสุ่มแบบ uniform ในช่วง 0-5 วินาที
ขนาดของมุมเมื่อมีการเปลี่ยนองศาการเคลื่อนที่	ใช้การสุ่มแบบ uniform ในช่วง 0-360 องศา
ความเร็วของโหนด	ใช้การสุ่มแบบ uniform ในช่วง 0-20 เมตรต่อวินาที
จำนวนโหนดต้นทาง	10 โหนด
อัตราการส่งข้อมูล	ใช้การสุ่มแบบ uniform ในช่วง 1-5 แพ็คเกตต่อวินาที
ขนาดของแพ็คเกต	64 byte

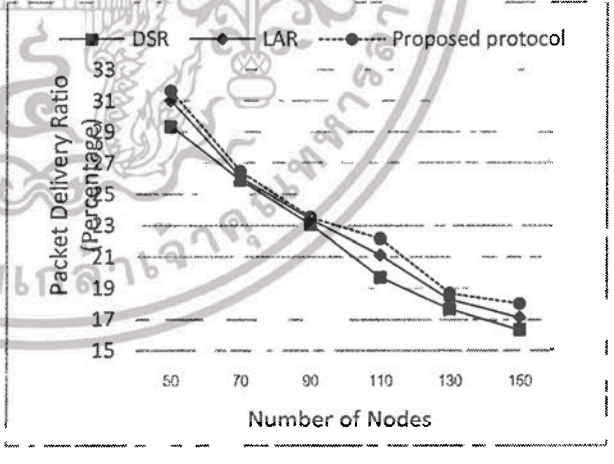
โดยสาเหตุที่ใช้จำนวนโหนดต้นทางมากกว่า 1 โหนดนั้นเนื่องจากผู้วิจัยต้องการให้เกิดการเรียกใช้งานฟังก์ชั่น route cache บนโปรโตคอลที่ใช้ในการทดสอบทั้งสามตัว เนื่องจากโปรโตคอล DSR ไม่มีกลไกอื่นที่สามารถช่วยลดโอเวอร์เฮดได้นอกจากการใช้งานแคชเพียงอย่างเดียว

ในการสรุปผลการทดลองจะใช้ตัวชี้วัดทั้งหมด 4 ประเภทคือ ปริมาณโอเวอร์เฮดในระบบเครือข่าย อัตราความสำเร็จในการส่งข้อมูล ระยะเวลาที่ใช้ในการสร้างเส้นทาง และความล่าช้าในการส่งข้อมูลระหว่างโหนด โดยแสดงผลด้วยกราฟดังต่อไปนี้



รูปที่ 4. กราฟแสดงปริมาณโอเวอร์เฮดในระบบเครือข่าย

จากกราฟจะเห็นได้ว่าโปรโตคอลที่นำเสนอสามารถลดจำนวนโอเวอร์เฮดได้เมื่อเปรียบเทียบกับโปรโตคอล DSR และ LAR เนื่องจากการเปลี่ยนเงื่อนไขในการกระจายข้อมูลให้มีความรัดกุมมากยิ่งขึ้นโดยค่าโอเวเวอร์เฮดนั้นเป็นสัดส่วนระหว่างจำนวนแพ็คเกตที่ใช้ในการค้นหาเส้นทางต่อจำนวนแพ็คเกตทั้งหมดที่เกิดขึ้นในระบบเครือข่าย

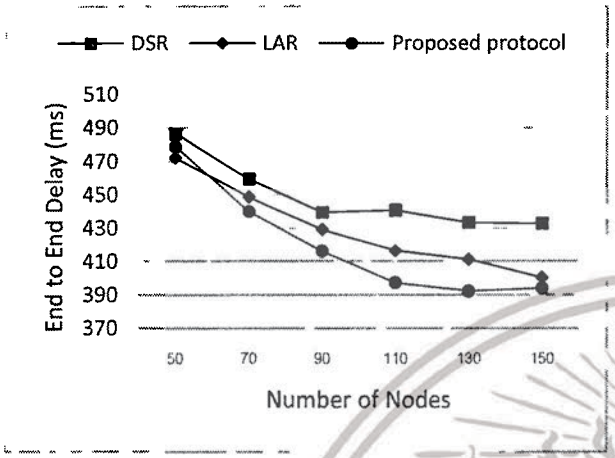


รูปที่ 5. กราฟแสดงอัตราความสำเร็จในการส่งข้อมูล

วิธีการจำกัดพื้นที่ในการกระจายข้อมูลเพื่อลดโอเวอร์เฮดที่นำเสนอนั้นมีจุดประสงค์เพื่อลดจำนวน forwarding node ลง การกำหนดเงื่อนไขเพื่อควบคุมจำนวน forwarding node ให้เหมาะสม จะส่งผลกระทบต่ออัตราความสำเร็จในการส่งข้อมูล จากรูปที่ 5 แสดงให้เห็นว่าโปรโตคอลที่นำเสนอนั้นสามารถช่วยลดโอเวอร์ได้ ในขณะเดียวกันยังช่วยเพิ่มอัตราความสำเร็จในการส่งข้อมูลอีกด้วย ในกรณีของโปรโตคอล LAR และ DSR ที่ทีอัตราความสำเร็จในการส่งข้อมูลน้อยกว่าเนื่องจากโอ

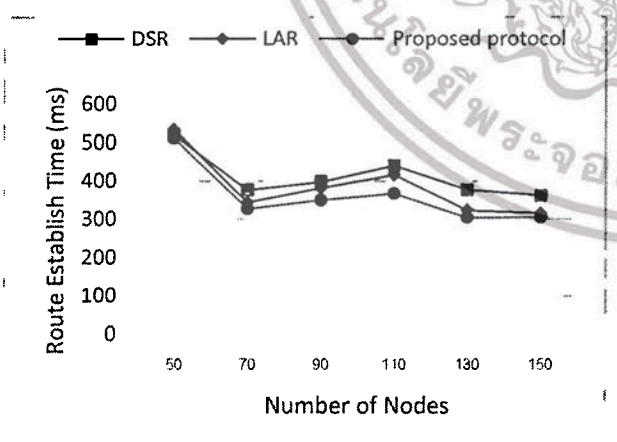
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เวอร์เฮดที่เกิดจากขั้นตอน route discovery ส่งผลกระทบต่อระบบเครือข่ายทำให้เกิดความแออัดในระบบเน็ตเวิร์คจนกระทั่งเกิดการชนกันของข้อมูล ซึ่งเป็นการขัดขวางการส่งข้อมูลจากต้นทางไปยังปลายทาง



รูปที่ 6. กราฟแสดงความล่าช้าในการส่งข้อมูลระหว่างโหนด

ค่าความล่าช้าในการส่งข้อมูลระหว่างโหนดนั้นแปรผันตรงกับความคับคั่งในระบบเน็ตเวิร์ค ในกรณีของโปรโตคอลที่นำเสนอนั้นสามารถลดปริมาณ forwarding node ในระบบเครือข่ายลง ซึ่งช่วยลดปริมาณการจราจรในระบบเน็ตเวิร์คได้ ค่าความล่าช้าที่ลดลงเมื่อจำนวนโหนดเพิ่มมากขึ้นเป็นผลมาจากความหนาแน่นของ forwarding node ที่เพิ่มขึ้น ทำให้ในการส่งต่อข้อมูลไปยังโหนดใกล้เคียงเป็นไปได้รวดเร็วยิ่งขึ้น ผลลัพธ์ในการช่วยลดค่าความล่าช้าในระบบเน็ตเวิร์คของโปรโตคอลสามารถตรวจสอบได้จากรูปที่ 6



รูปที่ 7. กราฟแสดงระยะเวลาที่ใช้ในการสร้างเส้นทาง

จากรูปที่ 7 จะสังเกตได้ว่าในกรณีที่จำนวน forwarding node มีจำนวนน้อย จะต้องใช้ระยะเวลาในการสร้างเส้นทางเป็นจำนวนมาก เนื่องจากการค้นหาโหนดที่จำเป็นต้องใช้ในการติดต่อไปยังปลายทางนั้นเป็นไปได้ยาก เมื่อจำนวน forwarding node เพิ่มขึ้นก็จะส่งผลให้ระยะเวลาในการสร้างเส้นทางลดลง แต่เมื่อโอเวอร์เฮดมีค่าสูงขึ้น ณ จุดหนึ่ง จะทำให้ระยะเวลาในการสร้างเส้นทางเพิ่มขึ้นเนื่องจากความหนาแน่นของระบบเน็ตเวิร์คที่เพิ่มขึ้น และในกรณีที่มีจำนวนโหนดเพิ่มขึ้นถึง 130 โหนดจากการทดสอบ จะสังเกตได้ว่าระยะเวลาในการสร้างเส้นทางค่อยๆลดลง เป็นผลมาจากโอกาสที่ฟังก์ชั่น route cache จะทำงานมีมากขึ้น ซึ่ง route cache นั้น สามารถช่วยลดระยะเวลาในขั้นตอนการทำ route discovery ให้สั้นลงได้

5. บทสรุป

การจำกัดการกระจายข้อมูลในขั้นตอน route discovery โดยการลดจำนวนโหนดที่ทำหน้าที่เป็น forwarding node อย่างเหมาะสม สามารถช่วยลดอัตราการเกิดโอเวอร์เฮดในระบบเครือข่ายไร้สายเฉพาะกิจ และยังคงรักษาประสิทธิภาพของระบบเครือข่ายเอาไว้ได้ แต่อย่างไรก็ตามผลการทดลองยังคงแสดงให้เห็นว่าประสิทธิภาพในการลดโอเวอร์เฮดของโปรโตคอลที่นำเสนอนั้นยังไม่ส่งผลต่อระบบเครือข่ายไร้สายเฉพาะกิจอย่างมีนัยสำคัญ และเนื่องจากเงื่อนไขที่ใช้ในการจำกัดการกระจายข้อมูลในรายงานฉบับนี้ จะลดปริมาณ forwarding node ในบริเวณรอบข้างโหนดต้นทางเป็นจำนวนมาก ซึ่งอาจก่อให้เกิดปัญหาเมื่อไม่มีโหนดใดๆ มารับข้อมูลจากโหนดต้นทางเลย เป็นสาเหตุให้การสร้างช่องทางในการติดต่อสื่อสารในระบบเครือข่ายนั้นล้มเหลว

ในส่วนของปัญหาดังกล่าว ผู้วิจัยมีแนวคิดที่จะปรับเปลี่ยนเงื่อนไขในการจำกัดการการะจายตัวข้อมูลให้มีความยืดหยุ่นมากยิ่งขึ้น และเพื่อให้โปรโตคอลใหม่นั้น สามารถลดปริมาณโอเวอร์เฮดในระบบเครือข่ายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

เอกสารอ้างอิง

[1] Sunil taneja and Ashwani kush." A survey of routing protocols in mobile ad hoc networks". international journal of innovation, management and technology, vol. 1, no. 3, august, 2010.

[2] S. Sen and J. Wang. "Analyzing Peer-to-Peer Traffic Across Large Networks", *Proc. Internet Measurement Workshop, Proc. Internet Measurement Workshop, 2002.*

[3] Young-Bae Ko and Nitin H. Vaidya. "Location-Aided Routing (LAR) in mobile Ad Hoc Networks". September, 2000.

[4] Johnson, D., Maltz, D., Broch, J., DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, 2001.

[5] Ghaith Bader Al-Suwaidi, Mohamed Jamal Zemerly. "Locating Friend and Family Using Mobile Phones with Global Positioning System (GPS)". 2009 IEEE, 2009.

[6] R. Bajaj, S. L. Ranaweera and D. P. Agrawal, "GPS: Location-Tracking Technology", IEEE Computer, Vol. 35, No. 4, 2002, pp. 92-94.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การปรับปรุงกลไกการแพร่กระจายข้อความ เพื่อลดการแลกเปลี่ยนข้อมูล บนเครือข่ายดีทีเอ็น

ธีรพงษ์ โชคสถิตย์, เบญจพร ปาวะรีย์, วรวัชร ณรงคะชวนะ และ สุเมธ ประภาวัต

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: TeerapongC@outlook.com, benjabhon@gmail.com, worravat@gmail.com, sumet@it.kmitl.ac.th

บทคัดย่อ

เราจะทำอย่างไร หากคุณต้องการใช้โทรศัพท์มือถือเพื่อแจ้งข่าวไปยังเพื่อนที่อยู่ไกลออกไป แต่เสากระจายสัญญาณกลับใช้การไม่ได้ ทางออกของจุดวิกฤตนี้คือ สร้างเครือข่ายสื่อสารเฉพาะกิจ เก็บและส่งต่อข้อความจากโทรศัพท์มือถือเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ซึ่งในทางปฏิบัติ กระบวนการดังกล่าวทำให้เครือข่ายต้องรองรับข้อความจำนวนมาก ส่งผลให้เกิดความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสาร และการที่โทรศัพท์มือถือต้องสูญเสียพลังงานในการส่งข้อความ ทำให้จำนวนโทรศัพท์มือถือที่สามารถช่วยส่งต่อข้อความลดลงอย่างต่อเนื่อง เพราะฉะนั้นการพัฒนา n-Anti Entropy ซึ่งได้ดัดแปลงข้อดีของ Anti Entropy และ n-Epidemic โดยผลการทดสอบในโมเดลจำลองแสดงให้เห็นว่า n-Anti Entropy มีแนวโน้มในการแก้ไขปัญหาข้างต้นได้ดีกว่ากลยุทธ์การส่งข้อความรูปแบบอื่นๆซึ่งสะท้อนให้เห็นถึงประสิทธิภาพของการสื่อสารในสถานการณ์จริงได้เป็นอย่างดี

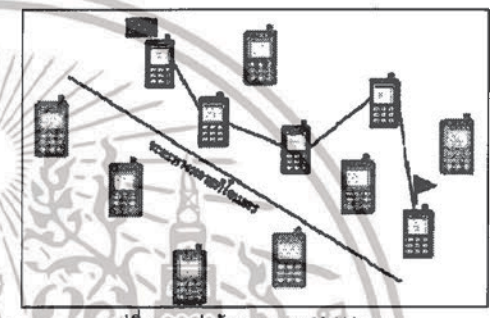
คำสำคัญ– เครือข่ายเฉพาะกิจ; เครือข่ายดีทีเอ็น; Anti Entropy; การแพร่กระจายข้อมูล; ลดการแลกเปลี่ยนข้อมูล

1. บทนำ

ระบบสื่อสารเป็นสิ่งจำเป็น เพราะในทุกๆกิจกรรมที่เกิดขึ้นในการดำรงชีวิตล้วนมีความเกี่ยวข้องกับการสื่อสารไม่มากก็น้อย ในขณะที่โลกกำลังก้าวข้ามผ่านการสื่อสารแบบเก่า ไปสู่โลกแห่งการสื่อสารไร้สาย นักพัฒนาก็กำลังสร้างเครือข่ายสื่อสารเฉพาะกิจ ที่อนุญาตให้อุปกรณ์สื่อสารต่างๆสามารถติดต่อระหว่างกันได้โดยตรง

ในบทความนี้ ผู้เขียนให้ความสนใจกับเครือข่ายที่มีความคงทนต่อความหน่วง (DTN : Delay Tolerant Network) ซึ่งเป็นเครือข่ายสื่อสารเฉพาะกิจ (Ad Hoc Network) ถูกออกแบบสำหรับแก้ไขปัญหาต้นทางไม่สามารถคาดการณ์ได้ว่าจะพบปลายทางได้เมื่อใด โดยอาศัยกระบวนการเก็บและส่งต่อข้อความ (Store-and-Forward Message Switching) เป็นการส่งข้อความไปกับอุปกรณ์อื่นๆหลายต่อ (Multi-hop) จนกระทั่งถึงปลายทาง[1] ดังรูปที่ 1 แสดงให้เห็นว่า ยิ่งสามารถแพร่กระจายข้อความไปได้มากเท่าไร โอกาสที่ข้อความถูกส่งไปยังโหนดปลายทางก็เพิ่มมากขึ้นเท่านั้น

ถึงแม้การสื่อสารบนเครือข่ายดีทีเอ็นมีความยืดหยุ่นมาก แต่ก็แลกมาด้วยโจทย์หลายข้อที่เป็นอุปสรรคต่อประสิทธิภาพในการแพร่กระจายข้อความ ในบทความนี้ผู้เขียนให้ความสนใจกับโจทย์สองข้อได้แก่ ความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสาร และแหล่งพลังงานที่จำกัดของอุปกรณ์สื่อสาร ซึ่งโจทย์ทั้งสองมักพบบนเครือข่ายสื่อสารเฉพาะกิจที่มีการส่งข้อมูลแบบบรอดแคสต์ (Broadcast) ด้วยเหตุนี้จึงนำไปสู่แนวคิดในการพัฒนากลยุทธ์การส่งข้อความ (Routing Strategies) เพื่อแก้ไขโจทย์ทั้งสองข้อ โดยไม่ส่งผลกระทบต่อประสิทธิภาพในการแพร่กระจายข้อความจนทำให้การสื่อสารของเครือข่ายล้มเหลว



รูปที่ 1. การส่งข้อความแบบ Multi-hop

หัวข้อต่อไปที่จะกล่าวถึงงานวิจัยต่างๆที่เกี่ยวข้อง ตามด้วยหัวข้อแนวทางการพัฒนา ซึ่งนำเสนอกลยุทธ์การส่งข้อความที่ได้พัฒนาขึ้นโดยกลยุทธ์ดังกล่าวถูกนำมาเปรียบเทียบกับกลยุทธ์ชนิดอื่นๆในหัวข้อการวิเคราะห์และประเมินผล และหัวข้อสุดท้ายเป็นการอภิปรายถึงบทสรุปการพัฒนา

2. งานวิจัยที่เกี่ยวข้อง

ความท้าทายของเทคโนโลยีเครือข่ายดีทีเอ็นคือ การสร้างกลยุทธ์การส่งข้อความ บนเครือข่ายที่ไม่สามารถทราบได้ถึงการเชื่อมต่อระหว่างโหนดใดๆ เพื่อสร้างเส้นทางการสื่อสารจากต้นทางไปยังปลายทางได้เลย ซึ่ง Jones E., Li L., Schmidtke J. และ Ward P. ได้เสนอกลยุทธ์การส่งข้อความเพื่อแก้ไขจุดบกพร่องดังกล่าว โดยใช้ข้อมูลจากเครือข่ายประมาณเวลาที่ข้อความบนโหนดจะถูกส่งต่ออีกครั้ง[2] นอกจากนั้น Jones E. และ Ward P. ได้ศึกษารวบรวมกลยุทธ์ในการส่งข้อความหลากหลายรูปแบบ ที่ได้ถูกสร้างขึ้นมาเพื่อแก้ไขโจทย์หัวข้อต่างๆ ซึ่ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เป็นอุปสรรคต่อการสื่อสารบนเครือข่ายดีทีเอ็น [3] เช่น Tree-Based Flooding, Epidemic Routing, Link Metrics เป็นต้น

ในสถานการณ์การสื่อสารปกติของเครือข่ายดีทีเอ็น นิยมใช้กลยุทธ์การส่งข้อความแบบฟลัด ที่อาศัยการคัดลอกข้อความส่งไปยังโหนดเพื่อนบ้านโดยรอบ เพื่อเพิ่มประสิทธิภาพในการแพร่กระจายข้อความ ซึ่งหมายถึงโอกาสที่ข้อความจะถูกส่งต่อไปยังโหนดปลายทางมีโอกาสมากขึ้น เมื่อเปรียบเทียบกับกลยุทธ์รูปแบบอื่น แต่ทั้งนี้กลยุทธ์ดังกล่าวก็เป็นต้นเหตุให้เกิดความคับคั่งของปริมาณข้อความบนเส้นทางการสื่อสาร นอกจากนี้การส่งข้อมูลแบบบรอดแคสต์ของอุปกรณ์ไร้สาย ยังทำให้พลังงานในแหล่งพลังงานสำรองสูญเสียไปกับการเคลื่อนที่ของโหนด และการส่งข้อความจำนวนมากเกินความจำเป็น

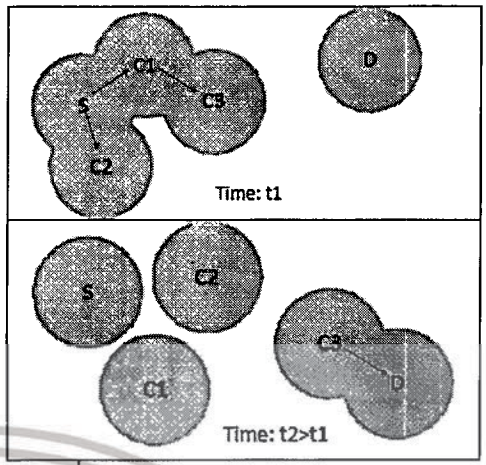
Epidemic Routing มีวิธีการส่งข้อความชนิดหนึ่งเรียกว่า Anti Entropy ซึ่งมีจุดประสงค์เพื่อลดความคับคั่งของปริมาณข้อความบนเส้นทางการสื่อสาร โดย Alan D. และคณะ ได้เสนอแนวคิดให้โหนดมีการแลกเปลี่ยนรายชื่อของข้อความ เพื่อตรวจสอบสถานะ ก่อนการส่งข้อความจริง[4] หลังจากนั้น Anti Entropy ก็มีการพัฒนาอย่างต่อเนื่องจนกระทั่ง Vahdat A., Becker D. และ คณะ ได้พัฒนากระบวนการดังกล่าว ให้เหมาะสมกับการใช้งานมากขึ้น โดยให้โหนดร้องขอเฉพาะข้อความที่ตนเองต้องการได้ [5]

แต่อย่างไรก็ตามการลดปริมาณการสูญเสียพลังงานของโหนด ก็เป็นอีกหนทางหนึ่งในการแก้ไขปัญหา จากการศึกษา n-Epidemic Routing ของ Lu X. และ Pan H. ซึ่งมีแนวคิดที่จะลดจำนวนครั้งการส่งข้อความ โดยการกำหนดให้มีการส่งข้อมูลแบบบรอดแคสต์ เมื่อมีโหนดเพื่อนบ้านครบตามจำนวนที่กำหนด เงื่อนไขดังกล่าวส่งผลให้การสูญเสียพลังงานจากการส่งข้อมูลลดลง อีกทั้งยังทำให้การส่งแต่ละครั้งมีโหนดที่ได้รับข้อความเพิ่มมากขึ้น[6] นอกจากนี้ De R. และ Amelio S. ยังได้พัฒนาต่อยอดให้ n-Epidemic Routing มีกลไกในการเลือกส่งต่อข้อความ (Dynamic Forwarding) โดยพิจารณาจากความหนาแน่นของโหนดในแต่ละกลุ่มเป็นสำคัญ[7]

และเพื่อเป็นการพิสูจน์ว่า ประสิทธิภาพการกระจายข้อความของกลยุทธ์การส่งข้อความที่นำเสนอ ไม่ได้ลดลงไปจากกลยุทธ์ต้นแบบ ในหัวข้อการวิเคราะห์และประเมินผล จึงได้มีการนำสัดส่วนของจำนวนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา เมื่อเทียบกับจำนวนโหนดทั้งหมด ของแต่ละกลยุทธ์การส่งข้อความ มาแสดงผลเปรียบเทียบในรูปแบบของกราฟ ซึ่งการเปรียบเทียบลักษณะนี้ถูกใช้สำหรับการวิเคราะห์และประเมินผลในหลากหลายบทความ[5][6][7] โดยสัดส่วนโหนดที่ได้รับข้อความในช่วงเวลา t สามารถคำนวณได้จากสูตร

$$R(t) = \frac{m(t)}{Node} \qquad (1)$$

โดย $R(t)$ = สัดส่วนโหนดที่ได้รับข้อความในช่วงเวลา t
$m(t)$ = จำนวนโหนดทั้งหมดที่ได้รับข้อความ ณ เวลา t
$Node$ = จำนวนโหนดทั้งหมด



รูปที่ 2. กลยุทธ์การส่งข้อความแบบ Epidemic Routing

3. แนวทางการพัฒนา

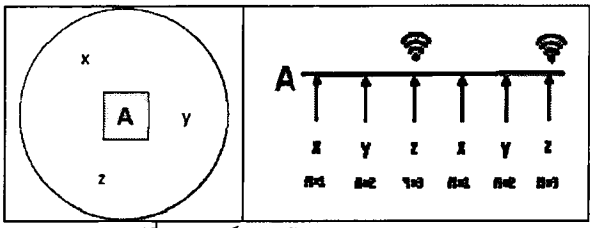
Epidemic Routing เป็นรูปแบบหนึ่งของกลยุทธ์การส่งข้อความแบบฟลัด ซึ่งอนุญาตให้โหนดคู่หนึ่งเชื่อมต่อกันเพื่อแลกเปลี่ยนข้อความของทั้งสองฝ่ายให้เหมือนกัน(Synchronize) โดยแต่ละข้อความจะถูกแลกเปลี่ยนไปเรื่อยๆ จนกระทั่งถึงโหนดปลายทาง อธิบายรูปแบบการทำงานตามรูปที่ 2 จากภาพแสดงให้เห็นว่ามีการแบ่งกลุ่มของโหนด ทำให้โหนด S ไม่สามารถส่งข้อความไปให้โหนด D ซึ่งอยู่คนละกลุ่มได้ ทำให้ที่เวลา t1 โหนด S จึงเพิ่มสัดส่วนโหนดที่ได้รับข้อความ โดยฝากข้อความดังกล่าวไปกับโหนด C1 C2 จากนั้นโหนด C1 จึงฝากข้อความไปให้โหนด C3 ตามลำดับ และที่เวลา t2>t1 โหนดต่างๆในเครือข่ายมีการเคลื่อนที่ ทำให้โหนด C3 อยู่ในระยะการสื่อสารของโหนด D ข้อความจึงถูกส่งไปถึงโหนด D ซึ่งเป็นโหนดปลายทางสำเร็จ

ดังที่กล่าวไปในหัวข้องานวิจัยที่เกี่ยวข้อง ผู้เขียนให้ความสนใจกับ Anti Entropy ซึ่งลดความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสารด้วยการส่งเฉพาะข้อความที่ได้รับการร้องขอ (Partial Message) และ n-Epidemic ที่สร้างเงื่อนไขให้การส่งข้อมูล เพื่อลดปริมาณการใช้พลังงาน (อายุของโหนดเพิ่มขึ้น) อีกทั้งผลลัพธ์ของทั้งสองกลยุทธ์ต่างทำให้ปริมาณข้อความที่ถูกส่งต่อทั้งหมดในเครือข่ายลดลง ดังนั้นผู้เขียนจึงนำเสนอกลยุทธ์การส่งข้อความใหม่ที่พัฒนาต่อเนื่องจาก n-Epidemic โดยอาศัยเทคนิคการส่งเฉพาะข้อความที่ถูกร้องขอของ Anti Entropy (n-Epidemic with Anti Entropy) โดยเรียกแบบย่อว่า n-Anti Entropy ซึ่งประกอบไปด้วยส่วนการทำงานหลัก ดังนี้

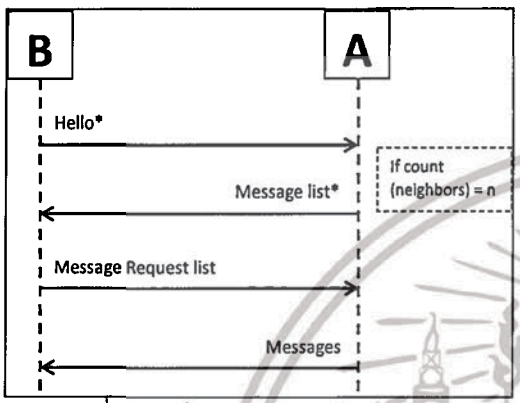
3.1 ส่วนกระบวนการก่อนส่งข้อความ

การทำงานในส่วนนี้ ใช้ประโยชน์จาก n-Epidemic ซึ่งจะเริ่มการส่งข้อมูลเมื่อโหนดมีจำนวนโหนดเพื่อนบ้านครบตามที่กำหนด ทำให้ไม่จำเป็นต้องส่งข้อมูลทุกครั้งที่พบโหนดอื่นๆในเครือข่าย โดยn-Epidemic อาศัยการส่งข้อมูลแบบบรอดแคสต์ ทำให้ในการส่งเพียงหนึ่งครั้ง โหนดเพื่อนบ้านจะได้รับข้อมูลทั้งหมด ส่งผลให้พลังงานที่โหนดสูญเสียไปกับการส่งข้อมูลแต่ละครั้งลดลง ตามรูปที่ 3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3. กลยุทธ์การส่งข้อความแบบ n-Epidemic



รูปที่ 4. กลยุทธ์การส่งข้อความแบบ n-Anti Entropy

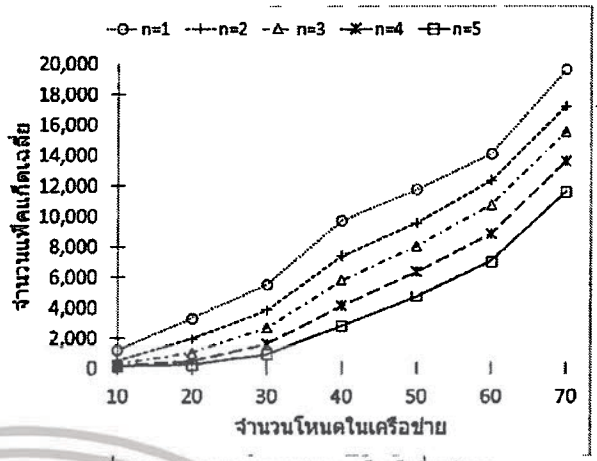
รูปที่ 4 อธิบายการทำงานที่ได้รับการพัฒนาขึ้น โดยกำหนดให้ ณ ช่วงเวลาหนึ่ง โหนด A มีโหนด x y และz เป็นโหนดเพื่อนบ้าน เมื่อโหนด A พบว่ามีโหนดเพื่อนบ้านครบ 3 โหนดตามที่ได้กำหนดไว้ หลังจากนั้นโหนด A ก็จะบรอดแคสต์ข้อมูลออกมาและเริ่มรอคอยโหนดเพื่อนบ้านใหม่อีกครั้ง

3.2 ส่วนคัดเลือกและส่งต่อข้อความ

โดยปกติในกระบวนการส่งข้อความ โหนดจำเป็นต้องส่งข้อความทั้งหมด เพราะไม่ทราบว่าโหนดที่กำลังติดต่อด้วยต้องการข้อความอะไรบ้าง ซึ่งเมื่อปริมาณข้อความภายในโหนดต่าง ๆบนเครือข่ายเพิ่มมากขึ้น ความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสารก็เกิดขึ้นอย่างหลีกเลี่ยงไม่ได้ แต่ทว่ากระบวนการส่งข้อมูลด้วย Anti Entropy ทำให้โหนดส่งเฉพาะข้อความที่โหนดเพื่อนบ้านต้องการเท่านั้น ปริมาณข้อมูลที่ต้องถูกส่งในแต่ละครั้งจึงลดลงอย่างมาก โดยหลักการทำงานที่ได้รับการพัฒนาเพื่อรองรับการทำงานต่อจากส่วนรอคอยการติดต่อจากโหนดเพื่อนบ้าน สามารถอธิบายการทำงานได้ตามรูปที่ 4 โดยแรกเริ่มโหนดแต่ละโหนดจะบรอดแคสต์ Hello แพ็คเก็ตออกไป เพื่อเป็นสัญญาณให้โหนดอื่นๆรู้ถึงการมีอยู่ของตน จากนั้นเมื่อโหนด A ได้รับสัญญาณจากโหนดต่าง ๆ ครบตามจำนวนที่กำหนด โหนด A จะบรอดแคสต์รายชื่อข้อความ (Message List) ที่มีออกไป และส่งข้อความ (Messages) ไปให้แต่ละโหนดตามที่ระบุไว้ในรายชื่อข้อความที่แต่ละโหนดต้องการ (Message Request List)

3.3 จำนวนข้อความทั้งหมดของ n-Anti Entropy

ดังที่กล่าวไปก่อนหน้านี้ การที่ผลรวมของจำนวนข้อความที่ถูกส่งออกของโหนดทั้งหมดในเครือข่ายลดลง ย่อมหมายถึงการที่โหนดทั้งหมดมีจำนวนข้อมูลที่ส่งในแต่ละครั้ง หรือจำนวนครั้งการส่งข้อมูลลดลงตามไปด้วย เพราะฉะนั้นจากการที่ n-Anti Entropy ซึ่งได้นำส่วนที่ดีของ n-Epidemic และ Anti Entropy มาทำงานร่วมกัน แสดงให้เห็นว่าการลดลงของจำนวนดังกล่าว ส่งผลให้ความคับคั่งของข้อมูลบนเส้นทางการสื่อสารได้รับการแก้ไขหรือบรรเทาลง ในขณะเดียวกันการสูญเสียพลังงานอันเนื่องมาจากการส่งข้อมูลของโหนดก็ลดลงเช่นกัน



รูปที่ 5. กราฟแสดงผลรวมของจำนวนแพ็คเก็ตที่ถูกส่งออก

ผลรวมของจำนวนข้อความที่ถูกส่งออกของโหนดทั้งหมดในเครือข่าย สามารถคำนวณได้จากสูตร

$$\text{sumPacket} = \sum_{i=1}^{m} f(i) \qquad (2)$$

โดย sumPacket = ผลรวมของจำนวนแพ็คเก็ตที่ถูกส่งออก

m = จำนวนครั้งการส่งข้อความทั้งหมด

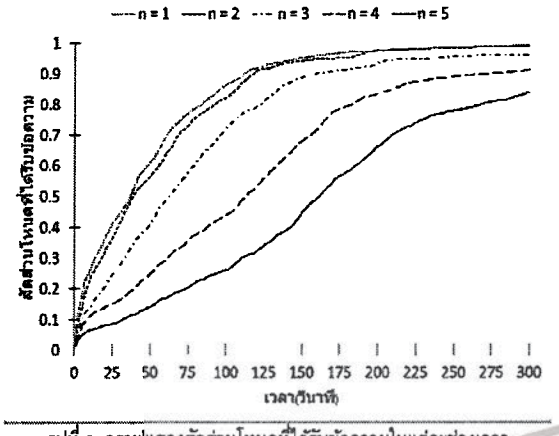
$f(i)$ = ขนาดข้อความที่ถูกส่ง ในการส่งครั้งที่ i ในหน่วยแพ็คเก็ต

รูปที่ 5 กราฟแสดงผลรวมของจำนวนแพ็คเก็ตเฉลี่ย ที่ถูกส่งออกไปในเครือข่าย เพื่อให้ทุกโหนดได้รับข้อความทั้งหมด ในช่วงเวลาที่น้อยที่สุดเปรียบเทียบกับจำนวนโหนดในเครือข่าย โดยกราฟแต่ละเส้นมีความแตกต่างกันตามจำนวนการรอคอยสัญญา (Hello) จากโหนดเพื่อนบ้าน โดยปกติการเพิ่มจำนวนของโหนดในกราฟแต่ละเส้นย่อมทำให้จำนวนแพ็คเก็ตที่ถูกส่งออกเพิ่มสูงขึ้น แต่จากการที่ n-Anti Entropy มีการสร้างเงื่อนไขให้โหนดต้องรอคอยสัญญาณจากโหนดเพื่อนบ้าน ส่งผลให้จำนวนแพ็คเก็ตที่ถูกส่งออกลดลงตามจำนวนการรอคอยสัญญาณที่เพิ่มขึ้น

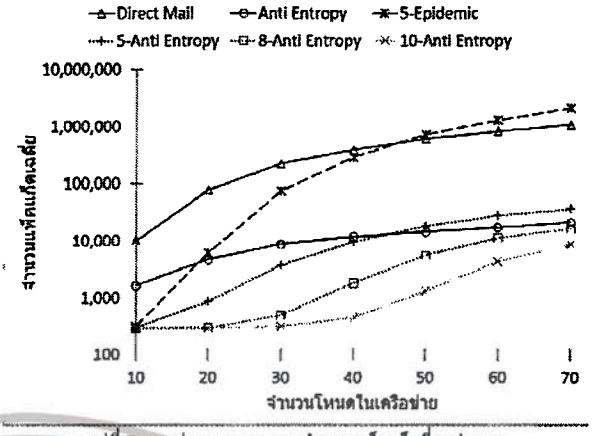
3.4 อัตราการกระจายข้อความของ n-Anti Entropy

เมื่อพิจารณา n-Anti Entropy การลดลงของผลรวมของจำนวนแพ็คเก็ตที่ถูกส่งออก สามารถพิสูจน์ได้จากรูปที่ 5 แต่ทั้งนี้เพื่อเป็นการตรวจสอบเพิ่มเติมถึงความถูกต้องของแบบจำลองที่สร้างขึ้น จึงได้มีการสร้างกราฟแสดงถึงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา ที่มีการกำหนดสภาพแวดล้อมของเครือข่ายตามบทความ[6] โดยกราฟในรูปที่ 6 แสดง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6. กราฟแสดงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา



รูปที่ 7. กราฟแสดงผลรวมของจำนวนแพ็คแก็ตที่ถูกส่งออก

ตารางที่ 1. ตารางแสดงสภาพแวดล้อมของเครือข่าย

จำนวนโหนด	30-70 โหนด
ขนาดของพื้นที่	1500 x 300 m^2
รัศมีการสื่อสารของโหนด	100 m
อัตราเร็วในการเคลื่อนที่ของโหนด	0-20 m/s
ความยาวของข้อความ	1 KB
อัตราการส่งสัญญาณของโหนด	ทุก 1 วินาที
เวลาที่ใช้ในการทดสอบ	300 วินาที

ให้เห็นว่า กราฟดังกล่าวมีลักษณะคล้ายคลึงกับกราฟสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลาในบทความที่อ้างอิง นอกจากนี้จากการศึกษาลักษณะของกราฟทั้งสองพบว่า ความชันเส้นกราฟแต่ละเส้นที่ลดลง มีความสัมพันธ์โดยตรงกับการเพิ่มขึ้นของจำนวนสัญญาณที่ต้องรอคอยก่อนการส่งข้อความ หรือกล่าวได้อีกนัยหนึ่งคือ การที่โหนดต้องรอคอยสัญญาณจากโหนดเพื่อนบ้านมากขึ้น ส่งผลอัตราการแพร่กระจายข้อความให้ทั่วทั้งเครือข่ายใช้เวลานานขึ้น

4. วิเคราะห์และประเมินผล

เพื่อพิสูจน์ว่า n-Anti Entropy มีผลรวมของจำนวนข้อความที่ส่งออกไปยังเครือข่ายน้อยกว่ากลยุทธ์ต้นแบบ ซึ่งประกอบไปด้วย Epidemic (Direct Mail) , Anti Entropy และn-Epidemic จึงได้มีการสร้างแบบจำลองของกลยุทธ์การส่งข้อความทั้ง 4 รูปแบบ ควบคู่ไปกับการศึกษาบทความของ Grasic S. และ Anders L. ที่ได้ศึกษาและพัฒนาโมเดล สำรับใช้ในการทดสอบกลยุทธ์การส่งข้อความของเครือข่ายดีทีเอ็น โดยมุ่งหวังให้การทดสอบมีความคล้ายคลึงกับการนำกลยุทธ์ดังกล่าวไปใช้สำหรับการสื่อสารในสถานการณ์จริงมากที่สุด[8]

4.1 สภาพแวดล้อมของเครือข่ายที่ใช้ในการทดสอบ

ในการทดสอบครั้งนี้ได้มีการกำหนดตามสถานการณ์การสื่อสารจากบทความ[5] ที่มีการทดสอบอัตราการแพร่กระจายข้อความของ Anti Entropy ในหลากหลายสถานการณ์ อีกทั้งสถานการณ์การสื่อสารจากบทความนี้ยังถูกใช้ในบทความอื่นๆ[9] ซึ่งการกำหนดสภาพแวดล้อมของเครือข่ายของสถานการณ์การสื่อสาร ที่ใช้ในการทดสอบถูกระบุไว้ในตารางที่ 1 ดังนี้

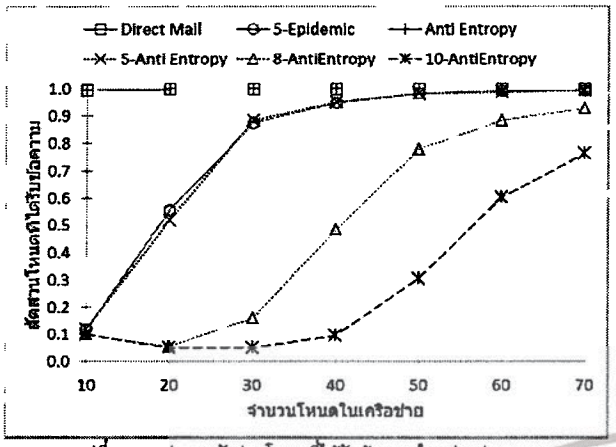
เพื่อให้การทดสอบแบบจำลอง มีความสอดคล้องกับการสื่อสารในสถานการณ์จริงมากที่สุด จึงได้มีการกำหนดให้ 90% ของโหนดทั้งหมดมีการสร้างข้อความเพื่อส่งถึงกันและกัน ส่วนโหนดอีก 10% ที่เหลือจะไม่มีการสร้างข้อความแต่ยังคงสามารถทำหน้าที่เป็นโหนดถ่ายทอดได้ ยกตัวอย่างเช่น มีโหนดทั้งหมดในเครือข่าย 50 โหนด เพราะฉะนั้นมีโหนดที่สามารถสร้างข้อความได้จำนวน 45 โหนด โดยโหนดที่ 1 จะสร้างข้อความจำนวน 44 ข้อความ เพื่อส่งไปหาโหนด 2-45 ส่วนโหนด 46-50 จะไม่มีการสร้างข้อความใดๆทั้งสิ้น ดังนั้นในการทดสอบในเครือข่าย 50 โหนด จะมีข้อความถูกสร้างทั้งหมด 1980 ข้อความ นอกจากนั้นเพื่อเป็นการหลีกเลี่ยงโอกาสที่โหนดจะส่งข้อความชนกัน จึงมีการกำหนดค่าความหน่วงในการส่งข้อความเท่ากับ 0.01 วินาที

4.2 กราฟแสดงผลรวมของจำนวนแพ็คแก็ต กับจำนวนโหนดในเครือข่าย

จากรูปที่ 7 แสดงให้เห็นว่า Direct Mail มีระดับจำนวนแพ็คแก็ตสูงที่สุด เนื่องจากการที่โหนดส่งข้อความทั้งหมดที่ตนมี เมื่อมีการแลกเปลี่ยนข้อมูลเกิดขึ้น ซึ่งระดับดังกล่าวถูกทำให้ลดลงด้วย Anti Entropy ที่อนุญาตให้โหนดส่งเฉพาะข้อความที่ถูกร้องขอเท่านั้น และเมื่อไม่นานมานี้ n-Epidemic ได้มีการเสนอแนวคิดที่น่าสนใจ เพื่อลดจำนวนครั้งการส่งข้อความ ซึ่งจากกราฟแสดงให้เห็นว่า สามารถลดจำนวนแพ็คแก็ตได้อย่างมาก เมื่อมีการกำหนดจำนวนโหนดที่ต้องรอคอยให้เหมาะสมกับจำนวนโหนดในเครือข่าย

เนื่องจาก n-Anti Entropy เป็นกลยุทธ์การส่งข้อความที่ได้รวมเอาข้อดีของ Anti Entropy และ n-Epidemic ทำให้จำนวนแพ็คแก็ตที่ถูกส่งออกไปในเครือข่ายน้อยกว่ากลยุทธ์อื่นๆที่เปรียบเทียบ และเมื่อมีการเพิ่มจำนวนโหนดเพื่อนบ้านของ n-Anti Entropy ก็ยิ่งทำให้ระดับของจำนวนแพ็คแก็ตลดลงมากยิ่งขึ้น แต่เมื่อพิจารณาจุดที่เครือข่ายมีโหนดมากกว่า 50 โหนด เส้นกราฟ 5-Anti Entropy จะมีจำนวนแพ็คแก็ตมากกว่า Anti Entropy ซึ่งแสดงให้เห็นว่า การนำ n-Anti Entropy มาใช้ในการสื่อสารเพื่อลดจำนวนแพ็ตแก็ตที่ถูกส่งออกไปยังเครือข่าย จำเป็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8. กราฟแสดงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา

ต้องรักษาสมดุลระหว่างจำนวนโหนดที่รอคอยกับจำนวนโหนดในเครือข่ายให้สอดคล้องกันมากที่สุด

4.3 กราฟแสดงสัดส่วนของจำนวนโหนดที่ได้รับข้อความ กับจำนวนโหนดในเครือข่าย

ในรูปที่ 8 กราฟแสดงให้เห็นถึงสัดส่วนของโหนดที่ได้รับข้อความครบต่อโหนดทั้งหมดในเครือข่าย ในช่วงเวลาหนึ่งๆซึ่งจากการพิจารณากราฟแต่ละเส้นสามารถสรุปได้ว่า เมื่อหยุดการจำลองวินาทีที่ 300 วินาที โหนดทั้งหมดในเครือข่ายที่ใช้กลยุทธ์การส่งข้อความแบบDirect Mail และAnti Entropy ได้รับข้อความครบทั้งหมด หรืออีกนัยหนึ่งหมายความว่าข้อความถูกส่งไปยังปลายทางครบทั้งหมดแล้ว แต่สำหรับ n-Epidemic และn-Anti Entropy สัดส่วนของโหนดที่ได้รับข้อความจะเพิ่มขึ้นตามความหนาแน่นของโหนด อีกทั้งการเพิ่มจำนวนโหนดเพื่อนบ้านที่ต้องรอคอย ส่งผลให้ความชันของสัดส่วนโหนดที่ได้รับข้อความเมื่อเทียบกับความหนาแน่นของโหนดลดลง

ปรากฏการณ์การเปลี่ยนแปลงสัดส่วนโหนดที่ได้รับข้อความของn-Epidemic และn-Anti Entropy สามารถอธิบายได้จากทฤษฎีการเชื่อมต่อของกราฟ (Connectivity Graph Theory) ซึ่งมีความคล้ายคลึงกับการทำงานของกลยุทธ์ทั้งสอง ถ้าเปรียบโหนดในเครือข่ายเป็นจุดบนกราฟ การเชื่อมต่อกันของโหนดคู่หนึ่งก็เปรียบเสมือนเส้นที่เชื่อมจุดหนึ่งไปยังอีกจุดหนึ่ง การที่กลยุทธ์มีการกำหนดจำนวนโหนดเพื่อนบ้าน(เชื่อมต่อ)ที่ต้องรอคอย ก็เปรียบเสมือนกราฟต้องมีเชื่อมต่อของจุดจำนวนหนึ่งด้วยเช่นกัน เพราะฉะนั้นจากกราฟจะสังเกตได้ว่า การที่จะทำให้กลยุทธ์ที่กำหนดจำนวนโหนดเพื่อนบ้านไว้สูง มีสัดส่วนของโหนดที่ได้รับข้อความเยอะ จำเป็นต้องอาศัยเครือข่ายที่มีความหนาแน่นของโหนดมากพอในระดับหนึ่งเช่นกัน นอกจากนั้นปัญหาดังกล่าวยังเป็นปัญหาเบื้องต้นในการออกแบบเครือข่ายเซ็นเซอร์ไร้สาย (Wireless Sensor Network) Gu X. และ Hailin F. ได้อธิบายไว้ว่า การทำให้โหนดใดๆเชื่อมต่ออยู่กับเครือข่ายนานที่สุดเท่าที่จะทำได้ คือรากฐานสำคัญในการออกแบบเครือข่ายเซ็นเซอร์ไร้สาย ซึ่งเป็นไปไม่ได้สำหรับโหนดในพื้นที่การสื่อสารขนาดใหญ่ และมีการการกระจายตัวที่ไม่สามารถคาดเดาได้ แต่อย่างไรก็ตามในสถานการณ์จริง ความเป็นไปไม่ได้มักเป็นไปได้ เพราะเราเพียงแค่ต้องการโหนดจำนวนหนึ่ง ซึ่งมากเพียงพอสำหรับสร้างเส้นทางการสื่อสาร เพื่อส่งข้อความจากโหนดหนึ่งไปยังอีกโหนดหนึ่งที่อยู่ไกลออกไปเท่านั้น[10]

จากกราฟในรูปที่ 7 เมื่อสังเกต 8-Anti Entropy ก่อนจำนวนโหนดในเครือข่ายจะมากกว่า 70 โหนด จำนวนแพ็คแก็ตยังคงน้อยกว่ากลยุทธ์รูปแบบอื่นๆ(จำนวนแพ็คแก็ตเข้าใกล้ Anti Entropy) ซึ่งเมื่อพิจารณาสัดส่วนของโหนดที่ได้รับข้อความ ในกราฟรูปที่ 8 เมื่อมีโหนดในเครือข่าย 60 โหนด จะพบว่า 8-Anti Entropy มีสัดส่วนมากกว่า 80% ทั้งที่ในขณะเดียวกัน 10-Anti Entropy ยังมีสัดส่วนที่ต่ำมาก และถึงแม้ว่า 5-Anti Entropy จะมีค่าเข้าใกล้ 100% แต่จำนวนแพ็คแก็ต(รูปที่7) ก็มีค่ามากกว่า Anti Entropy อย่างมาก ซึ่งกรณีดังกล่าวเป็นตัวอย่างการกำหนดโหนดเพื่อนบ้านให้มีความสอดคล้องกับโหนดในเครือข่ายของ n-Anti Entropy

5. สรุปการพัฒนา

ถ้าในเครือข่ายมีโหนดเพียงจำนวนหนึ่ง ซึ่งมีความต้องการการส่งข้อความเพื่อสื่อสารไปยังโหนดปลายทางที่น้อย เราควรให้ความสำคัญกับการเลือกใช้กลยุทธ์การส่งข้อความที่มีอัตราการแพร่กระจายสูง แต่ทว่าในสถานการณ์การสื่อสารจริง ที่โหนดแต่ละโหนดสร้างข้อความเพื่อสื่อสารไปยังโหนดต่างๆในเครือข่ายอย่างต่อเนื่อง สิ่งที่สำคัญมากกว่าอัตราการแพร่กระจายคือ ทำอย่างไรให้ทุกโหนดมีอายุการใช้งานเพิ่มขึ้นเพื่อช่วย(เพิ่มความเป็นไปได้) ในการส่งต่อข้อความไปยังปลายทาง และทำอย่างไรให้เส้นทางการสื่อสารสามารถรองรับข้อมูลได้อย่างต่อเนื่องโดยไม่เกิดปัญหาความคับคั่งของปริมาณข้อมูลเสียก่อน บทความนี้แสดงให้เห็นว่า n-Anti Entropy ซึ่งเป็นกลยุทธ์การส่งข้อความที่ได้รับการพัฒนามาจาก n-Epidemic และ Anti Entropy สามารถตอบโจทย์การสื่อสารในสถานการณ์จริงได้เป็นอย่างดี จากผลการทดลองแสดงให้เห็นว่า n-Anti Entropy มีผลรวมจำนวนข้อความที่ส่งออกน้อยกว่ากลยุทธ์ต้นแบบ ซึ่งสะท้อนให้เห็นว่าโหนดสูญเสียพลังงานในการส่งข้อมูลน้อยกว่า อีกทั้งยังสามารถลดปัญหาความคับคั่งของเส้นทางการสื่อสารได้ดีกว่าอีกด้วย และจากกราฟสัดส่วนของโหนดที่ได้รับข้อความ ยังแสดงให้เห็นถึงความสัมพันธ์ระหว่างความหนาแน่นของโหนดในเครือข่าย กับการกำหนดจำนวนโหนดเพื่อนบ้านที่ต้องรอคอย เพื่อให้ n-Anti Entropy มีประสิทธิภาพในการสื่อสารสูงสุด

เอกสารอ้างอิง

[1] Forrest Warthman. "Delay- and Disruption- Tolerant Networks (DTNs): A Tutorial" Interplanetary Internet Special Interest Group, July 2012.

[2] Jones, Evan PC, et al. "Practical routing in delay-tolerant networks." *Mobile Computing, IEEE Transactions on* 6.8 (2007): 943-959.

[3] Jones, Evan PC, and Paul AS Ward. "Routing strategies for delay-tolerant networks." *Submitted to ACM Computer Communication Review (CCR)* (2006).

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[4] Demers, Alan, et al. "Epidemic algorithms for replicated database maintenance." Proceedings of the sixth annual ACM Symposium on Principles of distributed computing. ACM, 1987.

[5] Vahdat, Amin, and David Becker. Epidemic routing for partially connected ad hoc networks. Technical Report CS-200006, Duke University, 2000.

[6] Lu, Xiaofeng, and Pan Hui. "An energy-efficient n-epidemic routing protocol for delay tolerant networks." *Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on*. IEEE, 2010.

[7] De Rango, and Amelio S. "Performance evaluation of scalable and energy efficient dynamic n-epidemic routing in Delay Tolerant Networks" Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2013 International Symposium on. IEEE, 2013.

[8] Grasic, Samo, and Anders Lindgren. "An analysis of evaluation practices for DTN routing protocols." Proceedings of the seventh ACM international workshop on Challenged networks. ACM, 2012.

[9] Mundur, Padma, Matthew Seligman, and Ginnah Lee. "Epidemic routing with immunity in delay tolerant networks." Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE, 2008.

[10] Gu, Xin, and Hailin Feng. "Connectivity analysis for a wireless sensor network based on percolation theory." Computer Application and System Modeling (ICCASM), 2010 International Conference on. Vol. 5. IEEE, 2010.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การปรับปรุงกลไกค้นหาเกตเวย์เพื่อลดโอเวอร์เฮด จากการแลกเปลี่ยนข้อมูลในเครือข่ายเฉพาะกิจ

สุเมธ ประภาวัต ทะนง ชูวณิชชานนท์ สารัช ศรีสวัสดิ์พงษ์ และ วรวัชร ณรงคะชวนะ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: sumet@it.kmitl.ac.th, tanong3200@hotmail.com, acecharmil@gmail.com, worravat@gmail.com

บทคัดย่อ

สำหรับระบบเครือข่ายสื่อสารที่สามารถใช้งานในสถานการณ์ภัยพิบัติหรือโครงสร้างพื้นฐาน (Infrastructure) ถูกทำลายโดยส่วนใหญ่จะใช้ระบบเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด (Mobile Ad hoc Network: MANET) เพื่อสร้างเครือข่ายที่ไม่พึ่งพาโครงสร้างพื้นฐาน อีกทั้งมีการขยายขีดการเชื่อมต่อให้เครือข่ายสื่อสารเฉพาะกิจสามารถเชื่อมต่อระหว่างเครือข่ายได้โดยการค้นหาเกตเวย์ (Gateway Discovery) ทำให้ผู้ใช้สามารถติดต่อขอความช่วยเหลือกับคนที่อยู่นอกเครือข่ายหรือเขตภัยพิบัติได้ แต่การค้นหาเกตเวย์ที่มีอยู่นั้นมีโอเวอร์เฮดในการแลกเปลี่ยนข้อมูลสำหรับการค้นหาเกตเวย์จำนวนมาก ดังนั้นในงานวิจัยนี้จึงทำการลดโอเวอร์เฮดดังกล่าวเพื่อปรับปรุงกลไกค้นหาเกตเวย์ ซึ่งอาจส่งผลให้การใช้แบนด์วิดธ์ (Bandwidth) และพลังงานของโมบายล์โหนดในการค้นหาเกตเวย์ลดลง

คำสำคัญ-- เครือข่ายสื่อสารเฉพาะกิจ; การเชื่อมต่อระหว่างเครือข่าย; การค้นหาเกตเวย์

1. บทนำ

การติดต่อสื่อสารเป็นสิ่งที่จำเป็นอย่างมาก และด้วยความก้าวหน้าทางด้านเทคโนโลยีที่มีการพัฒนาไปอย่างรวดเร็วจึงทำให้เกิดนวัตกรรมใหม่ ๆ ทางด้านการสื่อสารแบบไร้สายขึ้นและมีการใช้งานกันอย่างแพร่หลาย อาทิ การเชื่อมต่ออินเทอร์เน็ตความเร็วสูงผ่านทางเครือข่ายไร้สาย และ เครือข่ายอินเทอร์เน็ตโทรศัพท์ไร้สาย จนทำให้การสื่อสารแบบไร้สายกลายเป็นส่วนหนึ่งในการดำเนินชีวิตของมนุษย์ ทั้งนี้เองหากมีภัยพิบัติหรือเหตุการณ์ไม่คาดฝัน เช่น แผ่นดินไหว สึนามิ ซึ่งทำให้โครงสร้างพื้นฐาน (Infrastructure) ถูกทำลาย หรือขาดแคลนแหล่งพลังงาน (แหล่งจ่ายไฟฟ้ากระแสสลับ) ส่งผลให้การติดต่อสื่อสารระหว่างโมบายล์โหนดกับโครงสร้างพื้นฐานถูกตัดขาด จึงไม่สามารถติดต่อสื่อสารหรือขอความช่วยเหลือจากบุคคลภายนอกได้ โดยมีนักวิจัยหลายกลุ่มพยายามพัฒนาเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด (MANET : Mobile Ad-hoc Network) [1] ทำให้โมบายล์โหนดที่ติดต่อสื่อสารกันได้โดยไม่ต้องใช้โครงสร้างพื้นฐาน

ในเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด แต่ละโหนดจะส่งต่อแพ็กเก็ตให้กับโหนดข้างเคียง โดยอาศัยการเชื่อมต่อแบบโหนดต่อโหนด (Peer-to-Peer) ผ่านคลื่นความถี่วิทยุ (Radio Frequency) เช่น เครือข่ายระหว่างยานพาหนะ (VANET : Vehicular ad hoc network)

แต่การเชื่อมต่อกันเพียงในเครือข่ายดังกล่าวทำให้เกิดปัญหาการจำกัดทางด้านขอบเขตของเครือข่าย และในการที่โมบายล์โหนดต้องทำหน้าที่เป็นผู้ส่งต่อข้อมูลให้โหนดอื่น ๆ ทำให้มีการใช้พลังงานเพื่อทำหน้าที่ดังกล่าวนอกเหนือจากเพื่อการส่งข้อมูลของตนเอง ซึ่งส่งผลให้เกิดปัญหาในการใช้พลังงานที่มีอยู่อย่างจำกัด (จากแบตเตอรี่) ของโมบายล์โหนด

จากปัญหาดังกล่าว ผู้จัดทำจึงศึกษารูปแบบการหาเส้นทางบนเครือข่ายเฉพาะกิจของโมบายล์โหนด ให้สามารถหาเส้นทางเชื่อมต่อที่ผ่านเกตเวย์ออกไปยังโครงสร้างพื้นฐานได้ (อย่างเช่น เครือข่ายอินเทอร์เน็ต) เพื่อขยายขอบเขตเครือข่ายในการติดต่อสื่อสารให้กว้างขึ้น ทำให้ติดต่อสื่อสารออกไปนอกพื้นที่ได้ และเพื่อลดการใช้พลังงานที่มีอยู่อย่างจำกัดของโมบายล์โหนดให้ทำงานได้นานขึ้น ทำให้ลดโอกาสเกิดความไม่ต่อเนื่องในเครือข่าย ซึ่งเป็นการพัฒนาเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนดให้มีประสิทธิภาพมากยิ่งขึ้น

ในส่วนที่ 2 นั้นจะอธิบายถึงเทคโนโลยีที่นำมาใช้และทฤษฎีต่างๆ ที่เกี่ยวข้องในการพัฒนา ส่วนที่ 3 จะกล่าวถึงรายละเอียดของอัลกอริทึมในการค้นหาเกตเวย์ที่ได้ทำการพัฒนาขึ้น สำหรับส่วนที่ 4 จะเป็นการประเมินและวัดประสิทธิภาพของอัลกอริทึมดังกล่าว และสุดท้ายส่วนที่ 5 จะเป็นส่วนที่กล่าวถึงการสรุปผลของงานวิจัยนี้

2. ทฤษฎีและงานที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวกับเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนดทำให้ทราบได้ว่าโพรโทคอลค้นหาเส้นทาง (Routing Protocols) ในเครือข่ายดังกล่าวสามารถแบ่งได้เป็น 3 กลุ่มตามรูปแบบพฤติกรรมในการค้นหาเส้นทาง [2] คือ 1) โพรโทคอลค้นหาเส้นทางแบบรีแอกทีฟ (Reactive Routing Protocols) ซึ่งทำการค้นหาเส้นทางเมื่อต้องการส่งข้อมูล ตัวอย่างของโพรโทคอลค้นหาเส้นทางที่มีลักษณะแบบนี้ ได้แก่ โพรโทคอลเอโอดีวี (AODV : Ad hoc On-Demand Distance Vector) [6] และโพรโทคอลดีเอสอาร์ (DSR : Dynamic Sort Routing) [5] เป็นต้น 2) โพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ (Proactive Routing Protocols) ซึ่งจะทำการค้นหาเส้นทางไปยังทุกปลายทางที่น่าจะเป็นไปได้ก่อนที่จะมีการส่งข้อมูล ตัวอย่างของโพรโทคอลค้นหาเส้นทางที่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ลักษณะแบบนี้ เช่น โพรโทคอลโอแอลเอสอาร์ (OLSR : Optimized Link State Routing) [7] และสุดท้าย 3) โพรโทคอลค้นหาเส้นทางแบบไฮบริดจ์ (Hybrid Routing Protocols) ซึ่งจะมีการทำงานผสมผสานระหว่างโพรโทคอลค้นหาเส้นทางทั้ง 2 แบบที่ได้กล่าวไว้ก่อนหน้า ตัวอย่างของโพรโทคอลค้นหาเส้นทางที่มีลักษณะแบบนี้ เช่น โพรโทคอลแซดอาร์พี (ZRP : Zone Routing Protocol)

โดยทั้งหมดนี้มีงานวิจัยบางส่วนได้พูดถึงการเชื่อมต่อระหว่างเครือข่ายเฉพาะกิจของโมบายล์โหนดกับเครือข่ายอื่นๆ เช่น เครือข่ายโทรศัพท์ (Cellular Network) [11] เครือข่ายอินเทอร์เน็ต [8],[9],[10] โดยในการเชื่อมต่อนักวิจัยได้เลือกใช้การค้นหาโหนดเกตเวย์ซึ่งมีหน้าที่เป็นตัวกลางในการเชื่อมต่อ โดยโหนดที่เป็นเกตเวย์นั้นเปรียบเสมือนประตูในการเชื่อมต่อระหว่างเครือข่ายสื่อสารเฉพาะกิจและเครือข่ายอินเทอร์เน็ตหรือเครือข่ายอื่นๆ ซึ่งเกตเวย์นั้นมีหน้าที่ทำความเข้าใจโพรโทคอลในการค้นหาเส้นทางทั้งแบบลำดับชั้น (Hierarchical) ของเครือข่ายอินเทอร์เน็ต และแบบแบน (Flat) ในเครือข่ายสื่อสารเฉพาะกิจ

จากการศึกษางานวิจัยที่เกี่ยวข้องกับการค้นหาเกตเวย์ นักวิจัยได้นำโพรโทคอลค้นหาเส้นทาง AODV [8],[10] มาทำการปรับแก้รูปแบบและการส่งของข้อความ (Message) จากที่กำหนดใน RFC [6] โดยแก้ไข HELLO messages ซึ่งในโพรโทคอล AODV นั้นใช้ HELLO messages เพื่อบอกถึงการมีตัวตนของตนเองกับโหนดรอบข้างโดยการบรอดแคสต์ซึ่งถูกส่งก็ต่อเมื่อโหนดนั้นๆยังไม่มีการส่ง คำร้องขอเส้นทาง (Route Request) การตอบกลับเส้นทาง (Route Reply) หรือข้อความในชั้นสื่อสารเชื่อมต่อข้อมูล (Data Link layer) โดยในการปรับแก้รูปแบบข้อความนั้นได้ทำการเพิ่มแฟล็ก (Flag) พิเศษ ที่เรียกว่าแฟล็ก I (I-flag) เพื่อระบุว่าเป็น HELLO message ที่ส่งมาจากเกตเวย์ และยังทำการบันทึกแอดเดรสของเกตเวย์ (Gateway Address) ใน HELLO message ด้วยเพื่อระบุว่าถูกสร้างมาจากเกตเวย์โหนดใด ซึ่งทั้งค่าแฟล็ก I และ แอดเดรสของเกตเวย์ (Gateway Address) จะถูกเก็บในฟิลล์ที่ไม่ได้ใช้ (Unused Field) ของ HELLO messages ทั้งนี้จึงขอเรียก HELLO messages ที่มีการปรับแต่งว่า HELLO_I ซึ่งในการส่ง HELLO I นั้นจะเริ่มส่งจากโหนดเกตเวย์เพื่อบอกถึงการมีอยู่ของโหนดเกตเวย์ให้ทุกโหนดที่อยู่ภายในช่วงคลื่นสัญญาณของเกตเวย์รับรู้ผ่านการรับ HELLO_I (จากการบรอดแคสต์ HELLO_I ของเกตเวย์) และจากนั้นโหนดที่ได้รับ HELLO_I จะทำการบรอดแคสต์ (Rebroadcast) HELLO_I ซ้ำออกไป โดยก่อนหน้านั้นจะทำการบันทึกเส้นทางที่สามารถไปยังเกตเวย์ได้ให้เป็น Default Route และมีเป้าหมายที่จะส่งต่อไป (Next Hop) เป็นโหนดที่ส่ง HELLO_I มาหาโหนดตัวนั้น (สำหรับโหนดที่ได้รับจากเกตเวย์คือ แอดเดรสของเกตเวย์) แต่ถ้าโหนดใดไม่ได้รับ HELLO_I ในช่วงระยะเวลาของการส่ง HELLO messages (HELLO interval) โหนดนั้นก็จะทำการส่ง HELLO messages แบบดั้งเดิมแทน (แบบปกติที่ไม่มีการปรับแก้)

เพื่อง่ายต่อความเข้าใจจึงขอเรียกการค้นหาเส้นทางไปยังเกตเวย์นี้ว่า อัลกอริทึม HELLO ซึ่งภายในงานวิจัยดังกล่าวนักวิจัยได้ทำการเปรียบเทียบอัลกอริทึม HELLO เข้ากับอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ และแบบรีแอกทีฟ โดยผลสรุปของงานวิจัยที่ได้ศึกษานี้คือ อัลกอริทึม HELLO มีเวลาที่ใช้ในการค้นหาเกตเวย์ที่น้อยกว่าเมื่อเปรียบเทียบกับอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ และแบบรีแอกทีฟ โดยอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟนั้นจะใช้เวลาในการค้นหาเกตเวย์ที่มากและคงที่ ทั้งนี้เราจึงให้ความสนใจเพียงอัลกอริทึม HELLO และอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ

โดยสำหรับโพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ [10] เมื่อโหนดได้รับข้อมูลเกี่ยวกับเกตเวย์จะตัดสินใจว่าจะรับหรือทิ้งข้อมูลนั้น โดยจะรับข้อมูลนั้นก็ต่อเมื่อโหนดไม่รู้เส้นทางไปยังเกตเวย์หรือข้อมูลนั้นมีเส้นทางที่สั้นกว่าหรือข้อมูลนั้นมาจากแหล่งกำเนิดเดียวกันแต่มีความใหม่กว่า (มี sequence number ที่มากกว่า) และถ้าหากโหนดได้รับข้อมูลเส้นทางก็จะหยุดการร้องขอเส้นทาง จากนั้นจึงทำการตั้งค่าหรือปรับปรุงเส้นทางไปยังเกตเวย์ตามข้อมูลที่ได้รับมา และส่งต่อไปยังโหนดอื่นๆ

3. แนวคิดและการดำเนินงาน

จากตัวอย่างงานวิจัยที่เกี่ยวกับการค้นหาเกตเวย์ที่ได้ทำการศึกษาและแสดงอยู่ในส่วนที่ 2 ของงานวิจัยนี้ อัลกอริทึม HELLO ที่ใช้การปรับแก้ HELLO message นั้นมีความน่าสนใจเป็นอย่างมากเนื่องจากมีเวลาในการทำให้แต่ละโหนดรับรู้ถึงการมีอยู่ของเกตเวย์น้อยกว่าอัลกอริทึมอื่นๆ แต่ก็ยังมีข้อเสียอยู่เช่นกัน คือภายในกลไกของอัลกอริทึม HELLO นั้นมักจะเกี่ยวข้องกับการบรอดแคสต์ข้อมูลเป็นส่วนใหญ่ซึ่งมีส่วนทำให้เกิดการสูญเสียพลังงานของโมบายล์โหนดโดยไม่จำเป็น ซึ่งในงานวิจัยของเราได้เล็งเห็นถึงปัญหาในส่วนนี้ จึงนำอัลกอริทึม HELLO มาเพิ่มกลไกบางอย่าง เพื่อลดการบรอดแคสต์ข้อมูลเส้นทางที่เกี่ยวข้องกับเกตเวย์ โดยลดการบรอดแคสต์ที่มีปลายทางซ้ำ ๆ กันโดยไม่จำเป็นในเครือข่าย ด้วยวิธีการลดจำนวนโหนดที่ทำการบรอดแคสต์ ซึ่งกลไกนี้แต่เดิมจะถูกใช้ในโพรโทคอลค้นหาเส้นทาง OLSR และมีชื่อเรียกว่าการเลือกโหนดเอ็มพีอาร์ (MPR: Multipoint Relays Selection) โดยโหนด MPR นั้นเป็นกลุ่มของโหนดข้างเคียง (Neighbor nodes) ที่มีหน้าที่ในการส่งต่อข้อมูล (Retransmission) ซึ่งทุกโหนดที่เป็นโหนดข้างเคียงไม่จำเป็นต้องเป็นโหนด MPR โดยโหนดที่ทำหน้าที่ในการเลือกโหนด MPR จะถูกเรียกว่าผู้คัดเลือกโหนด MPR (MPR Selectors) และกลุ่มของโหนด MPR ก็สามารถเปลี่ยนแปลงได้ตลอดตามความเหมาะสม ด้วย โดยในการคัดเลือกโหนด MPR นั้นจะเลือกจากโหนดที่เป็นโหนดข้างเคียงในระยะ 1 hop (One Hop Neighbors) ที่สามารถเชื่อมต่อกับโหนดข้างเคียงในระยะ 2 hop (Two Hop Neighbors) ที่มากที่สุด ซึ่งโหนดข้างเคียงในระยะ 1 hop คือ โหนดที่ตนเองสามารถเชื่อมต่อได้ (โหนดที่อยู่ภายในช่วงคลื่นสัญญาณของตนเอง) แต่โหนดข้างเคียงในระยะ 2 hop คือ โหนดที่ตนเองไม่สามารถเชื่อมต่อได้แต่สามารถเชื่อมต่อโดยผ่านโหนดข้างเคียงในระยะ 1 hop ได้ ซึ่งในกลไกนี้โหนดข้างเคียงในระยะ 2 hop จะต้องมีการเชื่อมต่อแบบสองทิศทาง (Bi-Directional Link) กับโหนดข้างเคียงในระยะ 1 hop เพื่อยืนยันว่าทั้งคู่สามารถสื่อสารโต้ตอบกันได้มิใช่เพียงแต่โหนดข้างเคียงในระยะ 1 hop ส่งข้อมูลไปยังโหนดข้างเคียงในระยะ 2 hop ได้เท่านั้น โดยในงานวิจัยของเราจะนำกลไกการเลือกโหนด MPR มาปรับแก้และนำไปใช้เพื่อให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เข้ากับอัลกอริทึม HELLO เพื่อจะได้มีเวลาที่ใช้ในการค้นหาเกตเวย์ที่ต่ำตามอัลกอริทึม HELLO และมีจำนวนข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งเครือข่ายจำนวนน้อยตามอัลกอริทึมแบบโพรแอกทีฟ โดยข้อมูลที่จะนำมาใช้ในการคำนวณหาโหนด MPR สำหรับอัลกอริทึมที่ได้พัฒนานั้น คือ ข้อมูลโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงของตน โดยข้อมูลดังกล่าวถูกบรรจุอยู่ใน HELLO message แบบดั้งเดิมซึ่งหลักการในการคัดเลือกโหนด MPR ที่ได้พัฒนาขึ้นนั้นได้นำทฤษฎีเซ็ต (Set Theory) เข้ามาช่วย ซึ่งมีการทำงานตามโค้ดเทียมในรูปที่ 1

```
1:   for x in V
2:   assume N = Nx - Nx'
3:        for i in N
4:             for j in N - i
5:                  if Nj ⊆ Ni
6:                       N = N - j
7:                  end
8:             end
9:        end
10:       for i in N
11:            for j in N - i
12:                 Ni,j = Ni,j ∪ (Ni ∩ Nj)
13:            end
14:       end
15:       for i in N
16:            if Ni ⊆ Ni,j
17:                 N = N - i
18:                 Ni,j = Ni,j - Ni
19:            end
20:       end
21:       V = V - (Nx - N)
22:  end
```

รูปที่ 1. แสดงโค้ดเทียมของอัลกอริทึมในการหาโหนด MPR

โดย G = กราฟเชื่อมโยง (Connected Graph) โดยที่ G = (V,E)

V = เซ็ตของโมบายล์โหนด

E = เส้นทางการเชื่อมโยงของแต่ละโมบายล์โหนด

x' = โหนด MPR ก่อนหน้า (Predecessor node)

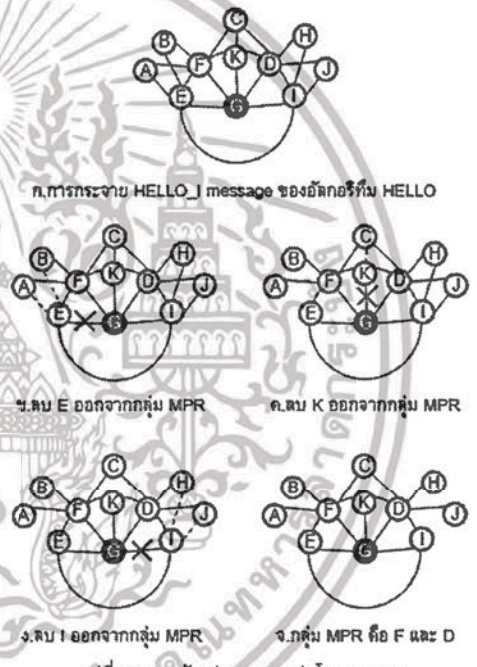
$N_{x \in V}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ของ x ใดๆใน V

$N'_{x \in V}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop ของ x ใดๆที่ไม่มีโหนดที่ก่อให้เกิดเส้นทางที่ซ้ำซ้อน (Redundancy Paths) โดยที่ $N'_{x \in V}$ เป็นเซ็ตย่อยของ $N_{x \in V}$ และทำให้ G' = (V',E') โดยที่ $V' = U_{(x \in V)} N'_x$ หรือกล่าวได้ว่า $N'_{x \in V}$ คือกลุ่มของโหนด MPR

$N_{i,j}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ร่วมของโหนด i และ j โดย $i,j \in N$ และ $i \neq j$

จากโค้ดเทียมในรูปที่ 1 นั้นจะแสดงให้เห็นถึงอัลกอริทึมที่ใช้ในการคำนวณหาโหนด MPR หรือ $N'_{x \in V}$ และรูปที่ 2 แสดงตัวอย่างการหาโหนด MPR โดยการทำงานของอัลกอริทึมสามารถแบ่งออกได้เป็น 2 ขั้นตอนคือ 1) หาความเป็นเซ็ตย่อย (Subset) ของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียง แสดงอยู่ในรูปที่ 1 บรรทัดที่ 3 ถึง 9 และรูปที่ 2 (ข และ ค) และขั้นตอนที่ 2) หาเซ็ตของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงที่เหลือที่ครอบคลุมโหนดข้างเคียงในระดับ 2 hop ของตนมากที่สุด แสดงอยู่ในรูปที่ 1 บรรทัดที่ 10 ถึง 20 และรูปที่ 2(ง) โดยทำการคำนวณในขั้นตอนที่ 2 ซ้ำไปเรื่อยๆจนกว่าจะไม่สามารถคัดเซ็ตใดออกจากการพิจารณาได้อีกซึ่งจะได้ออกมาเป็นเซ็ตของโหนด MPR ซึ่งแสดงให้รูปที่ 2 (จ)

โดยในการคำนวณหาโหนด MPR นั้นจะเริ่มทำการคำนวณจากโหนดเกตเวย์ โดยเมื่อคำนวณเสร็จเรียบร้อยแล้วเกตเวย์จะทำการส่ง HELLO_I message ที่บรรจุข้อมูลเกี่ยวกับโหนด MPR ที่เกตเวย์คำนวณได้ เพื่อระบุว่าโหนดใดเป็นโหนด MPR ไปยังโหนดข้างเคียงในระยะ 1 hop จากนั้นเมื่อโหนดข้องเคียงที่เป็น MPR ได้รับ HELLO_I message ดังกล่าวก็จะทำการคำนวณหาโหนด MPR ของตนต่อไป และส่ง HELLO_I message ไปยังโหนด MPR ที่คำนวณได้ต่อไปเรื่อยๆ พร้อมทั้งบันทึกเส้นทางไปยังเกตเวย์ตามอัลกอริทึม HELLO ที่ได้กล่าวไว้ในส่วนที่ 2 แต่สำหรับโหนดข้างเคียงที่ได้รับ HELLO_I message ไม่ใช่โหนด MPR ก็จะไม่ส่งต่อ HELLO_I message แต่บันทึกเส้นทางไป ยังเกตเวย์เพียงเท่านั้น



รูปที่ 2. แสดงตัวอย่างการหากลุ่มโหนด MPR

ดังนั้นสรุปว่าอัลกอริทึมที่เราได้พัฒนาได้มีการลดโอเวอร์เฮดจากการแลกเปลี่ยน HELLO_I message ของอัลกอริทึม HELLO คือ การลดจำนวนโหนดที่ทำหน้าที่กระจาย HELLO_I message ซึ่งอาจให้เกิดความซ้ำซ้อน ดังรูปที่ 2 (ก) ที่ทุกโหนดต้องทำหน้าที่บรอดแคสต์ข้อความ แต่สำหรับอัลกอริทึมที่เราได้พัฒนาขึ้นโดยขอเรียกว่า HELLOMPR จำมีเพียงบางโหนดที่ทำหน้าที่ในการบรอดแคสต์ ตัวอย่างเช่น ในรูปที่ 2 (ก) ที่ใช้อัลกอริทึม HELLO ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด E และ F เมื่อเปรียบเทียบกับรูปที่ 2 (จ) ที่ใช้อัลกอริทึม HELLOMPR ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด F เท่านั้น

ในส่วนถัดไปจะแสดงการเปรียบเทียบอัลกอริทึมในการค้นหาเกตเวย์ทั้ง 3 รูปแบบ คือ 1)อัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ 2) อัลกอริทึม HELLO และ 3)อัลกอริทึมที่เราได้พัฒนาขึ้นโดยขอเรียกว่า อัลกอริทึม HELLOMPR ผ่านทางโปรแกรมจำลอง OMNET++ ซึ่งใน 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

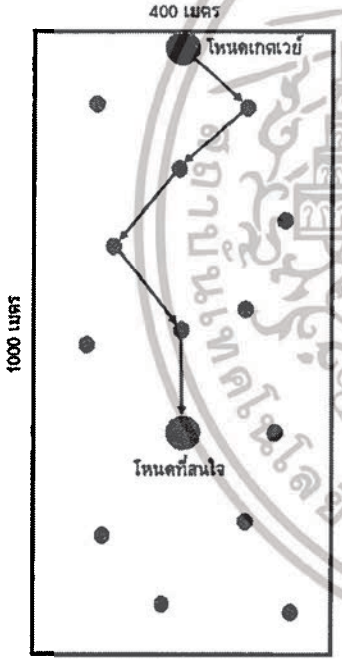
อัลกอริทึมแรกอ้างอิงการทำงานทำงานตามงานวิจัยที่ [8] เพื่อตรวจสอบความถูกต้องของอัลกอริทึมตามสมมติฐาน

4. การทดลองและการประเมินผล

ในการทดลองนั้นนักวิจัยได้ทำการจำลองการทำงานของอัลกอริทึมผ่านโปรแกรมจำลอง OMNET++ ซึ่งเป็นการเปรียบเทียบระหว่างอัลกอริทึมในการค้นหาเกตเวย์ทั้ง 3 รูปแบบ (อัลกอริทึมโพรแอกทีฟ อัลกอริทึม HELLO และอัลกอริทึม HELLOMPR) โดยมีข้อกำหนดเกี่ยวกับเหตุการณ์จำลอง และผลการทดลองเปรียบเทียบดังนี้

4.1 เหตุการณ์จำลองและตัวแปรต่าง ๆ ที่ใช้ในการจำลอง

ในการตรวจสอบและวัดประสิทธิภาพการทำงานของอัลกอริทึมในการค้นหาเกตเวย์ที่ได้กล่าวไปนั้นกำหนดให้การกระจายตัวของโหนดจะกระจายแบบสุ่มอยู่ในเครือข่ายมีพื้นที่ 2 รูปแบบคือ 1) ขนาดกว้าง 400 เมตร และยาว 1,000 เมตร ดังแสดงในรูปที่ 3 และ 2) ขนาดกว้าง 1,000 เมตร และยาว 400 เมตร



รูปที่ 3. แสดงภาพจำลองทอพอโลยีของเครือข่าย

ซึ่งแต่ละโหนดจะไม่มีการเคลื่อนที่ โดยในการทดลองแต่ละครั้งใช้การกระจายแบบสม่ำเสมอ (Uniform Distribution) เพื่อให้โหนดมีการกระจายตัวที่แตกต่างกัน และใช้เพียง ทราฟฟิค (Traffic) สำหรับการสร้างการเชื่อมต่อของโหนดภายในเครือข่ายสื่อสารเฉพาะกิจเท่านั้น โดยจากรูปที่ 3 กำหนดให้โหนดที่เป็นเกตเวย์ (Gateway node) อยู่ทางเหนือสุดของเครือข่าย และกำหนดให้โหนดที่สนใจซึ่งคือ โหนดที่จะต้องได้รับข้อมูลเส้นทางไปยังเกตเวย์ อยู่ห่างจากเกตเวย์ระยะ 600 เมตร โดยที่ทุกโหนดมีระยะในการส่งข้อมูล 250 เมตรรอบตัวโหนด

นอกเหนือจากข้อมูลที่ได้กล่าวไปยังมีตัวแปรต่าง ๆ ที่ได้กำหนดและใช้ในการจำลองเพิ่มเติมดังแสดงในตารางที่ 1

ตารางที่ 1. ตัวแปรต่างๆที่กำหนดในการทดลอง

จำนวนโหนดในเครือข่ายสื่อสารเฉพาะกิจ	15, 60
พื้นที่ของเครือข่าย	400 เมตร × 1,000 เมตร 1000 เมตร × 400 เมตร
ระยะส่งข้อมูลของโหนด	250 เมตร
เวลาทั้งหมดในการทดลอง	300 วินาที
ช่วงเวลาในการส่ง HELLO message	1, 5, 10, 15, 20, 25, 30
ระยะทางระหว่างโหนดเกตเวย์และโหนดที่สนใจ	600 เมตร
จำนวนรอบที่ใช้ในการทดลอง	100 รอบ (15 โหนด) 100 รอบ (60 โหนด)

4.2 ตัวชี้วัดและผลการทดลอง

ในการวัดผลการทดลองนั้นจะทำการเปรียบเทียบระหว่างอัลกอริทึมในการค้นหาเส้นทางไปยังเกตเวย์ดังนี้ คือ อัลกอริทึมโพรแอกทีฟ อัลกอริทึม HELLO และอัลกอริทึม HELLOMPR ซึ่งมีตัวชี้วัดที่ใช้ในการทดลองคือ 1) จำนวนของข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบ และ 2) เวลาที่ใช้ในการค้นหาเกตเวย์ เนื่องจากในการพัฒนาอัลกอริทึมนี้เป็นการพัฒนาเพื่อลดจำนวนข้อความที่ถูกส่งภายในเครือข่ายและยังสามารถคงสภาพเวลาที่ใช้ในการค้นหาเกตเวย์เพื่อให้เหมาะสำหรับการใช้งานในสถานการณ์ภัยพิบัติ

ในรูปที่ 4 รูปที่ 5 และตารางที่ 2 แสดงให้เห็นถึงผลลัพธ์ของการทดลองในตัวชี้วัดด้านจำนวนข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบ สำหรับเครือข่ายที่มีความหนาแน่นของโหนดจำนวน 15 โหนดและ จำนวน 60 โหนดตามลำดับ ซึ่งจะเห็นได้ว่าอัลกอริทึมแบบโพรแอกทีฟมีการส่งข้อความเกี่ยวกับ เกตเวย์ภายในเครือข่ายเป็นจำนวนน้อยที่สุด เนื่องจากโพรโทคอลที่นำมาพัฒนาให้ใช้อัลกอริทึมนี้คือโพรโทคอล OLSR ซึ่งมีกลไกในการลดจำนวนโหนดที่ใช้ในการส่งข้อมูลเส้นทาง แต่ในทางกลับกันอัลกอริทึม HELLO นั้นมีจำนวนข้อความที่ส่งในเครือข่ายมากที่สุด เนื่องจากกลไกในการส่งข้อความเส้นทางนั้นทุกโหนดในเครือข่ายจะมีส่วนร่วมในการบรอดแคสต์ทุกโหนด

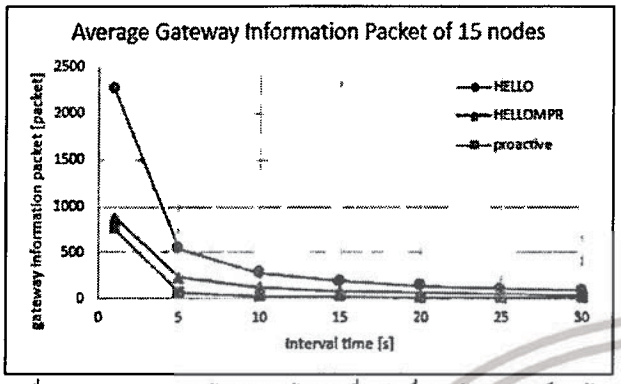
และจากผลลัพธ์สำหรับอัลกอริทึม HELLOMPR นั้นแสดงให้เห็นว่ามีจำนวนข้อความในระบบน้อยกว่าอัลกอริทึม HELLO แบบดั้งเดิมก่อนพัฒนา ซึ่งจากในตารางที่ 2 จะเห็นได้ว่าต่ำประมาณ 2 เท่า เนื่องจากได้มีการนำกลไกในการลดจำนวนโหนดที่ใช้ในการ ส่งข้อมูลเส้นทางของโพรโทคอล OLSR เข้ามาเป็นกลไกเพิ่มเติม แต่ทั้งนี้เองอัลกอริทึม HELLOMPR ก็ยังมีจำนวนข้อความที่มากกว่าอัลกอริทึมแบบโพรแอกทีฟอยู่ดี เนื่องจากอัลกอริทึม HELLOMPR นั้นแต่เดิมถูกพัฒนามาจากโพรโทคอล AODV ที่เป็นโพรโทคอลแบบรีแอกทีฟ

ในรูปที่ 6 รูปที่ 7 และตารางที่ 3 นั้นแสดงให้เห็นถึงผลลัพธ์ของการทดลองในตัวชี้วัดด้านเวลาที่ใช้ในการค้นหาเกตเวย์ (Gateway Discovery Time) สำหรับเครือข่ายที่มีโหนดจำนวน 15 โหนดและจำนวน 60 โหนดตามลำดับ โดยจะเริ่มจับเวลาตั้งแต่เกตเวย์เริ่มประกาศข้อมูลเกี่ยวกับเส้นทางจนกระทั่งถึงเวลาที่โหนดที่สนใจรู้เส้นทางในการติดต่อไปยังเกตเวย์

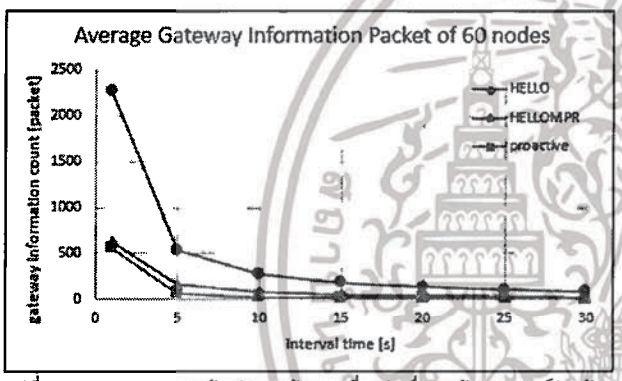
ซึ่งเห็นได้ชัดเจนว่าอัลกอริทึมแบบโพรแอกทีฟนั้นมีเวลาที่ใช้ในการค้นหาเกตเวย์เป็นครึ่งหนึ่งของช่วงเวลาในการส่งข้อความ ซึ่งถ้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ช่วงเวลาดังกล่าวเพิ่มขึ้นเวลาที่ใช้ในการค้นหาเกตเวย์ก็จะเพิ่มขึ้นจนกระทั่งสูงมาก ๆ ไม่ว่าจะเป็นเครือข่ายที่มีจำนวนโหนด 15 โหนด หรือ 60 โหนดก็ตาม



รูปที่ 4. แสดงผลการทดลองด้านจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์สำหรับโหนดจำนวน 15 โหนด



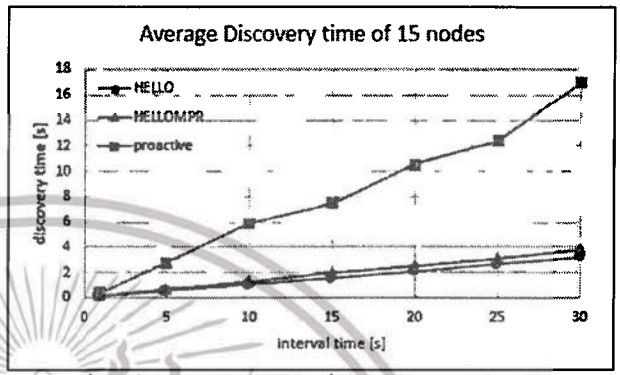
รูปที่ 5. แสดงผลการทดลองด้านจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด

ตารางที่ 2. ผลการทดลองสำหรับจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์

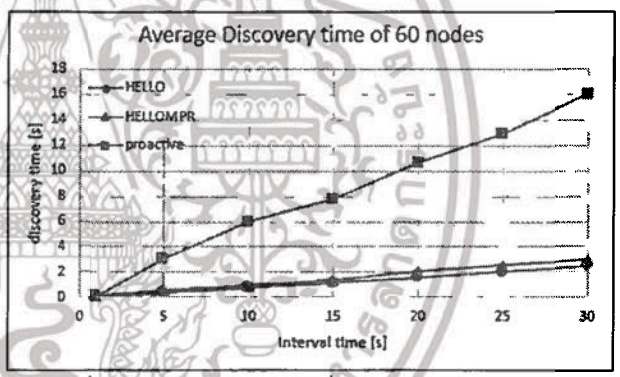
	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	764.679 packet	31.432 packet	12 packet
HELLO	2270.706 packet	277.093 packet	88.7103 packet
HELLOMPR	883.861 packet	124.876 packet	37.284 packet
60 nodes			
proactive	558.348 packet	31.384 packet	10 packet
HELLO	2269.694 packet	275.809 packet	87.39 packet
HELLOMPR	628.5188 packet	87.445 packet	27.771 packet

ส่วนอัลกอริทึม HELLO ถึงแม้ช่วงเวลาของการส่งข้อความมากขึ้น แต่เวลาที่ใช้ในการค้นหาเกตเวย์เพิ่มขึ้นเพียงเล็กน้อย ในตารางที่ 3 จะเห็นได้ว่าเครือข่ายที่มีความหนาแน่นสูงหรือมีโหนดจำนวน 60 โหนดมีเวลาเฉลี่ยที่ใช้ในการค้นหาที่ต่ำกว่าเครือข่าย ที่มีความหนาแน่นน้อยๆ

และอัลกอริทึม HELLOMPR เมื่อช่วงเวลาในการส่งข้อความเพิ่มขึ้นก็มีเวลาที่ใช้ในการค้นหาเกตเวย์เพิ่มเพียงเล็กน้อยเช่นเดียวกับอัลกอริทึม HELLO แต่เมื่อเทียบกับอัลกอริทึม HELLO แล้วยังมีเวลาที่ใช้ในการค้นหาเกตเวย์มากกว่าเล็กน้อยดังตารางที่ 3 เพราะผลของกลไกการเลือกโหนดบรอดแคสต์ทำให้บางครั้งโหนดที่สนใจจะได้รับ HELLO_I message ช้ากว่าในกรณีที่โหนดที่สนใจนั้นอยู่ใกล้กับโหนดที่ไม่ได้ถูกเลือกให้บรอดแคสต์มากกว่าโหนดที่ถูกเลือกให้บรอดแคสต์ ดังนั้นโหนดที่สนใจจึงได้รับ HELLO_I message ช้ากว่าอัลกอริทึม HELLO อีกทั้งยังมีเรื่องของระยะห่างระหว่างโหนดที่บรอดแคสต์และโหนดที่สนใจที่แตกต่างกันอีกด้วย



รูปที่ 6. แสดงผลการทดลองด้านเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับโหนดจำนวน 15 โหนด



รูปที่ 7. แสดงผลการทดลองด้านเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด

ตารางที่ 3. ผลการทดลองสำหรับเวลาเฉลี่ยที่ใช้ในการค้นหาเกตเวย์

	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	0.4s	5.862s	16.96s
HELLO	0.126s	1.027s	3.222s
HELLOMPR	0.197s	1.277s	3.832s
60 nodes			
proactive	0.094s	5.976s	16.1s
HELLO	0.108s	0.787s	2.509s
HELLOMPR	0.167s	0.967s	2.978s

โดยสรุปแล้วจากผลลัพธ์ของการทดลอง 100 ครั้งของเครือข่ายทั้ง 2 ขนาด โดยที่แต่ละการทดลองมีรูปแบบการกระจายของโหนดที่แตกต่างกัน ซึ่งโหนดมีการกระจายสุ่มแบบยูนิฟอร์ม ซึ่งผลที่ได้จากทั้ง 2 เครือข่ายมีใกล้เคียงกัน (แตกต่างกันเฉลี่ยเพียง 7% - 8%) และได้ค่าเฉลี่ยของผลลัพท์ดังกราฟในรูปที่ 4 ถึง 7 โดยมีความแปรปรวน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เท่ากับ 0.0271, 0.0294และ 0.0172 สำหรับผลของอัลกอริทึม HELLO HELLOMPR และโพรแอกทีฟตามลำดับ ในการค้นหาเกตเวย์ของอัลกอริทึมโพรแอกทีฟมีการส่งข้อความเกี่ยวกับเกตเวย์ในเครือข่ายจำนวนน้อยที่สุด ในเครือข่ายที่มีความหนาแน่นทั้ง 15 โหนด และ 60 โหนด แต่สำหรับเวลาในการค้นหาเกตเวย์นั้นมีอัตราที่สูงกว่าเมื่อเทียบกับอัลกอริทึม HELLO แม้ช่วงเวลาในการส่งข้อความจะเพิ่มขึ้นก็ตาม

แต่อย่างไรก็ตามจำนวนการส่งข้อความของอัลกอริทึม HELLO เกี่ยวกับเกตเวย์กลับมีจำนวนมากเมื่อเทียบกับอัลกอริทึมแบบโพรแอกทีฟ ซึ่งอัลกอริทึม HELLOMPR นั้นมีการส่งข้อความเกี่ยวกับเกตเวย์เป็นจำนวนน้อยใกล้เคียงกับอัลกอริทึมโพรแอกทีฟและใช้เวลาในการค้นหาเกตเวย์น้อยใกล้เคียงกับอัลกอริทึม HELLO ทั้งเครือข่ายที่มีความหนาแน่นจำนวนของโหนด 15 โหนด และ 60 โหนด หรืออาจบอกได้ว่าอัลกอริทึม HELLOMPR นั้นได้รวมเอาข้อดีในด้านการส่งข้อมูลเส้นทางเกี่ยวกับเกตเวย์ที่มีจำนวนน้อยของอัลกอริทึมแบบโพรแอกทีฟ และนำเอาข้อดีในด้านเวลาในการค้นหาเกตเวย์ที่ต่ำของอัลกอริทึม HELLO เข้าด้วยกัน

5. สรุปผล

ในงานวิจัยนี้เราได้พัฒนาอัลกอริทึมในการค้นหาเกตเวย์สำหรับเครือข่ายสื่อสารเฉพาะกิจโดยมีพื้นฐานมาจากโพรโทคอล AODV ซึ่งได้นำหลักการในการคัดเลือกโหนด MPR จากโพรโทคอล OLSR และทฤษฎีเซ็ตมาใช้เพื่อเพิ่มประสิทธิภาพโดยการลดจำนวนข้อมูลที่ส่งต่อภายในเครือข่าย

จากผลการทดลองและการประเมินผลในส่วนที่ 4 ของงานวิจัยนี้สามารถสรุปผลได้ว่าเครือข่ายที่ใช้อัลกอริทึม HELLOMPR ที่ได้พัฒนาขึ้นนั้นมีจำนวนของข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบน้อยกว่าเครือข่ายที่ใช้อัลกอริทึม HELLO จนเข้าใกล้อัลกอริทึมแบบโพรแอกทีฟในการค้นหาเกตเวย์ เป็นผลจากการลดจำนวนโหนดที่ต้องบรอดแคสต์ข้อมูลที่ใช้ในการค้นหาเกตเวย์ และยังส่งผลให้โหนดในเครือข่ายมีพลังงานและอยู่ในระบบได้นานขึ้น เพราะทุกโหนดไม่จำเป็นต้องบรอดแคสต์ข้อมูลเส้นทางที่เกี่ยวข้องกับเกตเวย์จึงทำให้ไม่เสียพลังงานไปโดยเปล่าประโยชน์ และจากผลการทดลองเกี่ยวกับเวลาที่ใช้ในการทำให้โหนดที่สนใจรับจักเส้นทางไปยังเกตเวย์จะเห็นได้ว่าอัลกอริทึมที่พัฒนามิได้ลดประสิทธิภาพของอัลกอริทึม HELLO ก่อนพัฒนาลงอีกด้วย

ซึ่งในสถานการณ์ภัยพิบัตินั้นมีความจำกัดทางด้านแหล่งพลังงานของโมบายล์โหนด (จากแบตเตอรี่) ดังนั้นอัลกอริทึมที่มีความเหมาะสมคือ อัลกอริทึมแบบโพรแอกทีฟ และอัลกอริทึม HELLOMPR เพราะมีการส่งข้อความเป็นจำนวนน้อยเมื่อเทียบกับอัลกอริทึมแบบ HELLO และเนื่องด้วยการสื่อสารควรสามารถสื่อสารได้อย่างเร่งด่วนดังนั้นอัลกอริทึมที่มีความเหมาะสมมากที่สุดที่สำหรับสภานการณ์ภัยพิบัตินี้คืออัลกอริทึม HELLOMPR เพราะเมื่อเปรียบเทียบเวลาในการค้นหาเกตเวย์ระหว่างอัลกอริทึมแบบโพรแอกทีฟ และโพรโทคอล HELLOMPR จะเห็นได้ว่าอัลกอริทึม HELLOMPR นั้นมีเวลาที่น้อยกว่าตามผลการทดลอง

เอกสารอ้างอิง

[1] T. S. Rappaport. "Wireless Communications Principles & Practice." Upper Saddle River, New Jersey: Prentice-Hall, Inc.1996

[2] T. Lin. "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications." Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the Ph.D. in Computer Engineering. 2004

[3] Wireless Embedded Systems, Computer Science Department, University of California at Berkeley, "Self-organized wireless sensor network." August, 2001.
Available :http://webs.cs.berkeley.edu/800demo

[4] K.Gorantala. "Routing Protocols in Mobile Ad-hoc Networks" Master's Thesis in Computing Science at Ume°a University. June 15, 2006

[5] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)." Internet Engineering Task Force (IETF) draft, February 2007. [Online]
Available :http://datatracker.ietf.org/doc/rfc4728/

[6] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing." Internet Engineering Task Force (IETF) draft, July 2003.[Online]
Available :http://datatracker.ietf.org/doc/rfc3561/

[7] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol (OLSR)." Internet Engineering Task Force(IETF) draft, October 2003.[Online]
Available :https://datatracker.ietf.org/doc/rfc3626/

[8] M. Rosenschon. "Internet Gateway Discovery for Mobile Ad Hoc Networks" Submitted for the Degree of Doctor of Philosophy School of Engineering and Mathematical Sciences CITY University London. 2 October 2007

[9] J. Broch, et al. "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks" International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN99), Workshop on Mobile Computing, Perth, Western Australia. June 1999

[10] M. Rosenschon, T. Manz, J. Habermann, V. Rakocevic. "Gateway Discovery Algorithm for Ad-Hoc networks using HELLO Messages" International Workshop on Wireless Ad Hoc Networks IWWAN 2005, London. May 2005.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[11] H. Luo, R. Ramjeey, P. Sinhaz, L. Liy, S. Lu "UCAN: A Unified Cellular and AdHoc Network Architecture" MobiCom'03, San Diego, California, USA, September 2003.



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กลไกค้นหาเกตเวย์ที่มีโอเวอร์เฮดจากการแลกเปลี่ยนข้อความต่ำ สำหรับเครือข่ายเคลื่อนที่เฉพาะกิจ

Gateway Discovery Mechanism with Low Message Exchange Overhead for Mobile Ad Hoc Networks

สุเมธ ประภาวัต(Sumet Prabhavat) สารัช ศรีสวัสดิ์พงษ์ (Sarach Sriswadpong)

ทะนง ชูวณิชชานนท์ (Tanong Chuvanitchanon) วรวัชร ฉรงคะชวนะ(Worrawat Narongkhachavana)

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

sumet@it.kmitl.ac.th, acecharmil@gmail.com, tanong3200@hotmail.com, worravat@gmail.com

บทคัดย่อ

ในการค้นหาเกตเวย์เพื่อให้เครือข่ายเคลื่อนที่เฉพาะกิจติดต่อกับเครือข่ายภายนอกหรืออินเตอร์เน็ตได้ โอเวอร์เฮดที่เกิดจากการแลกเปลี่ยนข้อมูลระหว่างโหนดเพื่อการค้นหาเกตเวย์ และเวลาที่ต้องใช้ในการค้นหาเป็นปัจจัยที่ลดทอนประสิทธิภาพเครือข่ายอย่างหลีกเลี่ยงไม่ได้ ในงานวิจัยก่อนหน้านี้พยายามแก้ไขปัญหาดังกล่าว เช่น กลไกในโพรโทคอล AODV ที่ใช้เวลาในการค้นหาเกตเวย์น้อย แต่ก็ทำให้เกิดโอเวอร์เฮดมาก เมื่อเทียบกับกลไกในโพรโทคอล OLSR ที่มีโอเวอร์เฮดต่ำ แต่ก็ใช้เวลาในการค้นหานาน บทความนี้จึงเสนอกลไกที่สามารถค้นหาเกตเวย์ได้โดยมีโอเวอร์เฮดต่ำ และใช้เวลาในการค้นหาน้อย ซึ่งพิสูจน์ได้โดยการจำลองการทำงานและเปรียบเทียบกับกลไกค้นหาเกตเวย์จากงานวิจัยก่อนหน้าในสภาวะที่โหนดเคลื่อนที่แบบสุ่ม และมีพารามิเตอร์การจำลองที่แตกต่างกันออกไป

คำสำคัญ: เครือข่ายเคลื่อนที่เฉพาะกิจ การค้นหาเกตเวย์ โอเวอร์เฮด การแลกเปลี่ยนข้อมูลเพื่อหาเกตเวย์

Abstract

A gateway discovery mechanism on mobile ad hoc network (MANET) is applicable for connecting MANET to other networks or the Internet. However, it causes message exchange overhead and gateway discovery time (leading to network delay), which degrade network performance significantly. These issues have been addressed by previous works: A gateway discovery mechanism in a modified AODV takes short time to find a gateway but causes high overhead whereas that in a modified version of OLSR needs only a few number of message exchanges but requires long discovery time. This paper proposes an improved gateway discovery mechanism that can reduce message exchange overhead while maintains low gateway discovery time. Performance evaluations are conducted using simulations with different parameters and random waypoint mobility model.

Keyword: Mobile Ad Hoc Network, Gateway Discovery, Message Exchange Overhead

1. บทนำ

จากเทคโนโลยีด้านการสื่อสารที่มีการพัฒนาไปอย่างรวดเร็วอันส่งผลให้เกิดนวัตกรรมใหม่ ๆ เกิดขึ้น เช่น การสื่อสารแบบไร้สาย และมีการใช้งานกันอย่างแพร่หลายซึ่งการสื่อสารกลายเป็นสิ่งสำคัญในการดำเนินชีวิตของมนุษย์ไปแล้ว ทั้งนี้เองหากเกิดสถานการณ์ที่เกิดภัยพิบัติหรือเหตุการณ์ไม่คาดฝันซึ่งทำให้การติดต่อสื่อสารระหว่างโมบายล์โหนดกับโครงสร้างพื้นฐานถูกตัดขาด ส่งผลให้ไม่สามารถติดต่อสื่อสารและขอความช่วยเหลือจากบุคคลอื่น ๆ ได้ จากปัญหาดังกล่าวจึงมีนักวิจัยหลายกลุ่มพยายามพัฒนาเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด (MANET : Mobile Ad-hoc Network) [1] ซึ่งทำให้โมบายล์โหนดสามารถติดต่อสื่อสารกันได้โดยไม่ต้องพึ่งพาโครงสร้างพื้นฐาน

แต่การเชื่อมต่อกันเพียงในเครือข่ายเฉพาะกิจดังกล่าวทำให้เกิดปัญหาการจำกัดทางด้านขอบเขตของเครือข่าย และจากที่กล่าวมาการที่โมบายล์โหนดทำหน้าที่เป็นผู้ส่งต่อข้อมูลให้โหนดอื่น ๆ นั้นทำให้มีการใช้พลังงานสำหรับทำหน้าที่ดังกล่าวนอกเหนือจากเพื่อการส่งข้อมูลของตนเอง อันส่งผลให้เกิด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปัญหาในการใช้พลังงานที่มีอยู่อย่างจำกัด (จากแบตเตอรี่) ของโมบายล์โหนด

จากปัญหาที่กล่าวมาผู้จัดทำจึงศึกษารูปแบบการหาเส้นทางให้สามารถหาเส้นทางเชื่อมต่อที่ผ่านเกตเวย์ออกไปยังโครงสร้างพื้นฐานได้บนเครือข่ายเฉพาะกิจของโมบายล์โหนด (อย่างเช่น เครือข่ายอินเตอร์เน็ต) เพื่อแก้ไขปัญหาด้านการจำกัดขอบเขตเครือข่าย ซึ่งทำให้ติดต่อสื่อสารออกไปนอกพื้นที่ได้ และลดการใช้พลังงานที่มีอยู่อย่างจำกัดของโมบายล์โหนดให้ทำงานได้นานขึ้น ไปจนกระทั่งลดโอกาสเกิดความไม่ต่อเนื่องในเครือข่าย

2. ทฤษฎีและงานที่เกี่ยวข้อง

โพรโทคอลค้นหาเส้นทาง (Routing Protocols) ในเครือข่ายสื่อสารเฉพาะกิจถูกแบ่งเป็น 3 กลุ่ม [2] คือ 1) โพรโทคอลค้นหาเส้นทางแบบรีแอกทีฟ (Reactive Routing Protocols) ซึ่งค้นหาเส้นทางเมื่อต้องการส่งข้อมูล เช่น โพรโทคอลเอโอดีวี (AODV : Ad hoc On-Demand Distance Vector) [4] และโพรโทคอลดีเอสอาร์ (DSR : Dynamic Sort Routing) [3] 2) โพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ (Proactive Routing Protocols) ทำการค้นหาเส้นทางไปยังทุกปลายทางที่เป็นไปได้ก่อนที่จะมีการส่งข้อมูล เช่น โพรโทคอลโอแอลเอสอาร์ (OLSR : Optimized Link State Routing) [5] และสุดท้าย 3) โพรโทคอลค้นหาเส้นทางแบบไฮบริดจ์ (Hybrid Routing Protocols) ซึ่งมีการทำงานผสมผสานระหว่างโพรโทคอลค้นหาเส้นทางทั้ง 2 แบบก่อนหน้า

โดยมีงานวิจัยที่ได้ศึกษาการเชื่อมต่อระหว่างเครือข่ายเฉพาะกิจของโมบายล์โหนดกับเครือข่ายอื่น ๆ เช่น เครือข่ายโทรศัพท์ (Cellular Network) [10] เครือข่ายอินเทอร์เน็ต [6],[7],[8] โดยใช้การค้นหาโหนดเกตเวย์ในการเชื่อมต่อระหว่างเครือข่ายสื่อสารเฉพาะกิจและเครือข่ายอินเทอร์เน็ตหรือเครือข่ายอื่น ๆ ซึ่งเกตเวย์มีหน้าที่เป็นตัวกลางในการเชื่อมต่อ

จากการศึกษางานวิจัยที่เกี่ยวข้องกับการค้นหาเกตเวย์ มีการนำโพรโทคอลค้นหาเส้นทาง AODV [6],[8] มาปรับแก้รูปแบบและการส่งของข้อความ (Message) จากที่กำหนดใน RFC [4] โดยแก้ไข HELLO messages ที่ใช้เพื่อบอกถึงการมีตัวตนของตนเองกับโหนดรอบข้างโดยการบรอดแคสต์ซึ่งถูกส่งก็ต่อเมื่อโหนดนั้น ๆ ยังไม่มีการส่งคำร้องขอเส้นทาง (Route Request) การตอบกลับเส้นทาง (Route Reply) โดยในการปรับแก้รูปแบบข้อความนั้นได้ทำการเพิ่มแฟล็ก (Flag) พิเศษ ที่เรียกว่าแฟล็ก I (I-flag) เพื่อระบุว่าเป็น HELLO message ที่ส่งมาจากเกตเวย์ และบันทึกแอดเดรสของเกตเวย์ (Gateway Address) ใน HELLO message ด้วยเพื่อระบุว่าถูกสร้างมาจากเกตเวย์โหนดใด ขั้นตอนในการส่ง HELLO_I นั้นจะเริ่มส่งจากโหนดเกตเวย์เพื่อบอกถึงการมีอยู่ของโหนดเกตเวย์ให้ทุกโหนดที่อยู่ภายในช่วงคลื่นสัญญาณของเกตเวย์รับรู้ผ่านการรับ HELLO_I (จากการบรอดแคสต์ HELLO_I ของเกตเวย์) จากนั้นโหนดที่ได้รับ HELLO_I จะทำการการบันทึกเส้นทางที่สามารถไปยังเกตเวย์ และบรอดแคสต์ (Rebroadcast) HELLO_I ซ้ำออกไป แต่ถ้าโหนดใดไม่ได้รับ HELLO_I ในช่วงระยะเวลาของการส่ง HELLO messages (HELLO interval) โหนดนั้นก็จะทำการส่ง HELLO messages แบบปกติที่ไม่มีการปรับแก้แทน ซึ่งขอเรียกการค้นหาเส้นทางไปยังเกตเวย์นี้ว่า อัลกอริทึม HELLO และภายในงานวิจัยดังกล่าวนักวิจัยได้ทำการเปรียบเทียบอัลกอริทึม HELLO กับอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ และแบบรีแอกทีฟ โดยผลสรุปคือ อัลกอริทึม HELLO มีเวลาที่ใช้ในการค้นหาเกตเวย์ที่น้อยกว่าเมื่อเปรียบเทียบกับอัลกอริทึมทั้งสอง

โดยสำหรับโพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ [8] เมื่อโหนดได้รับข้อมูลเกี่ยวกับเกตเวย์จะตัดสินใจว่าจะรับหรือทิ้งข้อมูลนั้น โดยจะรับข้อมูลนั้นก็ต่อเมื่อโหนดไม่รู้เส้นทางไปยังเกตเวย์หรือข้อมูลนั้นมีเส้นทางที่สั้นกว่าหรือข้อมูลนั้นมาจากแหล่งกำเนิดเดียวกันแต่มีความใหม่กว่า (มี sequence number ที่มากกว่า) และถ้าหากโหนดเลือกรับข้อมูลเส้นทางก็จะหยุดการร้องขอเส้นทาง จากนั้นจึงทำการตั้งค่าหรือปรับปรุงเส้นทางไปยังเกตเวย์ตามข้อมูลที่ได้รับมา และส่งต่อไปยังโหนดอื่น ๆ

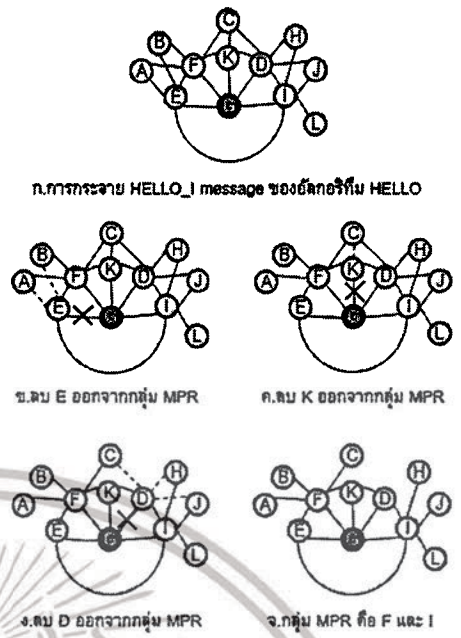
3. แนวคิดและการดำเนินงาน

จากงานวิจัยในส่วนที่ 2 เห็นได้ว่าอัลกอริทึม HELLO มีเวลาในการทำให้แต่ละโหนดรับรู้เส้นทางเชื่อมต่อไปยังเกตเวย์น้อยที่สุดเมื่อเทียบกับอัลกอริทึมอื่นๆ [8] แต่ยังมีข้อเสียเรื่องโอเวอร์เฮดเพราะทุกโหนดต้องทำการบรอดแคสต์ข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
1:    for x in V
2:    assume N = Nx - Nx'
3:          for i in N
4:                for j in N - i
5:                      if Nj ⊆ Ni
6:                            N = N - j
7:                      end
8:                end
9:          end
10:         for i in N
11:               for j in N - i
12:                     Ni,j = Ni,j ∪ (Ni ∩ Nj)
13:               end
14:         end
15:         for i in N
16:               if Ni ⊆ Ni,j
17:                     N = N - i
18:                     Ni,j = Ni,j - Ni
19:               end
20:         end
21:         V = V - (Nx - N)
22:   end
```

ภาพที่ 1: แสดงโค้ดเทียมของอัลกอริทึมในการหาโหนด MPR



ภาพที่ 2: แสดงตัวอย่างการหากลุ่มโหนด MPR

ในงานวิจัยนี้จึงนำอัลกอริทึม HELLO มาเพิ่มกลไกเพื่อลดจำนวนการบรอดแคสต์ข้อมูลเส้นทางที่เกี่ยวข้องกับเกตเวย์ด้วยวิธีการลดจำนวนโหนดที่ทำการบรอดแคสต์ ซึ่งกลไกนี้ถูกใช้ในโพรโทคอลค้นหาเส้นทาง OLSR เรียกว่าการเลือกโหนดเอ็มพีอาร์ (MPR: Multipoint Relays Selection) โดยมีหน้าที่ในการส่งต่อข้อมูล (Retransmission) โดยโหนดที่เริ่มต้นบรอดแคสต์นั้นจะมีทำหน้าที่ในการคัดเลือกโหนด MPR หรือเป็น MPR Selector ซึ่งโหนด MPR จะอยู่ในกลุ่มของโหนดข้างเคียง (Neighbor nodes) แต่ทุกโหนดที่เป็นโหนดข้างเคียงไม่จำเป็นต้องเป็นโหนด MPR ซึ่ง สามารถเปลี่ยนแปลงได้ตลอดตามความเหมาะสม ในการคัดเลือกโหนด MPR นั้นโหนด MPR Selector จะเลือกจากกลุ่มโหนดข้างเคียงในระยะ 1 hop (One Hop Neighbors) ของตนที่สามารถเชื่อมต่อกับโหนดข้างเคียงในระยะ 2 hop (Two Hop Neighbors) ของตนที่มากที่สุด ซึ่งโหนดข้างเคียงในระยะ 1 hop คือ โหนดที่ตนเองสามารถเชื่อมต่อได้ (โหนดที่อยู่ภายในช่วงคลื่นสัญญาณของตนเอง) แต่โหนดข้างเคียงในระยะ 2 hop คือ โหนดที่ตนเองไม่สามารถเชื่อมต่อได้แต่สามารถเชื่อมต่อผ่านโหนดข้างเคียงในระยะ 1 hop ได้ โดยมีงานวิจัยบางส่วนได้นำเอากลไกการเลือกโหนด MPR มาประยุกต์เข้ากับกลไกการแลกเปลี่ยน HELLO messages บนโพรโทคอล AODV [11] ซึ่งมีความแตกต่างกับงานวิจัยของเราเนื่องจากผู้จัดทำได้ทำการออกแบบกลการคัดเลือกโหนด MPR และกลไกการทำงานของโหนด MPR ขึ้นเอง ซึ่งแต่ละกลไกมีการทำงานดังนี้ กลการคัดเลือกโหนด MPR จะทำโดยการแลกเปลี่ยน HELLO message เพื่อเรียนรู้โหนดข้างเคียงในระยะ 1 hop และโหนดข้างเคียงในระยะ 2 hop ของทุกโหนดข้างเคียงในระยะ 1 hop จากนั้นจะนำข้อมูลดังกล่าวที่เรียนรู้มาทำการคัดเลือกโหนด MPR ซึ่งมีการทำงานตามโค้ดเทียมในภาพที่ 1

โดย G = กราฟเชื่อมโยง โดยที่ G = (V,E)

V = เซ็ตของโมบายล์โหนด

E = เส้นทางการเชื่อมโยงของแต่ละโมบายล์โหนด

x' = โหนด MPR ก่อนหน้า (Predecessor node)

$N_x \in V$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ของ x ใดๆใน V

$N'_x \in V$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop ของ x ใดๆที่ไม่มีโหนดที่ก่อให้เกิดเส้นทางที่ซ้ำซ้อน (Redundancy Paths) โดยที่ $N'_x \in V$ เป็นเซ็ตย่อยของ $N_x \in V$ และทำให้ G' = (V',E') โดยที่ $V' = U(x \in V)N'_x$ หรือกล่าวได้ว่า $N'_x \in V$ คือกลุ่มของโหนด MPR

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$N_{i,j}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ร่วมของโหนด i และ j โดย $i,j \in N$ และ $i \neq j$

จากโค้ดเทียมในภาพที่ 1 แสดงถึงอัลกอริทึมที่ใช้ในการคำนวณหาโหนด MPR หรือ $N'x \in V$ และภาพที่ 2 แสดงตัวอย่างการหาโหนด MPR โดยการทำงานของอัลกอริทึมแบ่งออกได้เป็น 2 ขั้นตอน 1) หาความเป็นเซ็ตย่อย (Subset) คือ หาเซ็ตของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงที่เหลือที่ครอบคลุมโหนดข้างเคียงในระดับ 2 hop ที่เหมือนกันกันหรือน้อยกว่า แสดงอยู่ในภาพที่ 1 บรรทัดที่ 3 ถึง 9 และภาพที่ 2(ข และ ค) และ 2) หาเซ็ตของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงที่เหลือที่ครอบคลุมโหนดข้างเคียงในระดับ 2 hop ของตนมากที่สุด แสดงอยู่ในภาพที่ 1 บรรทัดที่ 10 ถึง 20 และภาพที่ 2(ง) โดยทำขั้นตอนที่ 2) ซ้ำจนกว่าจะไม่สามารถตัดเซ็ตใดออกจากการพิจารณาได้อีกซึ่งจะผลเป็นเซ็ตของโหนด MPR ซึ่งแสดงให้ภาพที่ 2(จ)

และสำหรับกลไกการทำงานของโหนด MPR จะระบุให้โหนดที่กำลังส่งข้อมูลเกตเวย์ขณะนั้นจะเป็นผู้เลือกโหนด MPR โดยใช้กลไกการเลือกโหนด MPR ที่ได้กล่าวไว้ข้างต้น ดังนั้นคำนวณหาโหนด MPR นั้นจึงเริ่มต้นคำนวณจากโหนดเกตเวย์เมื่อคำนวณเสร็จเกตเวย์จะทำการส่ง HELLO_I message ที่บรรจุข้อมูลเพื่อระบุว่าโหนดใดเป็นโหนด MPR ไปยังโหนดข้างเคียงในระยะ 1 hop จากนั้นเมื่อโหนดข้างเคียงที่เป็น MPR ได้รับ HELLO_I message ดังกล่าวก็จะทำการคำนวณหาโหนด MPR ของตนต่อไป และส่ง HELLO_I message ไปยังโหนด MPR ที่คำนวณได้ต่อไปเรื่อยๆ พร้อมทั้งบันทึกเส้นทางไปยังเกตเวย์ตามอัลกอริทึม HELLO ที่ได้กล่าวไว้ในส่วนที่ 2 แต่สำหรับโหนดข้างเคียงที่ได้รับ HELLO_I message ไม่ใช่โหนด MPR ก็จะไม่ส่งต่อ HELLO_I message แต่บันทึกเส้นทางไป ยังเกตเวย์เท่านั้น

ดังนั้นอัลกอริทึมที่ได้พัฒนาได้มีการลดโอเวอร์เฮดจากการแลกเปลี่ยน HELLO_I message ของอัลกอริทึม HELLO คือทุกโหนดที่ทำหน้าที่บรอดแคสต์ HELLO_I message ซึ่งอาจทำให้เกิดความซ้ำซ้อน ดังภาพที่ 2(ก) ที่ทุกโหนดต้องทำหน้าที่บรอดแคสต์ข้อความ แต่สำหรับอัลกอริทึมที่ได้พัฒนาโดยขอเรียกว่า HELLOMPR จะมีเพียงบางโหนดที่ทำหน้าที่ในการบรอดแคสต์ ตัวอย่างเช่น ในภาพที่ 2(ก) ที่ใช้อัลกอริทึม HELLO ที่โหนด A และ B ได้รับ HELLO_I message จากทั้งโหนด E และ F เมื่อเปรียบเทียบกับภาพที่ 2(จ) ที่ใช้อัลกอริทึม HELLOMPR ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด F เท่านั้น

4. การทดลองและการประเมินผล

ในการทดลองได้ทำการจำลองการทำงานของอัลกอริทึมผ่านโปรแกรมจำลอง OMNET++ ซึ่งเป็นการเปรียบเทียบระหว่างอัลกอริทึมในการค้นหาเกตเวย์ทั้ง 3 ได้แก่ 1) อัลกอริทึมโพรแอกทีฟ 2) อัลกอริทึม HELLO และ 3) อัลกอริทึม HELLOMPR ซึ่งในอัลกอริทึมที่ 1) และ 2) อ้างอิงการทำงานทำงานตามงานวิจัยที่ [6] โดยมีข้อกำหนดเกี่ยวกับเหตุการณ์จำลอง และผลการทดลองเปรียบเทียบดังนี้

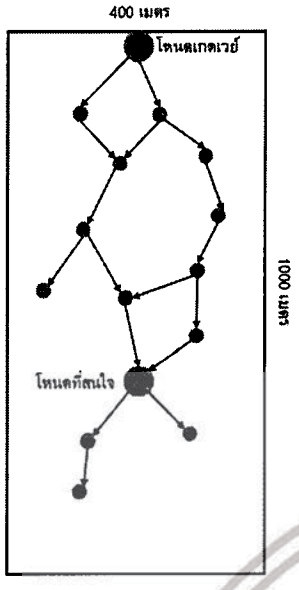
4.1 เหตุการณ์จำลองและตัวแปรต่าง ๆ ที่ใช้ในการจำลอง

กำหนดให้การกระจายตัวของโหนดจะกระจายแบบสุ่มอยู่ในเครือข่ายพื้นที่ขนาดกว้าง 400 เมตร และยาว 1,000 เมตร ดังแสดงในภาพที่ 3 ซึ่งแต่ละโหนดจะเคลื่อนที่ภายใต้ความเร็วสูงสุด 10 เมตร / วินาที โดยในการทดลองแต่ละครั้งใช้การกระจายตัวของโหนดแบบสม่ำเสมอ (Uniform Distribution) เพื่อให้แต่ละการทดลองโหนดมีการกระจายตัวที่แตกต่าง โดยจากภาพที่ 3 กำหนดให้โหนดที่เป็นเกตเวย์ (Gateway node) อยู่บนสุดของเครือข่าย และกำหนดให้โหนดที่สนใจซึ่งคือโหนดที่จะต้องได้รับข้อมูลเส้นทางไปยังเกตเวย์ อยู่ห่างจากเกตเวย์ระยะ 600 เมตร โดยที่ทุกโหนดมีระยะในการส่งข้อมูล 250 เมตรรอบตัวโหนด และมีตัวแปรต่าง ๆ ที่ได้กำหนดและใช้ในการจำลองเพิ่มเติมดังแสดงในตารางที่ 1

ตารางที่ 1: ตัวแปรต่างๆที่กำหนดในการทดลอง

จำนวนโหนดในเครือข่ายสื่อสารเฉพาะกิจ	15, 60
พื้นที่ของเครือข่าย	400 เมตร × 1,000 เมตร
ระยะส่งข้อมูลของโหนด	250 เมตร
เวลาทั้งหมดในการทดลอง	300 วินาที
ช่วงเวลาในการส่ง HELLO message	1, 5, 10, 15, 20, 25, 30
จำนวนรอบที่ใช้ในการทดลอง	100 รอบ (ทั้ง 15,60 โหนด)
รูปแบบการเคลื่อนที่ของโหนด	Random Waypoint
ความเร็วสูงสุดในการเคลื่อนที่	10 เมตร/วินาที

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



ภาพที่ 3: แสดงภาพจำลองทอพอโลยีของเครือข่าย

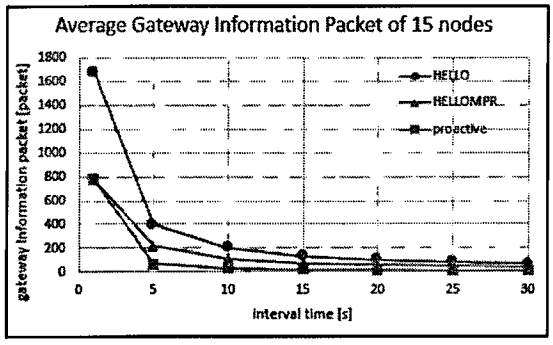
4.2 ผลการทดลองและตัวชี้วัด

สำหรับการทดลองเพื่อเปรียบเทียบระหว่างอัลกอริทึมค้นหาเกตเวย์เราได้เลือกตัวชี้วัดในการทดลองคือ 1) จำนวนของข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบ 2) เวลาที่ใช้ในการค้นหาเกตเวย์

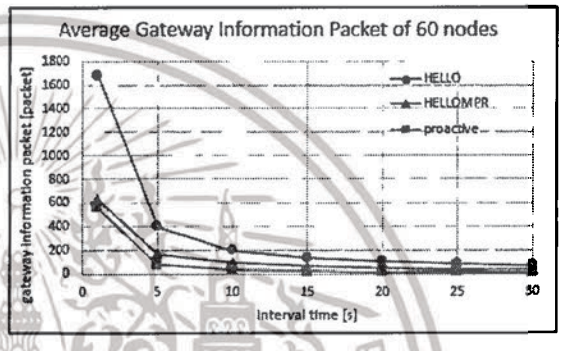
ในภาพที่ 4 ภาพที่ 5 และตารางที่ 2 แสดงให้เห็นถึงผลการทดลองในตัวชี้วัดด้านจำนวนข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ โดยอัลกอริทึม HELLO มีจำนวนข้อความที่ส่งในเครือข่ายมากที่สุด เนื่องจากทุกโหนดต้องทำการบรอดแคสต์ข้อมูลของเกตเวย์ แต่อัลกอริทึม HELLOMPR มีจำนวนน้อยกว่าในอัลกอริทึม HELLO มากเนื่องจากมีกลไกในการลดจำนวนโหนดที่ทำการบรอดแคสต์ แต่อัลกอริทึมแบบโพรแอกทีฟก็ยังมีจำนวนข้อความน้อยที่สุดเนื่องมาจากทุกโหนดจะทราบ topology ของทั้งระบบทำให้สามารถคำนวณหาโหนด MPR ได้อย่างเต็มประสิทธิภาพแต่สำหรับอัลกอริทึมที่ได้พัฒนานั้นทราบเพียงโหนดข้างเคียงในระยะ 1 และ 2 hop

ตารางที่ 2: ผลลัพธ์จำนวนข้อความที่ส่งเพื่อการค้นหาเกตเวย์

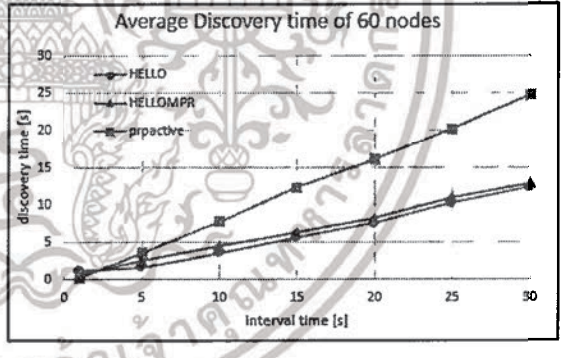
	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	784.443 pkt	31.402 pkt	10 pkt
HELLO	1683.25 pkt	200.39 pkt	66.124 pkt
HELLOMPR	778.248 pkt	110.69 pkt	37.009 pkt
60 nodes			
proactive	558.348 pkt	31.384 pkt	10 pkt
HELLO	1680.24 pkt	192.42 pkt	65.234 pkt
HELLOMPR	628.518 pkt	87.446 pkt	27.771 pkt



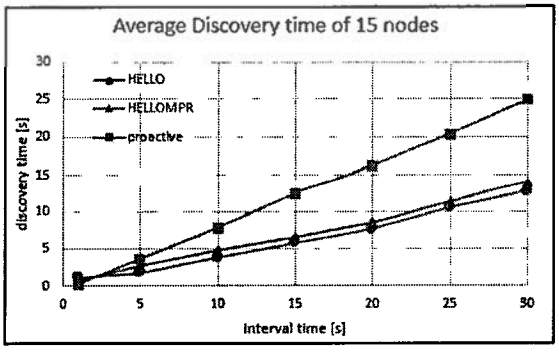
ภาพที่ 4: กราฟจำนวนข้อความที่ใช้เพื่อค้นหาเกตเวย์สำหรับ 15 โหนด



ภาพที่ 5: กราฟจำนวนข้อความที่ใช้เพื่อค้นหาเกตเวย์สำหรับ 60 โหนด



ภาพที่ 6: กราฟเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับจำนวน 15 โหนด



ภาพที่ 7: กราฟเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับจำนวน 60 โหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3: ผลลัพธ์เวลาเฉลี่ยที่ใช้ในการค้นหาเกตเวย์

	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	0.231s	7.741s	24.83s
HELLO	1.148s	3.757s	12.69s
HELLOMPR	0.717s	4.677s	13.91s
60 nodes			
proactive	0.221s	7.727s	24.74s
HELLO	1.015s	3.532s	12.34s
HELLOMPR	0.621s	4.391s	12.89s

ในภาพที่ 6 ภาพที่ 7 และตารางที่ 3 แสดงผลลัพธ์ในตัวชี้วัดด้านเวลาที่ใช้ในการค้นหาเกตเวย์ (Gateway Discovery Time) โดยจะเริ่มนับตั้งแต่เกตเวย์ประกาศข้อมูลเส้นทางจนกระทั่งโหนดที่สนใจรับรู้เส้นทางไปยังเกตเวย์ โดยอัลกอริทึมแบบโพรแอกทีฟใช้เวลาในการค้นหาเกตเวย์สูง แต่สำหรับอัลกอริทึม HELLO และอัลกอริทึม HELLOMPR ก็มีเวลาที่ใช้ในการค้นหาเกตเวย์เพียงเล็กน้อย แต่อัลกอริทึม HELLO จะใช้เวลาน้อยที่สุดเนื่องจากการเพิ่มกลไกคัดเลือกโหนด MPR ทำให้โหนดที่สนใจอาจได้รับ HELLO_I message ช้ากว่าในกรณีที่โหนดที่สนใจนั้นอยู่ใกล้กับโหนดไม่ใช่ MPR มากกว่าโหนดที่ทำหน้าที่เป็น MPR

5. สรุปผล

ในงานวิจัยนี้ได้พัฒนาอัลกอริทึมในการค้นหาเกตเวย์สำหรับเครือข่ายสื่อสารเฉพาะกิจโดยมีพื้นฐานมาจากโพรโทคอล AODV และได้นำหลักการในการคัดเลือกโหนด MPR จากโพรโตคอล OLSR โดยใช้ทฤษฎีเซ็ตมาช่วยในการคำนวณเพื่อลดจำนวนข้อมูลที่ส่งต่อภายในเครือข่าย

จากผลการทดลองสรุปได้ว่าเครือข่ายที่ใช้อัลกอริทึม HELLOMPR มีการส่งข้อมูลเกี่ยวกับเกตเวย์น้อยกว่าอัลกอริทึม HELLO จนเข้าใกล้อัลกอริทึมแบบโพรแอกทีฟ ซึ่งเป็นผลจากการลดจำนวนโหนดที่ต้องบรอดแคสต์ข้อมูลที่ใช้ในการค้นหาเกตเวย์ ซึ่งส่งผลให้โหนดในเครือข่ายมีพลังงานทำให้โหนดอยู่ในระบบได้นานขึ้น และประสิทธิภาพด้านเวลาที่ใช้ในการทำให้โหนดที่สนใจรู้จักเส้นทางไปยังเกตเวย์ไม่ได้ลดลง ซึ่งในสถานการณ์ภัยพิบัตินั้นมีความจำกัดด้านแหล่งพลังงานของโมบายล์โหนด (จากแบตเตอรี่) และความเร่งด่วนในการสื่อสารนั้นก็มีความสำคัญ ดังนั้นอัลกอริทึมที่มีความเหมาะสมคืออัลกอริทึม HELLOMPR เพราะมีการส่งข้อความเป็นจำนวนน้อย และมีเวลาในการค้นหาเกตเวย์ต่ำ

เอกสารอ้างอิง

[1] T. S. Rappaport. "Wireless Communications Principles & Practice." Upper Saddle River, New Jersey: Prentice-Hall, Inc.1996

[2] T. Lin. "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications." Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the Ph.D. in Computer Engineering. 2004

[3] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)." Internet Engineering Task Force (IETF) draft, February 2007.

[4] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing." Internet Engineering Task Force (IETF) draft, July 2003.

[5] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol (OLSR)." Internet Engineering Task Force(IETF) draft, October 2003.

[6] M. Rosenschon. "Internet Gateway Discovery for Mobile Ad Hoc Networks" Submitted for the Degree of Doctor of Philosophy School of Engineering and Mathematical Sciences CITY University London. 2 October 2007

[7] J. Broch, et al. "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks" International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN99), Workshop on Mobile Computing, Perth, Western Australia. June 1999

[8] M. Rosenschon, T. Manz, J. Habermann, V. Rakocevic. "Gateway Discovery Algorithm for Ad-Hoc networks using HELLO Messages" International Workshop on Wireless Ad Hoc Networks IWWAN 2005, London. May 2005.

[9] M. Rosenschon, V. Rakocevic, J. Habermann "Performance Comparison of Gateway Discovery Algorithms in Ad Hoc Networks with Mobile Nodes" Wireless Conference 2006, 12th European, April 2006.

[10] H. Luo, R. Ramjeey, P. Sinhaz, L. Liy, S. Lu "UCAN: A Unified Cellular and AdHoc Network Architecture" MobiCom'03, San Diego, California, USA, September 2003.

[11] A. Tahar, B. Azeddine. "AODV Extension Using Multi Point Relay for High Performance Routing in VANETS" International Journal of Computer Science Department, 2007.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Load Distribution using Modified RED for Multipath TCP Communication

Sumet Prabhavat[1] Ruttikorn Varakulsiripunth[2] Satoshi Utsumi[3] Yasushi Kato[4]

[1]Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
[2]Faculty of Information Technology, Thai-Nichi Institute of Technology, Bangkok, Thailand
[3,4]Tsuruoka National College of Technology, Yamagata, Japan
[1]sumet@it.kmitl.ac.th, [2]kvruttik@gmail.com, [3]u.satoshi0215@gmail.com, [4]president@tsuruoka-nct.ac.jp

***Abstract*— Demand for large bandwidth network connections is growing continuously while network connections via multiple paths can exist because of high degree of connectivity. Utilization of the multiple paths is an economical solution for provisioning large network capacity to meet the users' requirements but it brings about key issues such as load imbalance (causing a large queue and buffer overflow at a gateway) and packet reordering problems that have significant impacts on TCP connections. In this paper, we propose a load distribution model for TCP transmission, called Load Distribution over Multipath with Extended Drop Slope Random Early Detection (LDM/ExRED). LDM/ExRED takes advantages of RED mechanism to maintain a small queue, avoid buffer overflow at a gateway, and mitigate packet reordering problem. In addition, it reduces peak buffer occupancy by using our modified RED (i.e., ExRED). Our work will be evaluated and compared to the other existing models by simulations under realistic traffic conditions.**

Keywords—Load Distribution; Load Balancing; Multipath TCP

I. INTRODUCTION

A wide variety of network service requirements demanded by users has been an important driving force for development of networking technologies [1]. By using today's technologies, multipath configurations can be established in various ways [2]. Their primary objectives are to improve network reliability by increasing network availability and reducing network downtime. A main path was used for data transmission while the others were backups which would be activated when the main path became unavailable. Currently, applications of multiple paths aims not only at avoiding a single point of failure but also at facilitating network provision [1–4] where its effectiveness is essential to quality of network services and Quality of Service (QoS) guarantee. Using multiple paths as a single path with aggregate bandwidth is a practical solution which is preferable rather than provisioning a large-bandwidth path because it offers a possibility to establish a very large-bandwidth connection. This improves scalability to support the future growth in bandwidth demand and affordability for network users. It also provides flexibility in bandwidth management within the communication protocol over the multipath network. Bandwidth aggregation and network-load balancing are important issues having been attractive research topics, and a large amount of load distribution approaches have been proposed. The rest of this paper is organized as follows. Section II briefly describes existing load distribution models, some studies on packet reordering problems, and an active queue management for TCP networks. Section III presents a new load distribution model with our modified active queue management mechanism. Section IV discusses performance evaluation under real traffic conditions. Conclusions are then given in Section V.

II. RELATED WORKS

A. Load Distribution Models

Load distribution can be classified into packet-based model and flow-based models. Packet-based models can be further classified into non-adaptive and adaptive models. Surplus Round Robin (SRR) [5] is a simple non-adaptive load distribution model. SRR is an enhanced version of round robin family model which is widely used schemes in the Internet because it can achieve starvation-free and acceptable load balancing efficiency. Least-loaded first (LLF) [6–8] is an adaptive load distribution model. LLF is a well-known load-sharing approach introduced to manage task loads with heavy-tailed distribution, where a task is assigned to the least-loaded server. In multipath load balancing with this scheme, a path having the smallest load or the shortest queue will be selected for an arrived packet. The most important drawback is that they do not consider task sequence, which can result in the packet reordering problem [9].

On the other hand, Direct Hashing (DH) [10], Table-based Hashing (TH) [11], and Fast Switching (FS) [12] are flow-based models which can prevent packet reordering but they can cause load imbalance problem due to inability to cope with variance of the flow size distribution. This problem can cause a large buffer occupancy leading to a high risk of buffer overflow [2]. Adaptive load distribution models, e.g., Load Distribution over Multipath (LDM) and Load Balancing for Parallel Forwarding (LBPF) [13–15] were introduced to mitigate the load imbalance problem. However, there is trade-off between balancing load and maintaining a low risk of packet reordering. This depends on the respective algorithms as well as their set parameters.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

978-1-4799-0425-9/13/$31.00 ©2013 IEEE

B. Packet Reordering Problem

Several works have studied on packet reordering problem [16–22]. Packet reordering can occur with high probabilities of splitting a flow and switching a path [18], [19]. On the other hand, the possibility of packet reordering will decrease if the interarrival time of two consecutive packets belonging to the same flow is longer than the longest time required to deliver a packet via the parallel paths [23]. The packet interarrival time must be greater than the difference between the longest and the shortest delays among parallel paths to ensure packet order preservation. If the load is not properly distributed among the parallel paths, some paths may experience congestion (leading to large queues) while the others are idle; consequently, the delay difference can be very large.

C. Active Queue Management for TCP Gateway

Random Early Detection (RED) [24] is a well-known active queue management mechanism introduced to improve performance of TCP communication. RED itself consists of two main parts, i.e., the estimation of an average queue size and the decision of whether or not to drop an incoming packet. An average queue size is calculated by a current queue size using an exponentially weighted moving average (EWMA). Based on the average queue size, RED decides whether or not to drop an incoming packet. Packet arrival rate of a flow plays an important role in determining packet drop probability. The higher the packet arrival rate, the higher the packet drop rate. This feature of RED is to prevent two major problems that have a significant impact on TCP connections: buffer overflow and synchronization of TCP flows [25] due to burst traffic. In LDM/RED [26], we uses RED for sensing congestion and marking a packet arriving at the time congestion occurs. The marked packet will be switched to a less congested path.

III. Load Distribution (over Multipath Networks) with Extended Drop Slope Random Early Detection

Figure 1 describes our approach called Load Distribution over Multipath with Extended Drop Slope Random Early Detection (LDM/ExRED), which is developed from LDM/RED [26] and our modified RED algorithm (i.e., ExRED) [27]. Assume that multiple and parallel connections are established between a source and a destination before data transmission is started. For each path p, bandwidth is μ_p. The other parameters, e.g., hop counts and path delay, are assumed reflected by a measured queue length q_p. The input traffic is split into flows, each of which independently takes a path determined by a path selection component. LDM/ExRED is a variant version of FS [12] and LDM [13], a table-based model which selects paths based on the flow-path mapping table. A packet belonging to an existing flow is sent via the same path as its previous ones. When a new flow appears, a packet belonging to the new flow will be sent via a new path having the shortest queue.

In LDM/ExRED, a mapping table is modified and the path for an existing flow will be changed. The existing flow is switched (to a new path having the shortest queue) with probability π_s which is determined by ExRED mechanism, as illustrated in Fig. 2. Based on an average queue length $\hat{q}_p$,

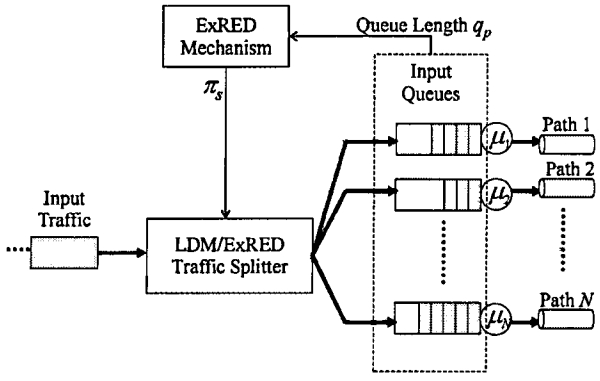


Figure 1. Description of the proposed model, LDM/ExRED

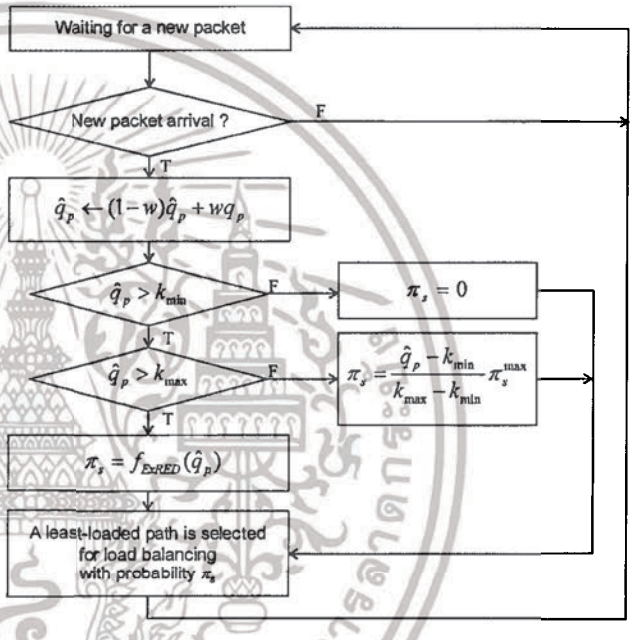


Figure 2. Flowchart to calculate π_s in traffic splitting algorithm

LDM/ExRED makes a decision of whether or not to split the flow. There are two queue thresholds: minimum and maximum thresholds, i.e., k_{min} and k_{max}. When $\hat{q}_p > k_{min}$, the flow is split with probability $\pi_s > 0$. The larger the average queue size $\hat{q}_p$, the higher the probability π_s. When $\hat{q}_p > k_{max}$, π_s increases according to polynomial function in (1) until $\pi_s = \pi_s^{max}$ (which is a desired maximum value of splitting probability). When $\pi_s^{max} = 1$ and $\pi_s = \pi_s^{max}$, all flows are always moved to a new path.

$$f_{ExRED}(\hat{q}) = a_2\hat{q}^2 + a_1\hat{q} + a_0 \quad (1)$$

where coefficients of the positive increasing function are

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$a_2 = \frac{(k_{max} - k_{min}) - (K - k_{min})\pi_s^{max}}{(k_{max} - k_{min})(K - k_{max})^2}$$

$$a_1 = \frac{(k_{max}^2 + K^2 - 2k_{max}k_{min})\pi_s^{max} - 2k_{max}^2 + 2k_{max}k_{min}}{(k_{max} - k_{min})(K - k_{max})^2}$$

$$a_0 = \frac{k_{max}^3 - k_{max}^2 k_{min} - (k_{max}^2 + 2k_{max}k_{min} + k_{min}K)K\pi_s^{max}}{(k_{max} - k_{min})(K - k_{max})^2}$$

Equation (1) shows that ExRED provides flexible increasing of path-switching probability. It can prevent a consecutive path-switching in case of the average queue size is over maximum threshold and not exceeds limit of buffer size (K). We expect that this will allow us to utilize a particular path as much as possible while not causing overload on the path.

IV. Performance Evaluation

In this section, comparative performance under different conditions of real traffics is demonstrated.

A. Simulation model and parameters

Three simulation scenarios are conducted to compare the performance of load distribution models, by using 1-hour long real traffic traces [28], i.e., DSet1, DSet2, and DSet3, which are captured from primary Internet access point between Digital Equipment Corporation and the Internet. Characteristics of the traces are listed in Table I. Three paths exist between a pair of source and destination. Bandwidth capacities (or mean service rates) of path 1, path 2, and path 3 are 1, 4, and 7 Mbps, respectively; the total bandwidth capacity is 12 Mbps. As compared to the total bandwidth capacity, traffics generated from trace DSet1 and DSet2 incur heavy load and some load-spikes. Moreover, we use trace DSet3 to generate extremely heavy traffic which peak load is much higher than the total bandwidth capacity, thus incurring network overload.

With the set-up simulation environment, LDM/ExRED, LDM, LLF, and SRR are evaluated. In LDM/RED and LDM/ExRED, the parameters are chosen: EWMA parameter w=0.02, k_{min}=10, k_{max}=30, and π_s^{max}=0.1. These parameters setting are recommended in [24], [27], and [29]. In SRR, weights assigned for path 1, path 2, and path 3 are 1, 4, and 7, respectively, which are used for specifying desired forwarding rates on each path [5]. In LBPF, the size of the table is 20, W=1000, and P=20, where W is window size for detecting aggressive flows and P is period for splitting the aggressive flows. LBPF's parameters can be further read at [14].

B. Load Balancing Efficiency

Tables II shows that LDM/ExRED can achieve load balancing, as compared to the others since probabilities of buffer occupancy of all paths are almost equal. This can be implied that all paths are fairly utilized. Moreover, Table III shows that LDM/RED and LDM/ExRED can prevent buffer overflow; maximum queue sizes incurred by both of them are significantly smaller than those incurred by SRR and LDM. This is because burst traffic (which can cause a large queue) is detected by RED and then distributed over multiple paths.

TABLE I. Profile of Traffic Traces

Trace ID	# Packets x10^6	Traffic Rate (Mbps.)			# Different Flows	Flow Size (Packets)		Flow Rate (Flows/Second)		
		Mean	Min.	Max.		Mean	CV	Mean	Min.	Max.
DSet 1	2.66	5.91	2.07	13.65	5865	453.87	7.52	137.89	77	204
DSet 2	2.87	6.38	0.46	12.24	12903	222.71	5.98	175.32	44	247
DSet 3	3.86	8.58	1.86	15.45	12710	303.88	7.11	184.50	90	269

TABLE II. Probability of Buffer Occupancy

Load Distribution Model	Dset 1			Dset 2			Dset 3		
	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3
LDM/ExRED	0.71	0.66	0.65	0.73	0.68	0.65	0.86	0.82	0.80
LDM/RED	0.70	0.66	0.65	0.73	0.67	0.65	0.87	0.82	0.80
LDM	0.86	0.71	0.59	0.89	0.73	0.58	0.95	0.85	0.77
LLF	0.77	0.53	0.47	0.80	0.55	0.48	0.91	0.74	0.70
SRR	0.35	0.66	0.66	0.37	0.68	0.68	0.61	0.81	0.82

TABLE III. Maximum Queue Size (Packets)

Load Distribution Model	Dset 1			Dset 2			Dset 3		
	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3
LDM/ExRED	83	81	82	85	83	82	319	318	317
LDM/RED	100	98	100	104	97	102	376	375	375
LDM	1685	422	180	3845	378	76	5976	2780	522
LLF	92	92	93	83	83	83	293	293	293
SRR	43	86	185	33	88	165	110	350	557

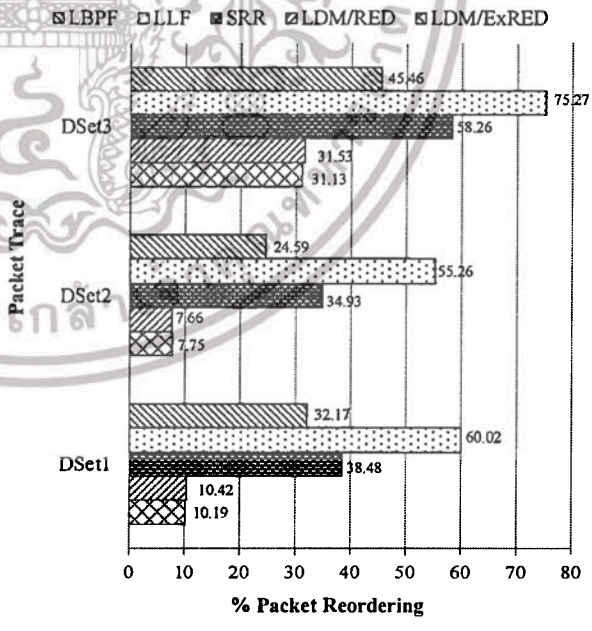


Figure 3. Risk of Packet Reordering

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

However, when buffer is highly utilized, RED causes consecutive marked packets while ExRED can prevent such problem. Therefore, LDM/ExRED can reduce peak buffer occupancy. A gateway device requires only a small buffer.

C. *Packet Order Preservation*

Fig. 3 illustrates that LDM/ExRED and LDM/RED can efficiently alleviate packet reordering inherently existing in packet-based models such as SRR and LLF. LDM is a flow-based model which can perfectly prevent packet reordering. SRR sends packets in a round robin manner. It can cause a risk of packet reordering. LLF choosing only the path with the shortest queue size can cause a high risk of packet reordering. LBPF splits a group of largest flows, thus leading to the risk of packet reordering. The discussion on this issue can be found in [2], [23], and [30]. As compared to LDM/RED, LDM/ExRED has a potential to maintain low risk of packet reordering because of a smaller path-switching probability. However, difference between delay on high congested path and that on a less congested path is also a factor of the risk of packet reordering [2], [23]. This is an open issue for further studies.

V. CONCLUDING REMARKS

This paper proposes a load distribution model for TCP transmission. LDM/ExRED takes advantages from RED mechanism in traffic splitting and distribute load subject to necessary condition to prevent packet reordering. With a modified RED, i.e., ExRED, it can prevent buffer overflow (due to burstiness of TCP flows) at a gateway and maintain low risk of packet reordering. The superiority of LDM/ExRED is presented by comparative performance among LDM/ExRED and the current existing load distribution models by simulations under variety of real traffic conditions.

REFERENCES

[1] L. Golubchik, J. Lui, T. Tung, A. Chow, W. Lee, G. Franceschinis, and C. Anglano, "Multi-path continuous media streaming: What are the benefits?," *Performance Evaluation*, vol. 49, pp. 429–449, Sep. 2002.

[2] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "On Load Distribution over Multipath Networks," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 3, pp. 662–680, 2012.

[3] M. Menth, R. Martin, A. Koster, and S. Orlowski, "Overview of resilience mechanisms based on multipath structures," in *Proc. the 6th International Workshop on Design and Reliable Communication Networks (DRCN)*, La Rochelle, France, Oct. 2007.

[4] N. Wang, K. Ho, G. Pavlou, and M. Howarth, "An overview of routing optimization for Internet traffic engineering," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 1, pp. 36–56, 2008.

[5] H. Adiseshu, G. Parulkar, and G. Varghese, "A reliable and scalable striping protocol," *ACM SIGCOMM Computer Communication Review*, vol. 26, no. 4, pp. 131–141, Oct. 1996.

[6] K. G. Shin and C. J. Hou, "Design and Evaluation of Effective Load Sharing in Distributed Real-Time Systems," *IEEE Trans. Parallel and Distributed Systems*, vol. 5, no. 7, pp. 704–719, Jul. 1994.

[7] O. Kremien and J. Kramer, "Methodical analysis of adaptive load sharing algorithms," *IEEE Trans. Parallel Distribution Systems*, vol. 3, no. 6, pp. 747–760, Nov .1992.

[8] C. C. Hui and S. T. Chanson, "Hydrodynamic load balancing," *IEEE Trans. Parallel and Distributed Systems*, vol. 10, no. 11, pp. 1118–1137, Nov. 1999.

[9] Z. Tari, J. Broberg, A. Zomaya, and R. Baldoni, "A least flow-time first load sharing approach for distributed server farm," *Journal of Parallel and Distributed Computing*, vol. 65, no. 7, pp. 832–842, Jul. 2005.

[10] C. Villamizar, "OSPF optimized multipath (OSPF-OMP)," Internet draft draft-ietf-ospf-omp-02.txt, Feb. 1999.

[11] D. Thaler and C. Hopps, "Multipath issues in unicast and multicast next-hop selection," RFC 2991, Nov. 2000.

[12] A. Zinin, Cisco IP Routing, packet forwarding and intra-domain routing protocols. Reading, MA: Addison Wesley, 2002.

[13] J. Song, S. Kim, M. Lee, H. Lee, and T. Suda, "Adaptive load distribution over multipath in MPLS networks," in *Proc. IEEE ICC*, Anchorage, Alaska, May 2003, pp. 233–237.

[14] W. Shi, M. H. MacGregor, and P. Gburzynski, "Load balancing for parallel forwarding," *IEEE/ACM Trans. Networking*, vol. 13, no. 4, pp. 790–801, Aug. 2005.

[15] S. Kandula, D. Katabi, S. Sinha, and A. Berger, "Dynamic load balancing without packet reordering," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 2, pp. 53–62, Apr. 2007.

[16] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis, "Framework for IP performance metrics," RFC 2330, May. 1998.

[17] C. Demichelis and P. Chimento, "IP packet delay variation metric for IP performance metrics (IPPM)," RFC 3393, Nov. 2002.

[18] N. M. Piratla, A. P. Jayasumana, A. A. Bare, and T. Banka, "Reorder buffer-occupancy density and its application for measurement and evaluation of packet reordering," *Computer Communications*, vol. 30, no.9, pp.1980–1993, Jun. 2007.

[19] N. M. Piratla and A. P. Jayasumana, "Reordering of packets due to multipath forwarding – An analysis," in *Proc. IEEE ICC*, Istanbul, Turkey, Jun. 2006, pp. 829–834.

[20] A. Morton, L. Ciavattone, G. Ramachandran, S. Shalunov, and J. Perser, "Packet reordering metrics," RFC 4737, Nov. 2006.

[21] A. Jayasumana, N. Piratla, T. Banka, and R. Whitner, "Improved packet reordering metrics," RFC 5236, Jun. 2008.

[22] S. Jaiswal, G. Iannaccone, C. Diot, J. Kurose, and D. Towsley, "Measurement and classification of out-of-sequence packets in a tier-1 IP backbone," *IEEE/ACM Trans. Networking*, vol. 15, no. 1, pp. 54–66, Feb. 2007.

[23] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "On the Performance Analysis of Traffic Splitting on Load Imbalancing and Packet Reordering of Bursty Traffic," in *Proc. IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC 2009)*, Beijing, China, Nov. 2009.

[24] S. Floyd and V. Jacobsan, "Random Early Detection Gateways for Congestion Avoidance," *IEEE/ACM Trans. Networking*, vol. 1, no. 4. pp. 397-413, Aug. 1993.

[25] S. Floyd and V. Jacobson, "On traffic phase effects in packet-switched gateways," *Internetworking: Research & Experience*, vol. 3, no. 3, Sep. 1992, pp.115-56, UK.

[26] S. Prabhavat, N. Kato, and R. Varakulsiripunth, "Load Distribution Mechanism for Multipath TCP Communication," in *Proc. International Symposium on Technology for Sustainability (ISTS 2011)*, Bangkok, Thailand, Jan. 2012, pp. 321–324.

[27] S. Prabhavat and R. Varakulsiripunth, "Performance Improvement on RED Based Gateway in TCP Communication Network," in *Proc. International Conference on Control, Automation and Systems (ICCAS 2004)*, Bangkok, Thailand, Aug. 2004, pp. 782–787.

[28] (Online Sources) P. Danzig, J. Mogul, V. Paxson, and M. Schwartz. (1995, Mar.). *The Internet Traffic Archive*. Available: http://ita.ee.lbl.gov/index.html.

[29] (Online Sources) S. Floyd (1967, Nov.), "RED: Discussions of Setting Parameters," Available: http://www.icir.org/floyd/REDparameters.txt.

[30] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "Effective Delay-Controlled Load Distribution over Multipath Networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 10, pp. 1730–1741, Oct. 2011.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Mark-Reverse Explicit Congestion Notification for Satellite IP Networks: Simulation and Analysis Results

Masato Inoue*, Pakapol Tangdumrongrat**, Sumet Prabhavat**, Satoshi Utsumi*, Salahuddin Muhammad Salim Zabir*** and Norio Shiratori****

*Tsuruoka National College of Technology, Yamagata, Japan
**King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
***France Telecom Japan, Tokyo, Japan
****Tohoku University/Waseda University, Sendai/Tokyo, Japan
e-mail: u-satoshi@tsuruoka-nct.ac.jp

***Abstract*—In this paper, we propose a new congestoin notification scheme, named as Mark-Reverse ECN (Explicit Congestion Notification) for satellite IP networks. Simulation and analysis are conducted for performance evaluation. This analytical model takes the packet drop ratio and the packet mark ratio into account. We show that the results from the analytical model and the simulation match quite closely.**

Primary Categories — **Informatics.**
Secondary Categories — **Computer System/Network.**
Keywords — **ECN (Explicit Congestion Notification), Congestion Control, Satellite IP Network, Analytical Model.**

I. Introduction

Explicit Congestion Notification (ECN) has been proposed for the Internet as a means for detecting an incipient congestion before it actually occurs and notifying that explicitly to the corresponding end hosts. This has the potential to improve the network performance under congestion scenarios than conventional packet dropping mechanisms [1]. Random Early Detection (RED) with ECN gives definite improvement in time delays for interactive traffic. In [1], they examined use of a Backward Explicit Congestion Notification (BECN) mechanism to inform the sender of the congestion situation in the network. Because this mechanism uses ICMP Source Quenches (ISQs) for backward notification, the TCP senders would be attacked by the blind throughput-reduction attack [2].

In this paper, we propose a new congestion notification scheme, we name as Mark-Reverse ECN for satellite IP networks. Contrary to the conventional ECN mechanisms, rather then marking the packets in the forward direction, our proposed scheme marks the packets containg the ACKs in the reverse direction bound for the source nodes. The ACKs eventually notify congestion to the source nodes. As such, this mechanism leads to a faster notification of an incipent congestion.

The rest of this paper is organized as follows. In section II, we propose our novel marking scheme, Mark-Reverse ECN following a brief outline of existing schemes. In section III, we evaluate our scheme by comparing with the conventional scheme through simulations. Section IV describes a new analytical model for ECN. Finally, we conclude this paper in section V.

II. Our Proposal: Mark-Reverse ECN

Before presenting our novel mechanism, we first provide a brief outline of the conventional marking schemes.

A. Conventional ECN Schemes

Fig. 1 demonstrates Mark-Tail ECN [3]. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. It will be marked before forwarded to its destination. Source S will be notified about the congestion after this packet arrives at destination D and its ACK packet returns (at time t_2). Notification delay is almost RTT (Round Trip Time).

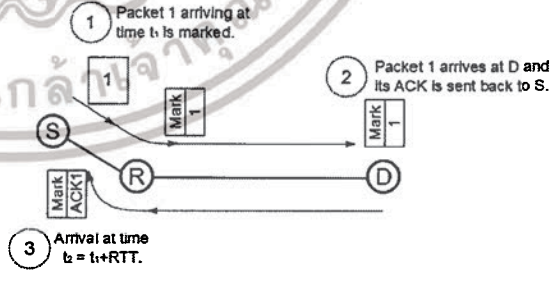


Fig. 1. Mark-Tail ECN Scheme.

B. Mark-Reverse ECN

Fig. 2 shows how our proposal Mark-Reverse ECN works. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. When an ACK packet of any previous packet arrives at the router, e.g., at time t_1^+,

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

it will be marked before being forwarded to its destination (i.e., Source S).Assume that the ACK packet acknowledges the successful delivery of packet 0 which is previously sent at time t_0. Notification delay $\Delta t = t_1^+ - t_1$ is very small.

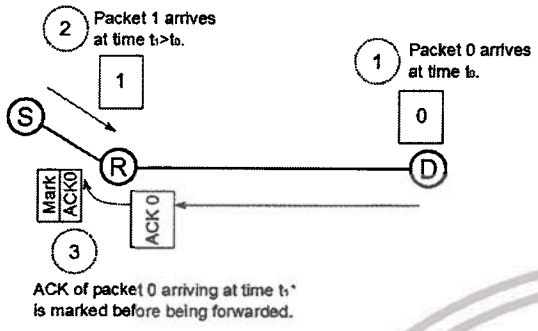


Fig. 2. Mark-Reverse ECN Scheme.

III. Simulation

We use ns-2 [4] for our simulations with respect to the simulation scenario as shown in Fig. 3. We set the packet size 1,000bytes, the maximum window size 1000 segments, the capacity of the satellite link between senders and receivers 10Mbps (about 1,300 packets/sec), round trip time of the satellite link 550ms, and the link error ratio 0%. We changed the number of TCP flows. We set RED for ECN on the forwarding node of the satellite link. We observed the throughput, the packet drop ratio and the packet marking ratio. The simulation time is 500s. Simulation results are in Fig. 4, Fig. 5, and Fig. 6.

IV. Analytical Models for ECN

Our proposed model is composed of four parts according to a typical short-lived flow evolution: the start of the connection (three-way-handshake), the initial slow-start phase, the first loss (or mark) part, and the subsequent losses or marks.

A. The Connection Start-Up Phase

Every TCP connection starts with the three-way-handshake process. Assuming that no ACK packets can get lost, this process can be well modeled as follows [5]:

$$E[T_{twhs}] = RTT + T_s(\frac{1-p}{1-2p} - 1), \quad (1)$$

where T_s is the duration of SYN time-out and p is the packet loss ratio.

B. The Initial Slow-Start Phase

In order to derive the latency for this phase, $E[Y^{SS}]$, the expected number of packets sent until a loss or a mark occurs is given by following enhanced equation (based on the one given in [5]):

$$E[Y^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q))}{p+q}, \quad (2)$$

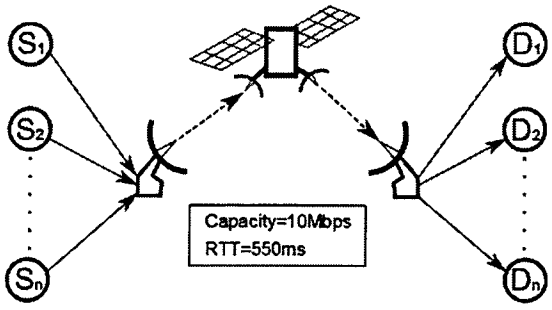


Fig. 3. Simulation scenario.

where d is the total file size measured in packets that must be transmitted and q is the packet marking ratio.

Substituting the value of $E[Y^{SS}]$ in the Equation (2), we get the expected size of congestion window at the end of the low-start phase due to the packet losses or the packet marks:

$$E[W^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q)) + 2(p+q)}{(p+q)g^2}, \quad (3)$$

where $g = 1.61804$ [5].

The expected slow-start latency is calculated as follows [5]:

$$E[n] = \begin{cases} \lceil log_g(\frac{W_m}{C_1}) \rceil \\ +\frac{1}{W_m}(E[Y^{ss}] - g^2 W_m - 2), when\ E[W^{ss}] > W_m \\ \lceil log_g(\frac{E[Y^{SS}]+2}{C_1}) \rceil - 2, when\ E[W^{SS}] \le W_m \end{cases} \quad (4)$$

C. The First Loss

Assume that the first indication to detect congestion is a packet loss. In the round where a TD (triple-duplicate) occurs, let W^{SS} be the current size of *cwnd*, which has a value w. In this round, w packets were sent. Among them, k packets are assumed to be ACKed. Since the connection is still in the slow-start phase, *cwnd* increases to $w + k$ and another $2k$ packets are sent in the next round. If more then three packets from these $2k$ packets get ACKed, then a TD would occur; otherewise, a TO would take place. Let

$$A(w,k) = \frac{(1-p)^k p}{1-(1-p)^w}, \quad (5)$$

be the probability that the first k packets have been successfully transmitted and ACKed in a round of w packets, provided that there might be one or more packets got lost. Now, let

$$h(m) = \sum_{i=0}^{2}(1-p)^i p, for\ m \ge 3, \quad (6)$$

be the probability that no more than 2 packets have been transmitted successfully in a round of m packets. We the

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

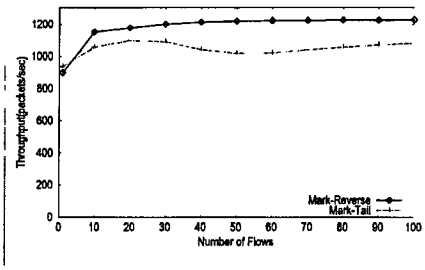


Fig. 4. Throughput comparisons between Mark-Reverse ECN and Mark-Tail ECN.(simulation results)

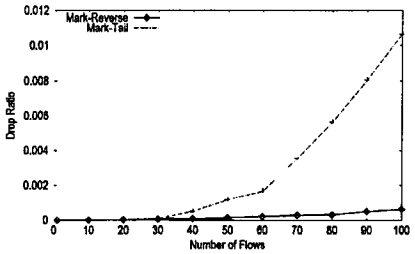


Fig. 5. Drop ratio comparisons between Mark-Reverse ECN and Mark-Tail ECN.(simulation results)

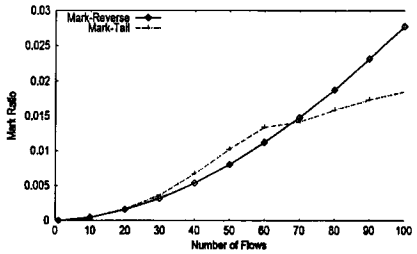


Fig. 6. Mark ration cmparisons between Mark-Reverse ECN and Mark-Tail ECN.(simulation results)

obtain $Q(w)$, the probability that a loss in a window size w is a TO (Timeout), is given by

$$Q(w) = \begin{cases} 1 & ,when\ w \leq 3 \\ \sum_{k=0}^{2} A(w,k) + \sum_{k=3}^{w-1} A(w,k)h(k) & ,otherwise \end{cases} \quad (7)$$

The expected time that TCP spends in the RTOs is given in [7] as:

$$E[Z^{TO}] = T_0 \frac{f(p)}{1-p}, \quad (8)$$

where T_0 is the average duration of the first time-out, and

$$f(p) = 1 + p + 2p^2 + 4p^3 + 8p^4 + 16p^5 + 32p^6. \quad (9)$$

Finally, the expected latency that this loss would incur is

$$T_{loss} = \frac{p}{p+q} \times (1-(1-(p+q))^d) \times (Q(W^{SS})E[Z^{TO}] + (1-Q(W^{SS}))RTT). \quad (10)$$

D. Sending the Rest of the Packets

After the first packet loss or the first packet mark, the transmission latency of the rest $(d - E[Y_{init}])$ packets is obtained as follows:

$$T_{rest} = \frac{d - E[Y^{SS}]}{H}, \quad (11)$$

where H is the throughput of a steady-state flow.

The expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = E[\alpha] + E[W^{TDM}] - 1, \quad (12)$$

where $E[\alpha]$ is the expected number of packets sent in a TDMP (triple-duplicate or marking period) up to and including the first packet that is lost or marked. Given our loss and mark model, the probability that $\alpha_i = k$ is equal to the probability that exactly $k-1$ packets are successfully acknowkedged before a loss or a mark occurs is

$$P[\alpha = k] = (1-(p+q))^{k-1}(p+q), k = 1, 2, \ldots. \quad (13)$$

The mean of α is thus,

$$E[\alpha] = (1-(p+q))^{k-1}(p+q)k = \frac{1}{p+q}. \quad (14)$$

From (12) and (14) it follows that

$$E[Y] = \frac{1-(p+q)}{p+q} + E[W^{TDM}]. \quad (15)$$

From [8] the expected round where the first loss or the first mark occurs, $E[X]$, is

$$E[X] = b(\frac{E[W^{TDM}]}{2} + 1). \quad (16)$$

From [8] the expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) + E[\beta]. \quad (17)$$

Then, from Equations (15) and (17), we get the following expression which involves $E[W^{TDM}]$:

$$\frac{1-(p+q)}{p+q} + E[W^{TDM}] = \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) + E[\beta]. \quad (18)$$

For simplicity, we assume β_i to be uniformly distributed between 1 and $W_i - 1$. Thus, $E[\beta] = E[W^{TDM}]/2$.

Combining (16) and (18), we get:

$$E[W^{TDM}] = -\frac{2(b-1)}{3b} + \sqrt{\frac{4(b(p+q)+2(1-(p+q)))}{3b(p+q)} + (\frac{2(b-1)}{3b})^2}. \quad (19)$$

From [8], the expected value of duration of a round, $E[A]$, is

$$E[A] = RTT(\frac{p}{p+q}(E[X]+1) + \frac{q}{p+q}E[X]). \quad (20)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

E. Impact of Window Limitation

At the beginning of TCP flow establishment, the receiver advertises a maximum buffer size which determines a maximum congestion window size, W_m. As a consequence, during a period without loss indications, the window size can grow up to W_m, but will not grow further beyond this value. During the first TDMP, the window grows linearly up to W_m for U rounds, then remains constant for V rounds, and then a triple-duplicate or marking indication occurs. The expected U rounds, $E[U]$, is as follows [7]:

$$E[U] = \frac{b}{2}W_m. \tag{21}$$

Since Y_i, the number of packets in the ith TDMP, does not depend on window limitation, $E[Y]$ is given by (12):

$$E[Y] = E[\alpha] + W_m - 1. \tag{22}$$

From [7],

$$E[Y] = \frac{3}{4}W_m E[U] + W_m E[V]. \tag{23}$$

Then,

$$\frac{1-(p+q)}{p+q} + W_m = \frac{3b}{8}W_m^2 + W_m E[V]. \tag{24}$$

Thus,

$$E[V] = \frac{1-(p+q)}{(p+q)W_m} + 1 - \frac{3b}{8}W_m. \tag{25}$$

Finally, since $X_i = U_i + V_i$ in ith TDMP, we have

$$E[X] = E[U] + E[V] = \frac{b}{8}W_m + \frac{1-(p+q)}{(p+q)W_m} + 1. \tag{26}$$

The expected number of packets that have been received in a TDMP, $E[Y']$, is

$$\begin{aligned} E[Y'] &= \frac{p}{p+q}(E[\alpha] + E[\beta] - 1.0) \\ &\quad + \frac{q}{p+q}(E[\alpha] + E[W^{TDM}] - E[\beta] - 1.0) \\ &= E[\alpha] + \frac{E[W^{TDM}]}{2} - 1.0. \end{aligned} \tag{27}$$

The expected number of packets received in the time-out phase,

$$E[R] = 1. \tag{28}$$

Thus, the throughput can be formulated as:

$$H = \frac{E[Y'] + \frac{p}{p+q}Q(W^{TDM}) * E[R]}{E[A] + \frac{p}{p+q}Q(W^{TDM}) * E[Z^{TO}]}. \tag{29}$$

From [5], the total expected latency is

$$T_{latency} = E[T_{twhs}] + E[n]RTT + T_{loss} + T_{rest} - \frac{RTT}{2}. \tag{30}$$

Here, the delay caused by the delayed acknowledgment for the first packet is 0ms. That is, the option of delayed acknowledgment is off.

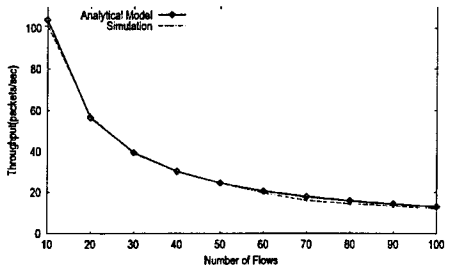


Fig. 7. Throughput comparisons between analytical model and simulation for Mark-Reverse ECN.

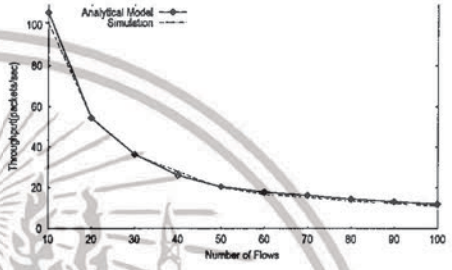


Fig. 8. Throughput comparisons between analytical model and simulation for Mark-Tail ECN.

F. Verification

Fig. 7 and Fig. 8 show the results of this analytical model comparing with simulation results.

V. Conclusion

In this paper, we propose a novel congestion notification scheme, that we name as Mark-Reverse ECN for satellite IP networks. Simulation results show that Mark-Reverse can ensure higher throughput and lower packet drop ratio. In addition, we propose an analytical model for ECN. Analytical results also verify that Mark-Reverse ECN yields better performance than conventional or Mark-Tail mechanisms.

References

[1] F. Akujobi, I. Lambadaris, R. Makkar, N. Seddigh, and B. Nandy, "BECN for Congestion Control in TCP/IP Neworks: Study and Comparative Evaluation," *IEEE Globecom 2002*, Nov. 2002.
[2] RFC 5927, "ICMP Attacks against TCP," July 2010.
[3] S. Floyd, "TCP and Explicit Congestion Notification," Computer Communications Review, vol. 24, no. 5, Oct. 1994.
[4] UCB/LBNL/VINT Network Simulation (NS).
[5] D. Zheng, G. Y. Lazarou, and R. Hu, "A Stochastic Model for Short-lived TCP Flows," IEEE International Conference on Communications 2003 (ICC 2003), May 2003, pp.11-15.
[6] N. Cardwell, S. Savage, and T. Anderson, "Modeling TCP Latency," in Proc. *IEEE INFOCOM 2000*, vol. 3, Mar. 2000, pp.1742-1751.
[7] J. Padhye, V. Firouiu, D. F. Towsley, and J. F. Kurose, "Modeling TCP Reno Performance: A Simple Model and Its Empirical Validation," *IEEE/ACM Trans. Networking*, vol. 8, no. 2, pp.133-145, Apr. 2000.
[8] D. Zheng, "On the modeling of TCP latency and throughput," Master's thesis Mississippi State University, 2002.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

杜団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

Mark-Reverse Explicit Congestion Notification: Concept, Analysis and Evaluation

Masato INOUE†, Pakapol TANGDUMRONGRAT††, Sumet PRABHAVAT††, Satoshi UTSUMI†,
Salahuddin MUHAMMAD SALIM ZABIR†††, and Norio SHIRATORI††††

† Tsuruoka National College of Technology 104 Sawada, Inooka, Tsuruoka, Yamagata, 997–8511 Japan
†† King Mongkut's Institute of Technology Ladkrabang Chalongkrung Rd., Ladkrabang, Bangkok 10520, Thailand
††† France Telecom Japan Co., Ltd Keio Shinjuku Oiwake Bldg. 9F, 3–1–13 Shinjuku, Shinkjuku-ku, Tokyo, 160–0022 Japan
†††† Tohoku University 2-1-1 Katahira, Aoba-ku, Sendai, 980–8577 Japan

Abstract In this paper, we propose a new congestion notification scheme, named as Mark-Reverse ECN (Explicit Congestion Notification) for satellite IP networks. When congestion is beginning to occur on a link, our scheme notifies a source node more quickly than a conventional scheme, i.e., Mark-Tail ECN. Instead of a packet on forwarding path, we marks an acknowledge (ACK) packet on backwarding path which is heading for the source node. We expect that latency time for congestion notification will be reduced and congestion control will thus work more accurately and effectively. Simulation and analysis are conducted for performance evaluation. Through simulation, we compare and evaluate performance of Mark-Reverse ECN and Mark-Tail ECN. Mark-Reverse ECN shows high throughput and low packet drop ratio in satellite IP networks. In analysis, we propose a new analytical model of TCP NewReno supporting ECN. This analytical model takes the packet drop ratio and the packet mark ratio into account for computing delay time and throughput. Analytical results also show superiority of our scheme, correspondingly. A considerably small discrepancy between the results verify our simulation and analysis.

Key words ECN (Explicit Congestion Notification), Congestion Control, Satellite IP Network, Analytical Model.

1. Introduction

Explicit Congestion Notification (ECN) was proposed for the Internet as a means of explicitly notifying end-hosts of network congestion by marking, instead of dropping packets [1]. Random Early Detection (RED) [2] with ECN gives definite improvement in time delays for interactive traffic. In [1], they examined use of a Backward Explicit Congestion Notification (BECN) mechanism to inform the sender of the congestion situation in the network. Because this mechanism uses ICMP Source Quenches (ISQs) for backward notification, the TCP senders would be attacked by the blind throughput-reduction attack [3].

In this paper, we propose a new congestoin notification scheme, named as Mark-Reverse ECN for satellite IP networks. Our proposal, i.e., Mark-Reverse ECN is a scheme that marks ACKs in the opposite direction of the same path when congestion is beginning to occur on the link. The ACKs notifies congestion to the distination node.

The rest of this paper is organized as follows: In section 2., we describe a conventional ECN scheme, i.e., Mark-Tail ECN. In section 3., we propose a new ECN scheme, i.e., Mark-Reverse ECN. In section 4., we evaluate our scheme comparing with the conventional scheme through simulations. Section 5. describes a new analytical model for ECN. Finally, section 6. concludes ths paper.

2. Conventional Scheme: Mark-Tail ECN [4]

Fig. 1 demonstrates Mark-Tail ECN [4]. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. It will be marked before forwarded to its destination. Source S will be notified about the congestion after this packet arrives at destination D and its ACK packet returns (at time t_2). Notification delay is almost RTT.

ไม่วาการณ์ใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

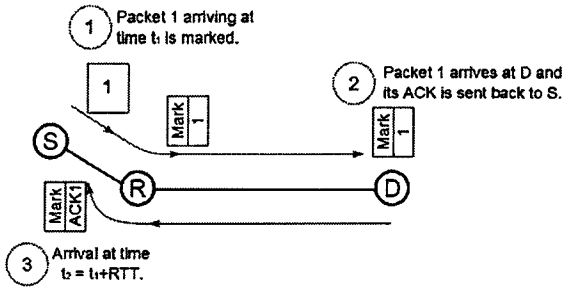


Fig. 1 Mark-Tail ECN Scheme.

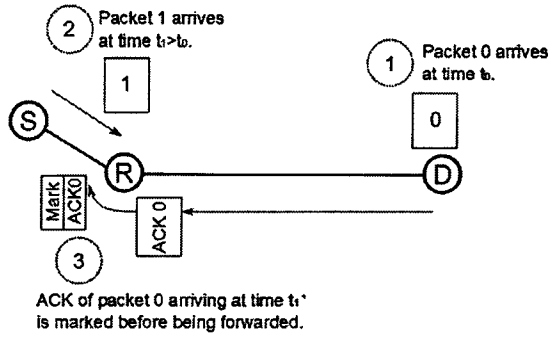


Fig. 2 Mark-Reverse ECN Scheme.

3. Our Proposal: Mark-Reverse ECN

Our proposal Mark-Reverse ECN scheme needs Mark-Reverse ECN-Capable Transport (MR-ECT) bit on IP packets. (MR-ECT bit should not be on at once with ECN-Capable Transport (ECT) bit.) Also, Mark-Reverse ECN scheme needs Congestion Experienced (CE) bit on IP packets. According to Random Early Detection (RED) mechanisms on the queue of the positive direction, the CE bit on the packet whose MR-ECT bit is on in the reverse direction of the same link supporting Mark-Reverse ECN becomes on when the packet is passing in the reverse direction. Mark-Tail ECN scheme and Mark-Front ECN scheme [5] need about RTT to notify congestion to the source node. Mark-Reverse ECN scheme needs about 0 msec to notify congestion to the source node, if the congestion link is near the source node. Because of the fast notification, the number of packet losses due to congestion can be minimized. Especially, it is very useful when the bottleneck link is satellite one. Because Mark-Reverse ECN scheme uses the packets of the same connection for congestion notification differing with Backward Explicit Congestion Notification (BECN), Mark-Reverse ECN scheme can avoid the blind throughput-reduction attack. That is, ICMP Source Quench (ISQ) message of BECN can be transmitted from an arbitrary node to the source node, the Mark-Reverse ECN is notified only from the nodes passed through by the flow using the connection. Moreover, there is no overhead by notifying messages as ISQ messages.

Fig. 2 shows how our proposal Mark-Reverse ECN works. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. When an ACK packet of any previous packet arrives at the router, e.g., at time t_1^+, it will be marked before being forwarded to its destination (i.e., Source S).Assume that the ACK packet acknowledges the successful delivery of packet 0 which is previously sent at time t_0. Notification delay $\Delta t = t_1^+ - t_1$ is very small.

4. Simulation

4.1 Evaluation of Throughput, Drop ratio and Mark ratio

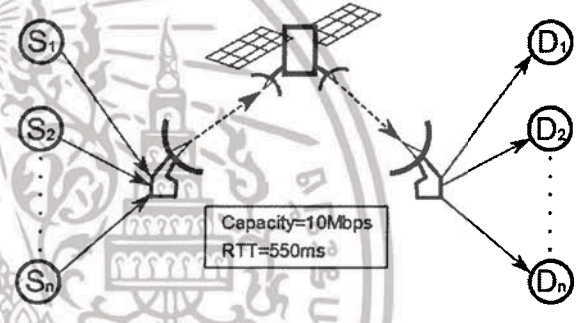


Fig. 3 Simulation scenario.

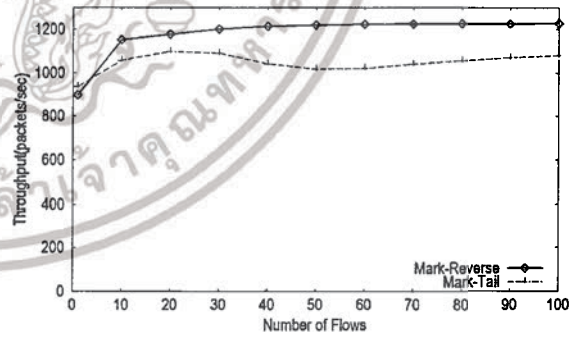


Fig. 4 Throughput comparisons between Mark-Reverse ECN and Mark-Tail ECN. (simulation results)

We use ns-2 [6] for network simulations. We evaluate throughput, drop ratio and mark ratio in the simulation scenario as shown in Fig. 3. We set the packet size 1,000bytes, the maximum window size 1,000 segments, the capacity of the satellite link between senders and receivers 10Mbps (about 1,300 packets/sec), round trip time of the satellite link 550ms, and the link error ratio 0%. We changed the number of TCP flows. We set RED for ECN on the forwarding node of the satellite link. We observed the throughput,

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

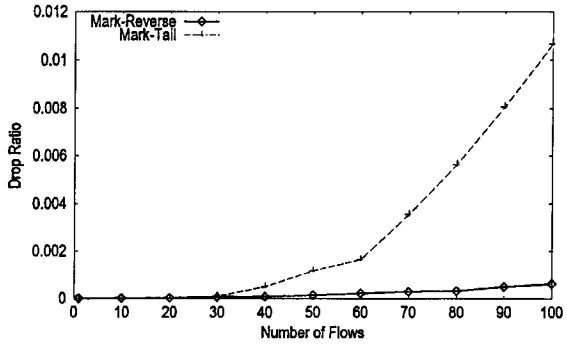


Fig. 5 Drop ratio comparisons between Mark-Reverse ECN and Mark-Tail ECN. (simulation results)

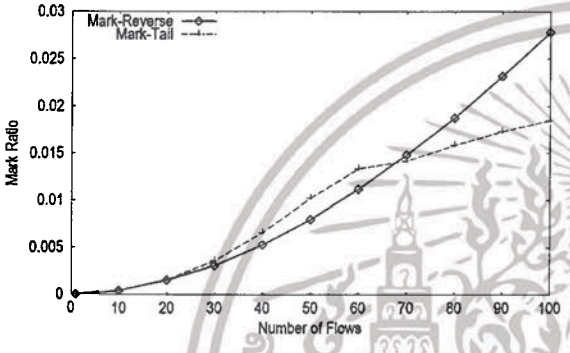


Fig. 6 Mark ratio cmparisons between Mark-Reverse ECN and Mark-Tail ECN. (simulation results)

the packet drop ratio and the packet mark ratio. The simulation time is 500s. Simulation results are in Fig. 4, Fig. 5, and Fig. 6.

5. Analytical Models for ECN

Our proposed model is composed of four parts according to a typical short-lived flow evolution: the start of the connection (three-way-handshake), the initial slow-start phase, the first loss (or mark) part, and the subsequent losses or marks.

5.1 The Connection Start-Up Phase

Every TCP connection starts with the three-way-handshake process. Assuming that no ACK packets can get lost, this process can be well modeled as follows [7]:

$$E[T_{twhs}] = RTT + T_s(\frac{1-p}{1-2p} - 1), \quad (1)$$

where T_s is the duration of SYN time-out and p is the packet loss ratio.

5.2 The Initial Slow-Start Phase

In order to derive the latency for this phase, $E[Y^{SS}]$, the expected number of packets sent until a loss or a mark occurs is given by following enhanced equation (based on the one given in [7]):

$$E[Y^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q))}{p+q}, \quad (2)$$

where d is the total file size measured in packets that must be transmitted and q is the packet mark ratio.

Substituting the value of $E[Y^{SS}]$ in the Equation (2), we get the expected size of congestion window at the end of the low-start phase due to the packet losses or the packet marks:

$$E[W^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q)) + 2(p+q)}{(p+q)g^2}, \quad (3)$$

where $g = 1.61804$ [7].

The expected slow-start latency is calculated as follows [7]:

$$E[n] = \begin{cases} \lceil log_g(\frac{W_m}{C_1})\rceil + \frac{1}{W_m}(E[Y^{ss}] - g^2 W_m - 2) \\ \qquad , when\ E[W^{ss}] > W_m \\ \lceil log_g(\frac{E[Y^{SS}]+2}{C_1})\rceil - 2 \\ \qquad , when\ E[W^{SS}] \leqq W_m \end{cases} \quad (4)$$

5.3 The First Loss

Assume that the first indication to detect congestion is a packet loss. In the round where a TD (triple-duplicate) occurs, let W^{SS} be the current size of *cwnd*, which has a value w. In this round, w packets were sent. Among them, k packets are assumed to be ACKed. Since the connection is still in the slow-start phase, *cwnd* increases to $w+k$ and another $2k$ packets are sent in the next round. If more then three packets from these $2k$ packets get ACKed, then a TD would occur; otherewise, a TO would take place. Let

$$A(w,k) = \frac{(1-p)^k p}{1-(1-p)^w}, \quad (5)$$

be the probability that the first k packets have been successfully transmitted and ACKed in a round of w packets, provided that there might be one or more packets got lost. Now, let

$$h(m) = \sum_{i=0}^{2}(1-p)^i p, \ for\ m \geqq 3, \quad (6)$$

be the probability that no more than 2 packets have been transmitted successfully in a round of m packets. As [7], we obtain $Q^{SS}(W^{SS})$, the probability that a loss in a window size W^{SS} of slow-start phase is a TO (Timeout), is given by

$$Q^{SS}(W^{SS}) = \begin{cases} 1 & , when\ w \leqq 2 \\ \sum_{k=0}^{1} A(W^{SS},k) & \\ +\sum_{k=2}^{w-1} A(W^{SS},k)h(2k) & , otherwise \end{cases} \quad (7)$$

The expected time that TCP spends in the RTOs is given in [9] as:

$$E[Z^{TO}] = T_0 \frac{f(p)}{1-p}, \quad (8)$$

where T_0 is the average duration of the first time-out, and

$$f(p) = 1 + p + 2p^2 + 4p^3 + 8p^4 + 16p^5 + 32p^6. \quad (9)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Finally, the expected latency that this loss would incur is

$$T_{loss} = \frac{p}{p+q}(1-(1-(p+q))^d) \times (Q(W^{SS})E[Z^{TO}] + (1-Q(W^{SS}))RTT). \quad (10)$$

5.4 Sending the Rest of the Packets

After the first packet loss or the first packet mark, the transmission latency of the rest $(d - E[Y_{init}])$ packets is obtained as follows:

$$T_{rest} = \frac{d - E[Y^{SS}]}{H}, \quad (11)$$

where H is the throughput of a steady-state flow.

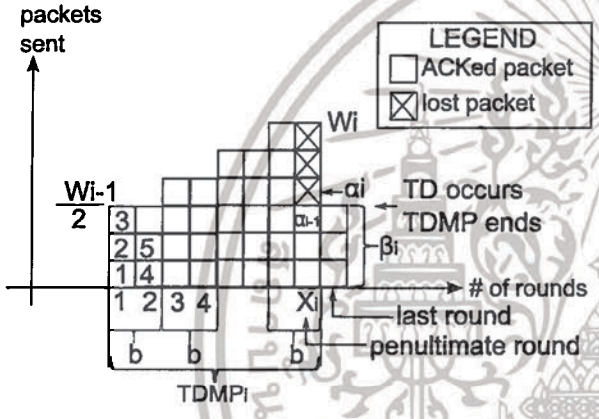


Fig. 7 Pacekts sent during a TDMP when a packet loss occurs.

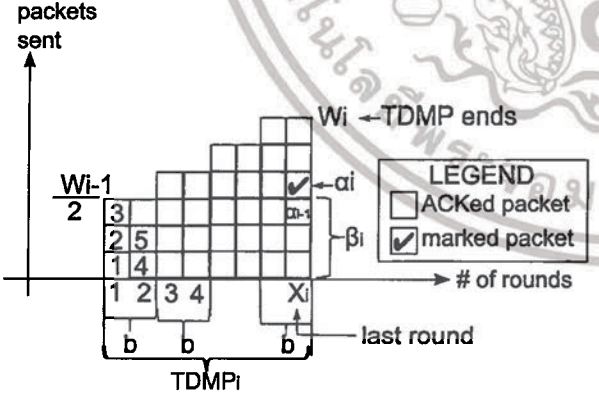


Fig. 8 Packets sent during a TDMP when a marking occurs.

We define TDMP (triple-duplicate or marked period) to be the period between tow triple-duplicate (TD) losses or receipts of marked ACKs. With reference to Fig. 7 when a packet loss occur, and with reference to Fig. 8 when receiving a marked ack, the following enhanced equations are given baesd on [8].

$$Y_i = \begin{cases} \alpha_i + W_i^{TDM} - 1 & ,when\ a\ packet\ loss \\ \alpha_i - (\beta_i + 1) + W_i^{TDM} & ,when\ a\ marked\ ack \end{cases} \quad (12)$$

$$A_i = \begin{cases} \Sigma_{j=1}^{X_i+1} r_{ij} & ,when\ a\ packet\ loss \\ \Sigma_{j=1}^{X_i} r_{ij} & ,when\ a\ marked\ ack \end{cases} \quad (13)$$

$$W_i^{TDM} = \frac{W_{i-1}^{TDM}}{2} + \frac{X_i}{b} - 1, \quad (14)$$

$$Y_i = \begin{cases} \frac{X_i}{2}(\frac{W_{i-1}^{TDM}}{2} + W_i^{TDM} - 1) + \beta_i \\ \qquad ,when\ a\ packet\ loss \\ \frac{X_i}{2}(\frac{W_{i-1}^{TDM}}{2} + W_i^{TDM} - 1) \\ \qquad ,when\ a\ marked\ ack \end{cases} \quad (15)$$

where X_i is the penultimate round in the TDMP which experiences packet losses, r_{ij} is the round trip tim, W_i^{TDM} is the window size at the end of a TDMP, α_i is the number of packets sent in a TDMP until the first loss or the first receipt of a marked ACK happens, and β_i is the number of packets sent before the loss or the receipt of a marked ack in the round.

The expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = \begin{cases} E[\alpha] + E[W^{TDM}] - 1 \\ \qquad ,when\ a\ packet\ loss \\ E[\alpha] - E[\beta] - 1 + E[W^{TDM}] \\ \qquad ,when\ a\ marked\ ack \end{cases} \quad (16)$$

where $E[\alpha]$ is the expected number of packets sent in a TDMP up to and including the first packet that is lost or marked. Given our loss and mark model, the probability that $\alpha_i = k$ is equal to the probability that exactly $k-1$ packets are successfully acknowkedged before a loss or a mark occurs is

$$P[\alpha = k] = (1-(p+q))^{k-1}(p+q), k = 1, 2, \ldots. \quad (17)$$

The mean of α is thus,

$$E[\alpha] = (1-(p+q))^{k-1}(p+q)k = \frac{1}{p+q}. \quad (18)$$

From (16) and (18) it follows that

$$E[Y] = \begin{cases} \frac{1-(p+q)}{p+q} + E[W^{TDM}] \\ \qquad ,when\ a\ packet\ loss \\ \frac{1-(p+q)}{p+q} - E[\beta] + E[W^{TDM}] \\ \qquad ,when\ a\ marked\ ack \end{cases} \quad (19)$$

From [10] the expected round where the first loss or the first mark occurs, $E[X]$, is

$$E[X] = b(\frac{E[W^{TDM}]}{2} + 1). \quad (20)$$

From [10] the expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = \begin{cases} \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) + E[\beta] \\ \qquad ,when\ a\ packet\ loss \\ \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) \\ \qquad ,when\ a\ marked\ ack \end{cases} \quad (21)$$

เอกสารนี้จัดทำขึ้นเพื่อสงวนไว้สำหรับใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Then, from Equations (20), (19) and (21), we get the following expression which involves $E[W^{TDM}]$:

$$\frac{1-(p+q)}{p+q} + E[W^{TDM}] = \frac{E[X]}{2}\left(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1\right) + E[\beta]. \quad (22)$$

For simplicity, we assume β_i to be uniformly distributed between 1 and $W_i - 1$. Thus, $E[\beta] = E[W^{TDM}]/2$.

Combining (20) and (22), we get:

$$E[W^{TDM}] = -\frac{2(b-1)}{3b} + \sqrt{\frac{4(b(p+q)+2(1-(p+q)))}{3b(p+q)} + \left(\frac{2(b-1)}{3b}\right)^2}. \quad (23)$$

From [10], the expected value of duration of a round, $E[A]$, is

$$E[A] = \begin{cases} RTT \cdot (E[X]+1) & ,when\ a\ packet\ loss \\ RTT \cdot E[X] & ,when\ a\ marked\ ack \end{cases} \quad (24)$$

That is,

$$E[A] = \frac{p}{p+q} RTT \cdot (E[X]+1) + \frac{q}{p+q} RTT \cdot E[X] \quad (25)$$

5.5 Impact of Window Limitation

At the beginning of TCP flow establishment, the receiver advertises a maximum buffer size which determines a maximum congestion window size, W_m. As a consequence, during a period without loss indications, the window size can grow up to W_m, but will not grow further beyond this value. During the first TDMP, the window grows linearly up to W_m for U rounds, then remains constant for V rounds, and then a triple-duplicate or marking indication occurs. The expected U rounds, $E[U]$, is as follows [9]:

$$E[U] = \frac{b}{2} W_m. \quad (26)$$

Since Y_i, the number of packets in the ith TDMP, does not depend on window limitation, $E[Y]$ is given by (16):

$$E[Y] = E[\alpha] + W_m - 1. \quad (27)$$

From [9],

$$E[Y] = \frac{3}{4} W_m E[U] + W_m E[V]. \quad (28)$$

Then,

$$\frac{1-(p+q)}{p+q} + W_m = \frac{3b}{8} W_m^2 + W_m E[V]. \quad (29)$$

Thus,

$$E[V] = \frac{1-(p+q)}{(p+q)W_m} + 1 - \frac{3b}{8} W_m. \quad (30)$$

Finally, since $X_i = U_i + V_i$ in ith TDMP, we have

$$E[X] = E[U] + E[V] = \frac{b}{8} W_m + \frac{1-(p+q)}{(p+q)W_m} + 1. \quad (31)$$

The expected number of packets that have been received in a TDMP, $E[Y']$, is

$$E[Y'] = \begin{cases} E[\alpha] + E[\beta] - 1.0 & \\ & ,when\ a\ packet\ loss \\ E[\alpha] + E[W^{TDM}] & \\ \quad -E[\beta] - 1.0 & \\ & ,when\ a\ marked\ ack \end{cases} \quad (32)$$

That is,

$$E[Y'] = \frac{p}{p+q}(E[\alpha] + E[\beta] - 1.0) + \frac{q}{p+q}(E[\alpha] + E[W^{TDM}] - E[\beta] - 1.0) = E[\alpha] + \frac{E[W^{TDM}]}{2} - 1.0. \quad (33)$$

As [9], we obtain $Q(w)$, the probability that a loss in a window size w of congestion-avoidance phase is a TO, is given by

$$Q(w) = \begin{cases} 1\ ,when\ w \leq 3 \\ \sum_{k=0}^{2} A(w,k) + \sum_{k=3}^{w} A(w,k)h(k) \\ ,otherwise \end{cases} \quad (34)$$

The expected number of packets received in the time-out phase,

$$E[R] = 1. \quad (35)$$

Thus, the throughput can be formulated as:

$$H = \frac{E[Y'] + \frac{p}{p+q} Q(W^{TDM}) * E[R]}{E[A] + \frac{p}{p+q} Q(W^{TDM}) * E[Z^{TO}]}. \quad (36)$$

From [7], the total expected latency is

$$T_{latency} = E[T_{twhs}] + E[n]RTT + T_{loss} + T_{rest} - \frac{RTT}{2}. \quad (37)$$

Here, the delay caused by the delayed acknowledgment for the first packet is 0ms. That is, the option of delayed acknowledgment is off.

5.6 Verification

We evaluate our proposal Mark-Reverse ECN scheme by the analytical model of Section 5. and by the network simulator ns-2 using the parameters used and given in the Section 4.1. Fig. 11 and Fig. 12 show that the results of this analytical model are very close to simulation results.

6. Conclusion

In this paper, we proposed a new congestoin notification scheme, named as Mark-Reverse ECN for satellite IP networks. Simulation results show that our scheme acheives

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

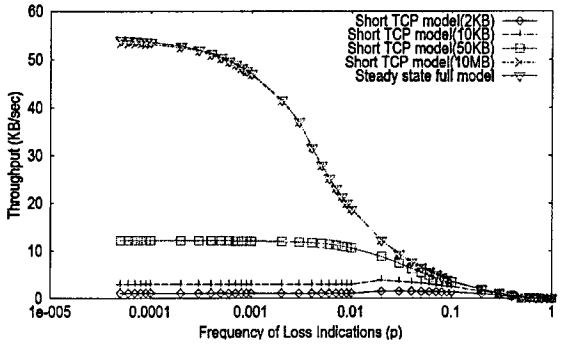


Fig. 9 Throughput predictions given by the short TCP model and the steady state model when drop ratio p is changing and mark ratio is constant $q = 0$. The conditions are: $RTT = 550ms$, $MSS = 1,000bytes$, $T_S = T_0 = 1sec$, $W_m = 30segments$, $b = 1$.

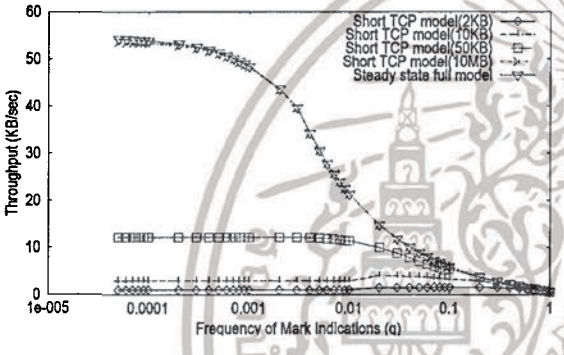


Fig. 10 Throughput predictions given by the short TCP model and the steady state model when drop ratio is constant $p = 0$ and mark ratio is changing. The conditions are: $RTT = 550ms$, $MSS = 1,000bytes$, $T_S = T_0 = 1sec$, $W_m = 30segments$, $b = 1$.

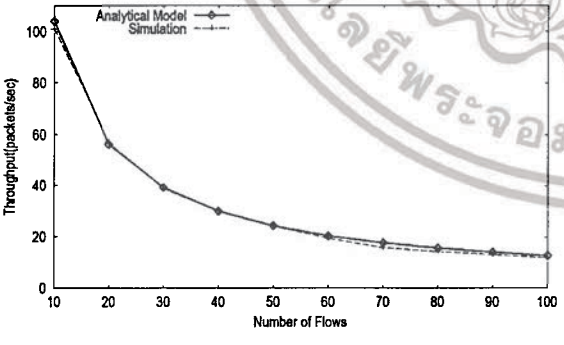


Fig. 11 Throughput comparisons between analytical model and simulation for Mark-Reverse ECN.

higher throughput than the conventional scheme. Analytical results also shows our superiority, correspondingly. A good match between analysis and simulation curves can be observed and validates our results.

REFERENCES

[1] F. Akujobi, I. Lambadaris, R. Makkar, N. Seddigh, and B. Nandy, "BECN for Congestion Control in TCP/IP Neworks: Study and Comparative Evaluation", *IEEE Globecom 2002*, Nov. 2002.

[2] S. Floyd, V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance", *IEEE/ACM Trans. Networking*, vol.1, no.4, August 1993.

[3] RFC 5927, "ICMP Attacks against TCP", July 2010.

[4] S. Floyd, "TCP and Explicit Congestion Notification", Computer Communications Review, vol. 24, no. 5, Oct. 1994.

[5] C. Liu, R. Jain, "Improving Explicit Congestion Notification with the Mark-Front Strategy", Computer Networks (elsevier), vol.35, issue 2-3, Feb. 2001.

[6] UCB/LBNL/VINT Nework Simulatior (NS).

[7] D. Zheng, G. Y. Lazarou, and R. Hu, "A Stochastic Model for Short-lived TCP Flows", IEEE International Conference on Communications 2003 (ICC 2003), May 2003, pp.11-15.

[8] N. Cardwell, S. Savage, and T. Anderson, "Modeling TCP Latency", in Proc. *IEEE INFOCOM 2000*, vol. 3, Mar. 2000, pp.1742-1751.

[9] J. Padhye, V. Firouiu, D. F. Towsley, and J. F. Kurose, "Modeling TCP Reno Performance: A Simple model and its Empirical Validation", *IEEE/ACM Trans. Networking*, vol. 8, no. 2, pp.133-145, Apr. 2000.

[10] D. Zheng, "On the modeling of TCP latency and throughput", Master's thesis Mississippi State University, 2002.

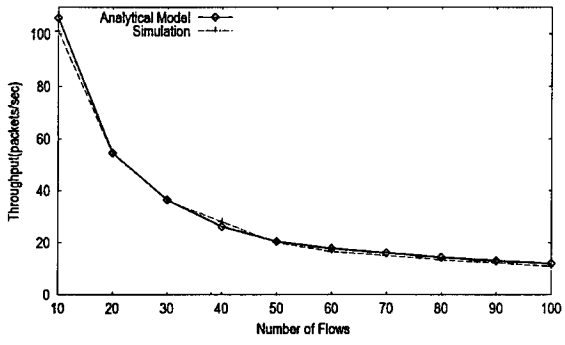


Fig. 12 Throughput comparisons between analytical model and simulation for Mark-Tail ECN.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทความสิ่งประดิษฐ์

การประชุมวิชาการ งานวิจัย และพัฒนาเชิงประยุกต์ ครั้งที่ 6 การพัฒนาเทคโนโลยีเพื่อให้โลกมีสันติสุข

ECTI-CARD Proceedings 2014, Chiang Mai, Thailand

การพัฒนาระบบสื่อสาร สมาร์ทโฟนด้วยเทคโนโลยี WiFi-Direct

Development of Smartphone Networks with WiFi-Direct

ธีรพงษ์ โชคสถิตย์ , เบญจพร ปาวะรีย์ และ สุเมธ ประภาวัต

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

E-mail: TeerapongC@outlook.com , iiniim20421@gmail.com , sumet@it.kmitl.ac.th

บทคัดย่อ

จากการสื่อสารผ่านสายสัญญาณบนเครือข่ายแลน จนถึงการสื่อสารไร้สายผ่านอุปกรณ์พกพาขนาดเล็ก รูปแบบการสื่อสารได้รับการพัฒนาปรับปรุงอย่างต่อเนื่อง ทั้งในเรื่องความสะดวกสบาย ความรวดเร็วในการสื่อสาร ความถูกต้องของข้อความที่ปลายทางได้รับ และความยืดหยุ่นในการใช้งาน ด้วยเหตุนี้ผู้เขียนจึงให้ความสนใจในการพัฒนาศักยภาพของระบบสื่อสารระหว่างสมาร์ทโฟน (Smartphone) เพื่อสนับสนุนกิจกรรมการสื่อสาร ในกรณีที่ระบบสาธารณูปโภคพื้นฐานไม่สามารถใช้การได้ ยกตัวอย่างเช่น การแจ้งเหตุป้องกันหรือการขอความช่วยเหลือ จากเหตุการณ์ภัยพิบัติ เป็นต้น

คำสำคัญ: Smartphone Networks; WiFi-Direct; Ad hoc Network

Abstract

From communication via data signals in LAN network to wireless communication via small portable devices. Form of communication has been developed continuously. In terms comfort and speed of communication. The accuracy of the text has received at destination. And resilience in applications. Thus, this project foresees potential for a study on smartphone ad hoc networks to support the activities communication infrastructures could not rely on it. For example, notifications or requests for assistance from catastrophic events. The ad hoc networks are expected to communicate support for the people who need it when such a situation arises.

Keyword: Smartphone Networks; WiFi-Direct; Ad hoc Network

1. บทนำ

ระบบสื่อสารเป็นสิ่งจำเป็น มีบทบาท และเป็นส่วนสนับสนุนสำคัญของกิจกรรมต่างๆ อย่างเช่น การแจ้งเหตุป้องกันหรือการขอความช่วยเหลือ จากเหตุการณ์ภัยพิบัติ จากการศึกษาพบว่า เหตุการณ์ภัยพิบัติมักจะก่อให้เกิดความเสียหายแก่สาธารณูปโภคพื้นฐานของระบบเครือข่ายสื่อสาร เช่น สถานีฐาน (Base Station) หรือเสากระจายสัญญาณ เป็นเหตุให้ระบบสื่อสารไม่สามารถใช้การได้

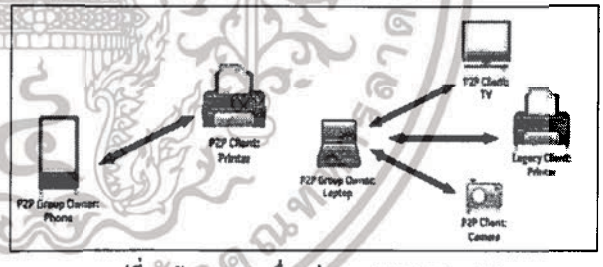
ระบบสื่อสารสำรองจึงมีความสำคัญ การพัฒนาระบบสื่อสารระหว่างสมาร์ทโฟน จึงเป็นการสร้างแอพลิเคชั่นเพื่อเชื่อมต่อระหว่างสมาร์ทโฟนเครื่องหนึ่งไปยังสมาร์ทโฟนอีกเครื่องหนึ่ง ให้สามารถแลกเปลี่ยนข้อมูลข่าวสาร ซึ่งเป็นช่องทางการสื่อสารที่ไม่ต้องพึ่งพาสาธารณูปโภคพื้นฐาน โดยอาศัยเทคโนโลยี Wi-Fi Direct นั่นเอง

2. ทฤษฎีและหลักการ

2.1 Wi-Fi Direct

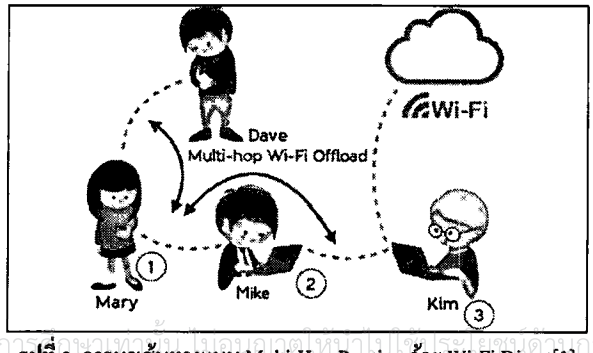
Wi-Fi Direct คือ เทคโนโลยีการสื่อสารตามมาตรฐาน Wi-Fi มีการเชื่อมต่อลักษณะ Peer-to-Peer โดยผู้ใช้สามารถเชื่อมต่อกับอุปกรณ์อื่นๆ ได้โดยตรง ไม่จำเป็นต้องติดต่อกับเครือข่ายโครงสร้างพื้นฐาน (Infrastructure network)

Wi-Fi Direct เริ่มต้นการทำงานโดยอุปกรณ์จะสร้างการเชื่อมต่อไปยังอุปกรณ์ใกล้เคียง เพื่อแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ทั้งสองโดยตรง ซึ่งการส่งสารในลักษณะนี้เรียกว่า 1 Hop ทั้งนี้ผู้ใช้ต้องร้องขอการเชื่อมต่อกับอุปกรณ์ใกล้เคียงผ่าน Wi-Fi Protected Setup ที่รักษาความปลอดภัยในการเชื่อมต่อด้วย industry-standard WPA2 security และเมื่ออุปกรณ์ทั้งสองเชื่อต่อกัน การเชื่อมต่อจะอยู่ในรูปแบบของ Wi-Fi Direct Group เพราะฉะนั้นอุปกรณ์ทั้งสองจะสามารถบริการได้ทุกอย่างที่อยู่บนมาตรฐานของ Wi-Fi Direct ดังรูปที่ 1 [1][2]



รูปที่ 1. ลักษณะการเชื่อมต่อของ Wi-Fi Direct[1]

แต่ Wi-Fi Direct มีข้อจำกัดคือรองรับการเชื่อมต่อเพียง 1 Hop เพราะฉะนั้นจะไม่สามารถนำมาใช้ในสถานการณ์ปกติได้ เพราะการสื่อสารประกอบไปด้วยเส้นทางย่อยหลาย Hop (Multi-Hop) จึงต้องประยุกต์ใช้การส่งต่อจากโหนดหนึ่งไปยังอีกโหนดหนึ่ง ต่อเนื่องหลาย Hop จนกระทั่งข้อความถูกส่งไปถึงปลายทาง ดังในรูปที่ 2

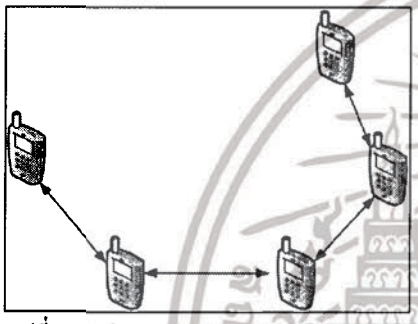


รูปที่ 2. การหาเส้นทางแบบ Multi-Hop Routing ด้วย Wi-Fi Direct[1]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 Mobile Ad hoc Network (MANET)

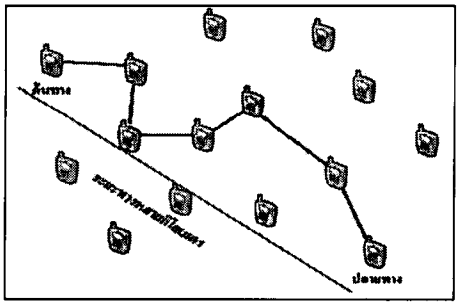
เครือข่ายไร้สายเฉพาะกิจ (Mobile Ad Hoc Network - MANET) ทำให้โหนดเคลื่อนที่แบบไร้สาย (Wireless Mobile Node) สามารถทำการสื่อสาร ในขณะกำลังสื่อสารได้อย่างอิสระ ผ่านการจองเส้นทางล่วงหน้าก่อนการส่งข้อมูลได้ ดังนั้นจึงสามารถนำมาปรุยุกต์ใช้บนเครือข่ายสื่อสารชั่วคราวที่ไม่จำเป็นต้องมีโครงสร้างพื้นฐาน เช่น เสากระจายสัญญาณ (Base Station) และเปลี่ยนการควบคุมของศูนย์กลางการควบคุม (Centralized Administration) เป็นการอาศัยความร่วมมือกันระหว่างโหนดในการส่งต่อข้อมูล โดยโหนดจะปฏิบัติตัวเองเป็นเสมือนเราเตอร์ (Router) ส่งต่อข้อมูลระหว่างจากโหนดหนึ่งไปยังอีกโหนดหนึ่ง ต่อเนื่องไปจนถึงโหนดปลายทางดังรูปที่ 3 [3][4]



รูปที่ 3.ตัวอย่างของ Mobile Ad hoc Networks[3]

2.3 Delay-Tolerant Network (DTNs)

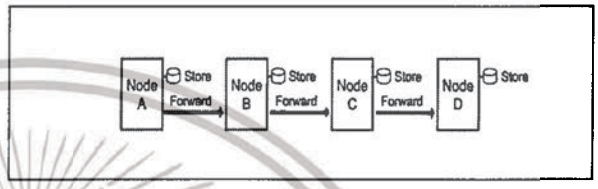
เครือข่ายที่มีความคงทนต่อความหน่วง (เครือข่ายดีทีเอ็น) เป็นเทคโนโลยีที่ทำให้เกิดการติดต่อสื่อสารบนพื้นที่เฉพาะ(Regions) ซึ่งเทคโนโลยีเครือข่ายในปัจจุบันไม่สามารถนำไปใช้ในทางปฏิบัติได้ เนื่องจากการสื่อสารบนพื้นที่เฉพาะนั้น โหนดและช่องทางการเชื่อมต่อระหว่างโหนด(Link) อาจจะมีปัญหาในเรื่องความน่าเชื่อถือ เช่น มีโอกาสในการเชื่อมต่อกันได้ยาก หากเกิดการเชื่อมต่อก็จะเกิดขึ้นเพียงแค่ในช่วงระยะเวลาสั้นๆเท่านั้น อันเป็นสาเหตุให้เกิดความผิดพลาดของข้อมูล ข้อมูลบางส่วนขาดหายระหว่างส่ง หรือการขาดการเชื่อมต่อของเครือข่ายเป็นเวลานาน ซึ่งปัญหาเหล่านี้ก็จะส่งผลกระทบต่อความแปรปรวนของ Hop (ช่องทางการส่งข้อมูลระหว่าง router หนึ่งๆ) หรือช่องทางการส่งข้อมูลของ router [5]



รูปที่ 4. ตัวอย่างของ Delay-Tolerant Networks[5]

ลักษณะเด่นของเครือข่ายดีทีเอ็น คือการสร้างการเชื่อมต่อระหว่างอุปกรณ์ Mobile Device ในสถานการณ์ที่ Network ไม่สามารถสร้าง End to End Connection ได้ เพื่อให้เกิดการติดต่อสื่อสาร ซึ่งจะเป็นการทำให้ Network มีความกว้างขึ้น จากเทคโนโลยี Wire และ Wireless ดังรูปที่ 4

กระบวณการทำงานของดีทีเอ็นนั้น จะมีลักษณะการทำงานโดย ทำการเชื่อมโยงโปรโตคอลของเครือข่าย ที่ยอมให้สามารถเกิดการติดต่อกันระหว่างอุปกรณ์สัญญาณได้ แม้ว่า Network จะไม่ได้มีการเชื่อมต่ออยู่ตลอดเวลาก็ตาม ซึ่งโหนดใด ๆ ที่อยู่ระหว่างโหนดต้นทางกับโหนดปลายทางอาจจะต้องทำหน้าที่ในการช่วยรับข้อมูลแล้วส่งต่อ ทำให้การส่งสามารถส่งถึงปลายทางได้ ดังรูปที่ 5



รูปที่ 5. กระบวณการทำงานของดีทีเอ็น [5]

โดยตัวอย่างกลไกการส่งข้อความบนเครือข่ายดีทีเอ็นเช่น Direct Mail, Gradient Routing และ Epidemic Routing เป็นต้น [8][9]

3. การวิเคราะห์และออกแบบ

3.1 ความต้องการของระบบ

3.1.1 ความต้องการหลักของระบบ

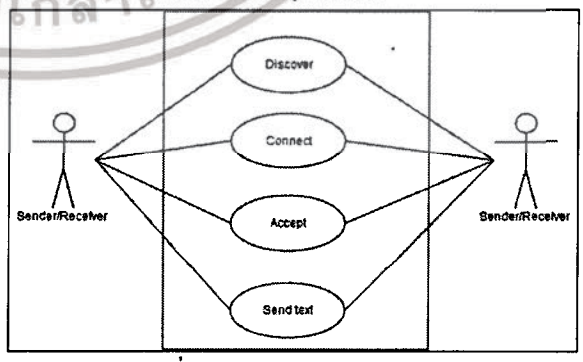
- สามารถค้นหาผู้ใช้อื่น
- เชื่อมต่อเข้ากับผู้ใช้อื่นที่ต้องการ
- สามารถสร้างข้อความและส่งข้อความ
- ยอมรับการเชื่อมต่อจากผู้ขอทำการเชื่อมต่อกลับได้

3.1.2 ความต้องการของระบบที่ไม่ใช่ หน้าที่หลักของระบบ

- ผู้ใช้งานระบบต้องเปิดสัญญาณ Wi-Fi Direct

3.2 ภาพรวมของระบบ

จากความต้องการของระบบ แสดงภาพรวมของระบบสื่อสารระหว่างสมาร์ทโฟนด้วย WiFi-Direct ได้ ดังรูปที่ 6 ดังนี้

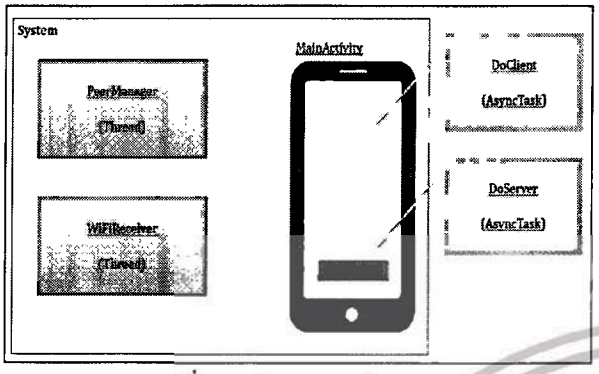


รูปที่ 6. ยูสเคสไดอะแกรมของระบบ

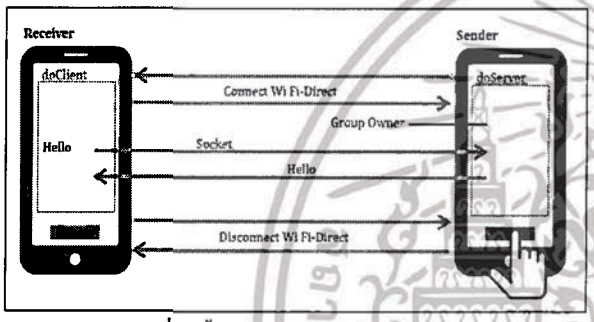
ภายในระบบจะประกอบไปด้วย เทรดสองชนิด ได้แก่ PeerManager ที่ทำหน้าที่ เกี่ยวกับการติดต่อจากผู้ที่เข้ามาร้องขอการเชื่อมต่อ และ WiFiReciever จะทำหน้าที่ดูแลการเชื่อมต่อของเทคโนโลยี WiFi-Direct กับการทำงานของเครื่อง และในส่วนของตัวเครื่อง(MainActivity) มีการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ แจกจ่าย หรือทำสำเนาเพื่อการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใช้ AsyncTask เพื่อสลับหน้าที่การทำงานของเครื่องไปมาระหว่าง Client และ Server ดังในรูปที่ 7 และ 8



รูปที่ 7. องค์ประกอบภายในระบบ



รูปที่ 8. ขั้นตอนการทำงานภายในระบบ

4. ผลการทำงานของระบบ

จากการทดลองการใช้งานแอพพลิเคชั้นที่พัฒนาขึ้น เพื่อส่งข้อความระหว่างสมาร์โฟน ด้วยWiFi-Direct แสดงผลดังรูปที่ 9, 10 และ 11



รูปที่ 9. แสดงการตั้งชื่อเครื่อง และพิมพ์ข้อความเพื่อส่งไปให้เครื่องถัดไป



รูปที่ 10. แสดงข้อความที่ได้รับจากการส่งข้อความผ่าน **WiFi-Direct**



รูปที่ 11. แสดงการส่งข้อความกลับไปยังเครื่องต้นทาง

5. สรุปผลทำงานของระบบและแนวทางในการพัฒนาต่อยอด

ระบบสื่อสารระหว่างสมาร์ทโฟนด้วย WiFi-Direct เป็นระบบที่สามารถสร้างช่องทาง เพื่อการสื่อสารหรือส่งข้อมูล โดยไม่ต้องพึ่งพาระบบสาธารณูปโภคพื้นฐาน เหมือนในระบบสื่อสารทั่วไป โดยอาศัยการทำงานของเทคโนโลยี WiFi-Direct ซึ่งจากการทำการทดลองการทำงานของระบบ แสดงให้เห็นว่า สามารถแลกเปลี่ยนข้อความระหว่างสมาร์ทโฟนแบบ 1-Hop ได้

ในการพัฒนาระบบทำให้เล็งเห็นถึงความเป็นไปได้ ในการพัฒนาให้ระบบสามารถส่งข้อมูลแบบ Multi-Hop ซึ่งจะทำให้ระบบมีประสิทธิภาพเกิดความเหมาะสมต่อการนำไปประยุกต์ใช้ได้มากขึ้น จึงมีการเสนอแนวทางการพัฒนาต่อในอนาคต โดยจะศึกษาความท้าทายในการสื่อสารของเครือข่ายไร้สายเคลื่อนที่ ขีดจำกัดการทำงานของเทคโนโลยี WiFi-Direct และศึกษาเทคโนโลยีเครือข่าย ซึ่งปัจจุบันมีเทคโนโลยีเครือข่ายไร้สายเคลื่อนที่ ที่ได้รับความสนใจคือ เทคโนโลยีเครือข่ายมาเน็ต (MANET : Mobile Ad-hoc Network) และเทคโนโลยีเครือข่ายดีทีเอ็น (DTN : Delay Tolerant Network) ซึ่งจะใช้ในการศึกษาเพื่อสร้างเครือข่ายเฉพาะกิจเพื่อนำมาใช้ในการพัฒนาระบบต่อไป[7]

โดยได้มีการวิเคราะห์ประสิทธิภาพของเครือข่ายที่มีความเหมาะสมต่อการนำมาใช้งานแล้ว สรุปได้โดยย่อว่า การนำสมาร์ทโฟนมาสร้างการเชื่อมต่อกันโดยตรง เป็นช่องทางการสื่อสารสำรอง แทนการเชื่อมต่อเข้าระบบสื่อสารหลักที่ล้มเหลว อันเนื่องมาจากสถานีฐานหรือเสากระจายสัญญาณได้รับความเสียหาย จำเป็นต้องอาศัยเทคโนโลยีการสื่อสารแบบไร้สาย (Wi-Fi) เพื่อสร้างเป็นเครือข่ายสื่อสารเฉพาะกิจของสมาร์ทโฟน ทำให้ผู้ใช้สมาร์ทโฟนสามารถทำการติดต่อสื่อสารระหว่างกันได้ แต่ทั้งนี้การที่สมาร์ทโฟนเป็นอุปกรณ์สื่อสารที่มีการเคลื่อนที่ตลอดเวลา และมีพลังงานที่จำกัด เป็นปัญหาสำคัญต่อประสิทธิภาพการทำงานของเครือข่ายสื่อสาร

เนื่องจากการสื่อสารเฉพาะกิจของสมาร์ทโฟน เป็นรูปแบบหนึ่งของเครือข่ายไร้สายเคลื่อนที่ จึงมีปัจจัยของปัญหาในการสื่อสาร[6]ดังต่อไปนี้

1. การเชื่อมต่อที่ไม่สม่ำเสมอ เป็นการขาดช่วงของเส้นทางการสื่อสารระหว่างผู้ส่งสารกับผู้รับสาร(Network Partitioning) เป็นผลมาจากการเคลื่อนที่อย่างไม่แน่นอนของโหนดในเครือข่าย

เอกสารนี้ใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ความหน่วงมีค่าสูง เนื่องจากเป็นการสื่อสารในเครือข่ายไร้สายเคลื่อนที่ จึงทำให้เกิดปัญหาเกี่ยวกับ ดีเลย์ในการส่งข้อมูลระหว่างโหนดมีค่ามาก และมีความแปรปรวนของดีเลย์ที่เกิดจากการรอคิว

3. ความไม่สมดุลของอัตราการส่งข้อมูล ในสถานการณ์จริง ความแตกต่างของพื้นที่ในการสื่อสารและความสามารถในการสื่อสารของโหนด ส่งผลให้เกิดความไม่สมดุลของอัตราการส่งข้อมูลมากเกินรองรับได้

4. อัตราความผิดพลาดสูง เมื่อพิจารณาลักษณะของการสื่อสารในเหตุการณ์ภัยพิบัติ เช่น โหนดมีการเคลื่อนที่ สภาพพื้นที่กีดขวางการสื่อสาร เป็นต้น ทำให้อัตราความผิดพลาดสูงกว่าเครือข่ายทั่วไป

เมื่อพิจารณาเครือข่ายมาเน็ตพบว่า การที่โหนดต้นทางต้องค้นหาเส้นทางเพื่อเชื่อมต่อไปยังโหนดปลายทาง จากนั้นจึงเริ่มทำการส่งข้อมูล ซึ่งการสื่อสารอาจเกิดความขัดข้องหรือล้มเหลวได้ จากปัญหาที่โหนดต้นทางไม่สามารถหาเส้นทางได้ ในกรณีที่เครือข่ายมีความหนาแน่นของโหนดน้อย หรือปัญหาการเชื่อมโยงขาดอันเนื่องมาจากการเคลื่อนที่ของโหนด รวมไปถึงปัญหาการพลาดโอกาสเลือกโหนดรับช่วงต่อ(ที่ดีกว่า)ที่พึ่งเข้ามาในรัศมีการสื่อสารด้วย โดยปัญหาเหล่านี้มักพบบ่อยในเครือข่ายมาเน็ต

แต่ในเครือข่ายดีทีเอ็น โหนดไม่จำเป็นต้องมีการสร้างเส้นทางเชื่อมระหว่างโหนดต้นทางกับโหนดปลายทาง การส่งต่อข้อมูลจะเกิดขึ้นผ่านโหนดรับช่วงต่อสามารถถูกเลือกจากโหนดจร(Mobile Node) ใดๆก็ได้ ที่เป็นไปตามเงื่อนไขที่ถูกกำหนดขึ้นเพื่อโอกาสสำเร็จในการส่งข้อมูลไปปลายทาง จากความยืดหยุ่นในการเลือกโหนดรับช่วงต่อที่เหมาะสมของเครือข่ายดีทีเอ็นนี้ จึงสามารถแก้ไขปัญหาที่เกิดในเครือข่ายมาเน็ตได้

เพราะฉะนั้นแนวทางการพัฒนาต่อเนื่องในอนาคตคือ นำกลไกการส่งข้อความแบบ 1 Hop ของสมาร์ทโฟนผ่าน WiFi-Direct มาสร้างการส่งข้อความแบบ Multipath routing บนเครือข่ายดีทีเอ็น ซึ่งหมายถึงการฝากและส่งต่อข้อความไปกับโหรดจรใด ๆ อย่างต่อเนื่อง จนกระทั่งข้อความถูกส่งไปให้โหนดปลายทางนั่นเอง

เอกสารอ้างอิง

[1] Wi-Fi CERTIFIED Wi-Fi Direct™ Consumer. Reading: Wi-Fi Alliance®, October 2010.

[2] Wi-Fi CERTIFIED Wi-Fi Direct™ Industry. Reading: Wi-Fi Alliance®, October 2010.

[3] M. K. Jeya Kumar, R. S. Rajesh. "A Survey of MANET Routing Protocols in Mobility Models." Medwell Journals, 2009. [Available Online]: http://www.medwelljournals.com /fulltext/?doi=ijscomp.2009.136.141

[4] Sunil Taneja, Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks." Reading: International Association of Computer Science and Information Technology, August 2010.

[5] Forrest Warthman, Delay- and Disruption- Tolerant Network(DTNs): A Tutorial. Reading: Interplanetary Internet Special Interest Group, July 2012.

[6] Forrest Warthman, Delay- and Disruption- Tolerant Network(DTNs): A Tutorial. Reading: Interplanetary Internet Special Interest Group, July 2012.

[7] Laurent Franck, Performance comparison of mobile ad-hoc and delay tolerant network. [Available Online]: http://www-public.int-evry.fr/~kohlenb/sites_web_projets/i_pluton/Livrables/i%20Pluton%2011%20_%20Manets%20_%20DTN.pdf

[8] Samo Grasic, Anders Lindgren, An Analysis of Evaluation Practices for DTN Routing Protocols. [Available Online]: http://soda.swedish-ict.se/5290/1/practices-camerarready.pdf

[9] Evan P.C. Jones, Paul A.S. Ward, Routing Strategies for Delay-Tolerant Networks. [Available Online]: http://ccng.uwaterloo.ca/~pasward/Publications/dtn-routing-survey.pdf

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การประยุกต์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉินและตำแหน่งที่อยู่ เพื่อขอรับบริการรถนำส่งและบริการทางการแพทย์

สุเมธ ประภาวัต ธนานพ ทองถาวร และ ณัชชา วัฒนอรุณกิจ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: sumet@it.kmitl.ac.th, St_freedom2@hotmail.com, ZinreF@gmail.com

บทคัดย่อ

ในปัจจุบันผู้ป่วยฉุกเฉินวิกฤตที่มีสาเหตุมาจากอาการเจ็บป่วยหรืออุบัติเหตุมีมากกว่า 200,000 รายต่อปี โดยระบบที่ใช้ในการรองรับผู้ป่วยดังกล่าวคือ ระบบสายด่วนฉุกเฉิน 1669 ซึ่งเป็นระบบการแจ้งเหตุผ่านทางโทรศัพท์เพื่อแจ้งที่อยู่ และอาการของผู้ป่วยแก่เจ้าหน้าที่ ก่อนที่เจ้าหน้าที่จะทำการช่วยเหลือต่อไป ซึ่งในบทความฉบับนี้จะกล่าวถึงการประยุกต์ใช้งานระบบระบุตำแหน่งบนพื้นโลกและสมาร์ทโฟนเพื่อใช้ในการระบุตำแหน่งของผู้ป่วยหรือพื้นที่ที่เกิดอุบัติเหตุ ก่อนที่จะส่งความช่วยเหลือทางการแพทย์ที่เหมาะสมไปยังผู้ป่วย โดยมีระบบช่วยตัดสินใจในการคัดกรองเส้นทางและเลือกทรัพยากรที่จำเป็นต่อการช่วยเหลือผู้ป่วยเพื่อลดระยะเวลาปฏิบัติการที่ใช้ในการตัดสินใจของเจ้าหน้าที่ ซึ่งจะส่งผลให้ผู้ป่วยมีอัตราการรอดชีวิตหรือรอดพ้นจากสภาวะพิการที่คาดเกิดขึ้นในขณะที่ทำการช่วยเหลือผู้ป่วยมากขึ้น และหลังจากศึกษาบทความนี้ ผู้อ่านจะได้ทราบถึงแนวคิดและวิธีการดำเนินงานของระบบ บทสรุป และแนวทางการพัฒนาต่อยอดของงานชิ้นนี้ต่อไป

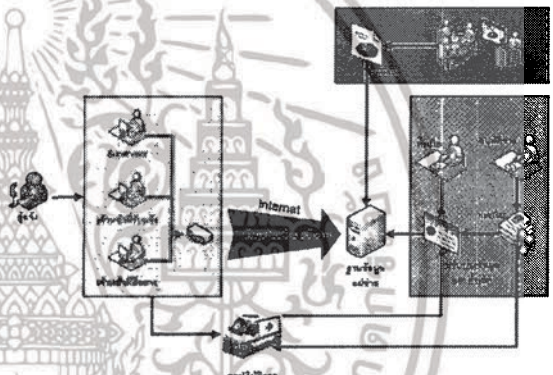
คำสำคัญ— แจ้งเหตุผ่านสมาร์ทโฟน; ระบบช่วยตัดสินใจ; การช่วยชีวิต

1. บทนำ

ในปัจจุบันสมาร์ทโฟนเป็นอุปกรณ์สื่อสารที่ได้รับความนิยมและสามารถพบเห็นได้ทั่วไป เนื่องจากสามารถเชื่อมต่ออินเตอร์เน็ตและระบุตำแหน่งบนพื้นโลกได้ ประกอบกับระบบที่ใช้ในการแจ้งเหตุฉุกเฉินในปัจจุบันยังคงใช้วิธีการติดต่อสื่อสารกับผู้ป่วยผ่านทางโทรศัพท์โดยตรง[1] ในการสอบถามอาการและที่อยู่ของผู้ป่วย ซึ่งต้องใช้เวลาและปัจจัยอีกหลายอย่างมาเกี่ยวข้องเพื่อทำให้การสื่อสารในลักษณะนี้ประสบความสำเร็จในสภาวะฉุกเฉิน จึงมีแนวคิดในการประยุกต์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉินเพื่อช่วยเพิ่มช่องทางในการแจ้งเหตุฉุกเฉินและลดระยะเวลาการติดต่อสื่อสารกับเจ้าหน้าที่ในการแจ้งเหตุฉุกเฉิน ประกอบกับระบบช่วยตัดสินใจในส่วนของเจ้าหน้าที่ซึ่งสามารถช่วยลดระยะเวลา และปริมาณข้อมูลที่ใช้ในการตัดสินใจ ส่งผลให้การช่วยเหลือผู้ป่วยมีประสิทธิภาพมากยิ่งขึ้น

2.ทฤษฎีและงานที่เกี่ยวข้อง

2.1 ระบบสนับสนุนการช่วยเหลือผู้ประสบเหตุ



รูปที่ 1. ภาพรวมของระบบ สพฉ.

ปัจจุบันมีหลายหน่วยงานที่ให้บริการนำส่งผู้ป่วยเหตุฉุกเฉินไม่ว่าจะเป็นภาครัฐหรือเอกชน สถาบันการแพทย์ฉุกเฉินแห่งชาติเป็นหน่วยงานหลักหน่วยหนึ่งที่ได้รับมอบหมายในการให้บริการดังกล่าว ซึ่งเป็นที่รู้จักกันในนาม "บริการสายด่วนฉุกเฉิน 1669[2]" ในการรับแจ้งเหตุฉุกเฉิน โดยมีเจ้าหน้าที่เป็นผู้ประสานงาน ทำหน้าที่ในการรับการแจ้งเหตุจากผู้ป่วย ตัดสินใจเลือกรถนำส่งและสถานพยาบาล ในส่วนของระบบสารสนเทศจะมีบทบาทเพียงแค่การรวบรวมผลรายงาน และการอนุมัติการเงินในการรักษาเท่านั้น ซึ่งหน่วยงานอื่นที่มาร่วมให้บริการ อย่างเช่น หน่วยรับแจ้งเหตุของโรงพยาบาลหรือมูลนิธิอาสาสมัครต่างๆ ก็มีรูปแบบการทำงานที่ไม่แตกต่างกันมากนัก

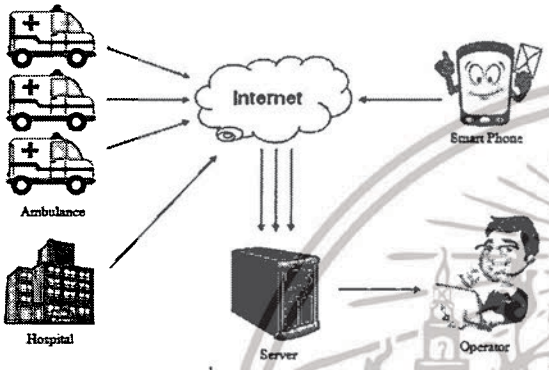
2.2 ระบบดาวเทียมนำร่อง

ระบบดาวเทียมนำร่องถูกพัฒนาขึ้นเพื่อระบุพิกัดสำหรับอ้างอิงตำแหน่งบนพื้นโลก อย่างเช่น ระบบจีพีเอส[3] ซึ่งเป็นหนึ่งในระบบนำร่องสำหรับการระบุตำแหน่งที่ถูกใช้กันอย่างแพร่หลาย โดยใช้ดาวเทียมเข้ามาช่วยในการคำนวณตำแหน่งต่างๆ ซึ่งในการระบุตำแหน่งต่างๆ นั้น ภายในอุปกรณ์ที่จะถูกระบุตำแหน่งจำเป็นต้องมีอุปกรณ์รับสัญญาณจากดาวเทียมติดตั้งอยู่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากนั้นในการคำนวณตำแหน่งของอุปกรณ์รับสัญญาณจะประมวลผลจากการรับสัญญาณดาวเทียมมากกว่าสามดวงขึ้นไป เพื่อหาพื้นที่คาบเกี่ยวระหว่างดาวเทียมทั้งหมดโดยใช้ Triangulation Method ซึ่งจะทำให้ทราบว่า อุปกรณ์รับสัญญาณนั้นอยู่ในพิกัดละติจูดและลองจิจูดที่เท่าไร นอกจากระบบจีพีเอสแล้วยังมีอีกหลายระบบอาทิเช่น โกลนาสของรัสเซีย กาลิเลโอของยุโรป คอมพาสของจีน เป็นต้น แต่ระบบเหล่านี้ส่วนใหญ่ยังไม่ถูกรองรับในอุปกรณ์สมาร์ทโฟนในไทย

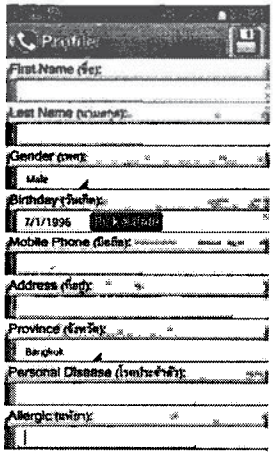
3. แนวคิดและการดำเนินงาน



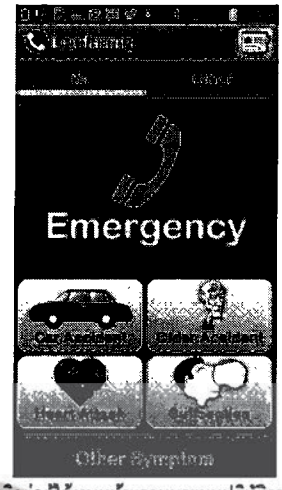
รูปที่ 2. ภาพรวมของระบบ

จากรูปที่ 2 หลังจากมีการส่งข้อมูลของผู้ป่วยเข้ามาที่เซิฟเวอร์แล้วระบบจะทำการตรวจสอบพิกัดจีพีเอสที่จุดเกิดเหตุและทำการค้นหาโรงพยาบาลและรถนำส่งที่อยู่ใกล้กับจุดเกิดเหตุ เพื่อสร้างตารางเส้นทางระหว่างโรงพยาบาลและรถนำส่งที่เหมาะสม โดยคำนึงถึงอาการของผู้ป่วยเป็นสำคัญ เพื่อให้สามารถเลือกรถนำส่งที่เหมาะสมไปทำการช่วยเหลือผู้ป่วยได้ ในกรณีที่ไม่สามารถระบุอาการได้ระบบจะนำประวัติส่วนตัวของผู้ป่วยมาประมวลผลแทน จากนั้นเจ้าหน้าที่จะทำการตัดสินใจครั้งสุดท้ายในการเลือกเส้นทางจากตารางที่ระบบสร้างขึ้น และประสานงานไปยังเจ้าหน้าที่ประจำรถนำส่งเพื่อทำการช่วยเหลือผู้ป่วยต่อไป

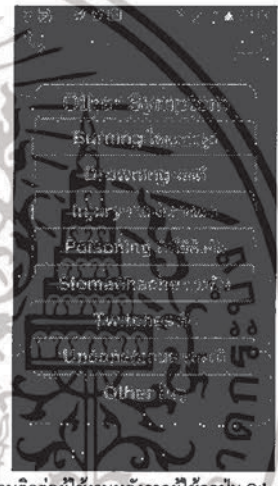
3.1. แอพพลิเคชั่นบนสมาร์ทโฟน



รูปที่ 3. ส่วนติดต่อผู้ใช้งานหลังจากผู้ใช้กดปุ่ม Profile (มุมขวา)



รูปที่ 4. ส่วนติดต่อผู้ใช้งานหน้าแรกบนระบบปฏิบัติการแอนดรอยด์



รูปที่ 5. ส่วนติดต่อผู้ใช้งานหลังจากผู้ใช้กดปุ่ม Other Symptom

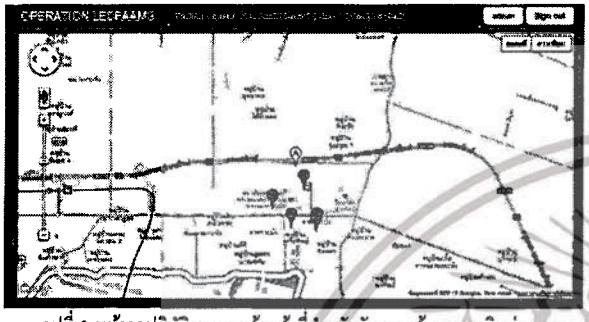
ระบบนี้ถูกพัฒนามาจากงานวิจัยการศึกษาการใช้งานระบบจีพีเอส[4][5] ซึ่งในการแจ้งเหตุฉุกเฉินผู้ป่วยจะต้องเรียกใช้งานแอพพลิเคชั่นบนสมาร์ทโฟนในการแจ้งเหตุฉุกเฉิน โดยจะมีการเก็บบันทึกประวัติส่วนตัวของผู้ป่วยเอาไว้ดังรูปที่ 3 ในกรณีที่เกิดเหตุฉุกเฉินและผู้ป่วยไม่มีสติมากพอที่จะตัดสินใจ ผู้ป่วยสามารถกดปุ่ม "Emergency" ดังรูปที่ 4 เพื่อแจ้งเหตุฉุกเฉิน หรือในกรณีที่ผู้ป่วยอยู่ในสภาวะพอมีสติในการตัดสินใจ ผู้ป่วยสามารถกดปุ่มเลือกอาการของผู้ป่วยในขณะนั้นได้ดังรูปที่ 4-5 โดยหลังจากผู้ใช้ทำการกดปุ่มอาการใดๆ บนสมาร์ทโฟนแล้ว จะมีการหน่วงเวลา 5 วินาที เพื่อให้โอกาสผู้ใช้ยกเลิกการแจ้งเหตุในกรณีที่เกิดการแจ้งเหตุโดยไม่ตั้งใจ แต่ในกรณีที่ต้องการยืนยันการแจ้งเหตุฉุกเฉิน ผู้ใช้สามารถกดปุ่ม "Send" เพื่อยกเลิกการหน่วงเวลา และทำการส่งข้อมูลในทันทีได้ จากนั้นระบบจะส่งข้อมูลของผู้ป่วยเช่น ประวัติส่วนตัว อาการ และพิกัดจีพีเอสไปยังเซิฟเวอร์เพื่อทำการประมวลผลต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2. ระบบช่วยตัดสินใจ

ในส่วนของระบบช่วยตัดสินใจนั้นแบ่งการทำงานออกเป็น 3 ส่วน คือ

1. ส่วนที่ทำการรับข้อมูล โดยจะรับข้อมูลจากการแจ้งเหตุของผู้ป่วย ข้อมูลเกี่ยวกับรถพยาบาล และข้อมูลของโรงพยาบาล
2. ส่วนประมวลผลข้อมูลและเปรียบเทียบข้อมูลเพื่อค้นหาเส้นทางที่เหมาะสม
3. ส่วนติดต่อกับเจ้าหน้าที่ในการแสดงผลข้อมูล



รูปที่ 6. หน้าจอปฏิบัติงานของเจ้าหน้าที่สำหรับรับการแจ้งเหตุฉุกเฉินต่างๆ

Path No.	Ambulance	Hospital	Path info	Estimate distance
1	ID:001(B)	LADKRABANG		3.9 KM
2	ID:001(B)	CHULARUT 7		4.1 KM
3	ID:002(A)	CHULARUT7		4.7 KM
4	ID:003(B)	LADKRABANG		5 KM

รูปที่ 7. ตารางเปรียบเทียบเส้นทางการนำส่งผู้ป่วย



รูปที่ 8. ข้อมูลเส้นทางที่ใช้ในการนำส่งผู้ป่วย

หลังจากระบบรับข้อมูลการแจ้งเหตุจากผู้ป่วยแล้ว ข้อมูลดังกล่าวจะถูกแสดงผลออกมาดังตัวอย่างในรูปที่ 6 ซึ่งจะแสดงหน้าจอระบบช่วยตัดสินใจของเจ้าหน้าที่ โดยจะแสดงผลตำแหน่งของจุดเกิดเหตุ รถพยาบาล และโรงพยาบาลที่อยู่ใกล้กับจุดเกิดเหตุลงบนแผนที่ จากนั้นจึงทำการประมวล และแสดงผลออกมาในรูปแบบตารางแนะนำเส้นทางดังรูปที่ 7 ซึ่งเรียงลำดับตามระยะทางจากรถพยาบาลไปยังจุดเกิดเหตุรวมกับระยะทางจากจุดเกิดเหตุไปยังโรงพยาบาลที่ใกล้ที่สุด และจะแสดงผลข้อมูลระดับของรถพยาบาลซึ่งมีอยู่ทั้งหมด 4 ระดับ[1] แบ่งตามความพร้อมของอุปกรณ์ช่วยเหลือที่มีอยู่บนรถพยาบาลนั้นๆ (ในรูปที่ 7 สมมุติว่ามีรถพยาบาลระดับ A และ B อยู่ในบริเวณที่มีการแจ้งเหตุ) โดยเจ้าหน้าที่จะทำการเลือกเส้นทางและรถพยาบาลที่เหมาะสมกับผู้ป่วย และส่งข้อมูลเส้นทางดังรูปที่ 8 ไปยังเจ้าหน้าที่ประจำรถพยาบาลผ่านทางเว็บไซต์ โดยจะนำเส้นทางที่ได้ไปแสดงผลบนอุปกรณ์ระบุพิกัดจีพีเอสที่ติดตั้งอยู่บนรถพยาบาล เพื่อให้เจ้าหน้าที่ประจำรถพยาบาลสามารถทำการช่วยเหลือผู้ป่วยได้อย่างรวดเร็ว

4. การประเมินและวิเคราะห์การทำงาน

เมื่อเปรียบเทียบกับระบบเก่าแล้ว[6] งานชิ้นนี้จะมีความแตกต่างจากระบบเก่าตามตารางต่อไปนี้

ตารางที่ 1. ตารางการเปรียบเทียบระบบ

รูปแบบการทำงาน	ระบบเดิม	ระบบใหม่
วิธีการแจ้งเหตุ	โทรศัพท์	แอพพลิเคชั่นบนสมาร์ทโฟน
ประวัติส่วนตัวของผู้ป่วย	ไม่ทราบ	ทราบ
การระบุตำแหน่ง	แจ้งผ่านโทรศัพท์	พิกัดจีพีเอส
การจัดการทรัพยากร	ไม่มี	มี
ระบบช่วยตัดสินใจ	ไม่มี	มี
การระบุอาการ	แจ้งผ่านโทรศัพท์	แอพพลิเคชั่นบนสมาร์ทโฟน
การป้องกันการแจ้งข้อมูลเท็จ	ไม่มี	ไม่มี

จากตารางที่ 1. ระบบที่นำเสนอจะสามารถแจ้งเหตุฉุกเฉินได้รวดเร็วกว่าเมื่อเปรียบเทียบการแจ้งเหตุผ่านโทรศัพท์ซึ่งต้องระบุทั้งที่อยู่ และอาการของผู้ป่วย ในขณะที่การใช้พิกัดจีพีเอสสามารถระบุตำแหน่งได้แม่นยำและใช้เวลาน้อยกว่าเพียงกดปุ่มบนสมาร์ทโฟนซึ่งใช้เวลาเพียงไม่กี่วินาที รวมทั้งสามารถระบุอาการของผู้ป่วยได้พร้อมกัน แต่อาจมีข้อเสียในเรื่องความละเอียดของอาการที่สามารถระบุได้ แต่ถ้าคำนึงถึงสภาวะของผู้ป่วยที่แตกต่างกันในกรณีที่ผู้ป่วยมีสติไม่มากพอที่จะสื่อสารได้ ระบบเก่าจะไม่สามารถทำงานได้เลย ในขณะที่ระบบใหม่ใช้ปริมาณการตัดสินใจน้อยกว่าการโทรศัพท์มาก ในส่วนปัญหาด้านความคลาดเคลื่อนของการระบุตำแหน่งจีพีเอส อาจส่งผลต่อความแม่นยำในการคำนวณเส้นทางในการนำส่งผู้ป่วยได้ แต่ปัญหานี้สามารถถูกแก้ไขได้ด้วยการอัพเดทพิกัดจีพีเอสใหม่ โดยระบบจะมีการอัพเดทพิกัดจีพีเอสของผู้ป่วยอยู่เป็นระยะ ดังนั้นปัญหานี้จึงได้รับการแก้ไขอย่างอัตโนมัติ ในด้านการจัดการทรัพยากร ระบบเก่าไม่มีการแสดงข้อมูลรถนำส่งทั้งหมดที่สามารถปฏิบัติการได้ในขณะนั้น จึงทำให้การตัดสินใจของเจ้าหน้าที่อาจผิดพลาดได้ ในส่วนของระบบช่วยตัดสินใจที่เพิ่มเข้ามาจะทำให้เจ้าหน้าที่สามารถทำงานได้ง่ายและรวดเร็วขึ้น แต่อย่างไรก็ตามระบบใหม่ก็ยังไม่สามารถป้องกันปัญหาการแจ้งข้อมูลเท็จได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. บทสรุป

โดยสรุปการใช้สมาร์ทโฟนเข้ามาช่วยในการแจ้งเหตุฉุกเฉินสามารถทำให้การแจ้งเหตุฉุกเฉินเป็นไปได้อย่างรวดเร็วและง่ายขึ้น โดยลดการสื่อสารระหว่างผู้ป่วยกับเจ้าหน้าที่เป็นการแจ้งเหตุผ่านแอพพลิเคชั่นและแจ้งตำแหน่งผ่านพิกัดจีพีเอส รวมทั้งระบบใหม่ยังมีระบบช่วยตัดสินใจเพื่อให้การช่วยเหลือมีโอกาสประสบความสำเร็จสูงขึ้นจากระยะเวลาที่ลดลง คุณภาพและปริมาณของข้อมูลที่ใช้ในการช่วยเหลือผู้ป่วยมีมากขึ้น แต่ระบบที่นำเสนอก็ยังไม่สามารถแก้ปัญหาการแจ้งข้อมูลเท็จได้ รวมทั้งมีข้อจำกัดด้านการใช้งานระบบ โดยสมาร์ทโฟนที่จะสามารถใช้งานแอพพลิเคชั่นนี้ได้ต้องสามารถเชื่อมต่ออินเตอร์เน็ตได้ในขณะที่ทำการแจ้งเหตุฉุกเฉินและต้องสนับสนุนการใช้งานระบบระบุพิกัดบนพื้นโลกได้

6. แนวทางการพัฒนาต่อยอด

6.1. แอพพลิเคชั่นบนสมาร์ทโฟน

ในส่วนของแอพพลิเคชั่นบนสมาร์ทโฟนมีส่วนที่พัฒนาต่อยอด ได้แก่ การเพิ่มเติมระบบการแจ้งเหตุอัตโนมัติโดยใช้ประโยชน์จากระบบเซนเซอร์บนสมาร์ทโฟน ซึ่งจะทำการตรวจสอบรูปแบบการเขย่าที่ผิดปกติที่สามารถสันนิษฐานได้ว่า ผู้ใช้เกิดการล้มหรือเกิดอุบัติเหตุหรือไม่ อีกทั้งการส่งข้อมูลรูปถ่ายที่เกิดเหตุหรือบริเวณจุดเกิดเหตุเพื่อเพิ่มข้อมูลในการตัดสินใจให้แก่เจ้าหน้าที่ได้ และเพิ่มฟังก์ชั่นการแจ้งเหตุผ่านทางโทรศัพท์ไปยังเจ้าหน้าที่เพื่อแจ้งข้อมูลเพิ่มเติมทันทีหลักจากมีการแจ้งเหตุฉุกเฉินผ่านทางแอพพลิเคชั่นบนสมาร์ทโฟน

6.2. ระบบช่วยตัดสินใจ

ในส่วนของระบบช่วยตัดสินใจสามารถพัฒนาในส่วนของความแม่นยำในการระบุตำแหน่งของผู้ป่วย เช่น การใช้ Altitude ในการคำนวณความสูงของจุดเกิดเหตุในกรณีที่ผู้ป่วยประสบอุบัติเหตุในอาคารที่มีความสูงหลายชั้น และเพิ่มความฉลาดของระบบช่วยตัดสินใจให้สามารถระบุจุดเกิดเหตุที่ละเอียดยิ่งขึ้นจากการคาดเดาพฤติกรรม และสถานที่ที่ผู้ใช้นำสมาร์ทโฟนไปบ่อยครั้ง ซึ่งมีโอกาสจะเกิดเหตุได้ เช่น บ้าน ที่ทำงาน หรือสถานที่ที่ไปเป็นกิจวัตรประจำวัน

เอกสารอ้างอิง

[1] สถาบันการแพทย์ฉุกเฉินแห่งชาติ. "รายงานประจำปี 2554 สถาบันการแพทย์ฉุกเฉินแห่งชาติ". พิมพ์ครั้งที่ 1, มีนาคม, 2555.

[2] คำรณ ไชยศิริ, วิทยา ชาติบัญชาชัย. "การประเมินผลโครงการพัฒนาระบบบริการการแพทย์ฉุกเฉินโดยความร่วมมือระหว่างภาครัฐ ภาคเอกชนและองค์กรปกครองส่วนท้องถิ่นจังหวัดขอนแก่น". วารสารวิชาการสาธารณสุข, ปีที่ 17, ฉบับเพิ่มเติม 4 (มีนาคม-เมษายน), 2551.

[3] Sheng-Cheng Yeh, Wu-Hsiao Hsu, Ming-Yang Su, Ching-Hui Chen and Ko-Hung Liu. "A Study on Outdoor Positioning Technology Using GPS and WiFi Networks". Proceedings of the 2009 IEEE International Conference on Networking, Sensing and Control, Okayama, Japan, March 26-29, 2009.

[4] Ankur Chandra, Shashank Jain, Mohammed Abdul Qadeer. "GPS Locator: An Application for Location Tracking and Sharing using GPS for Java Enabled Handhelds". 2011 IEEE International Conference on Computational Intelligence and Communication Systems, 2011.

[5] Ghaith Bader Al-Suwaidi, Mohamed Jamal Zemerly. "Locating Friend and Family Using Mobile Phones with Global Positioning System (GPS)". 2009 IEEE, 2009.

[6] สถาบันการแพทย์ฉุกเฉินแห่งชาติ. "ระบบสารสนเทศการแพทย์ฉุกเฉิน". http://ws.emit.go.th/items_front/CallCenter.aspx.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การประยุกต์ใช้สมาร์ทโฟนเพื่อการพิสูจน์ตัวตนด้วยข้อมูลพิกัดจีพีเอส

สุเมธ ประภาวัต นิติ ชัยกะเสวี ภรภัทร นนทะบรรหาญ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: sumet@it.kmitl.ac.th, numnoiiniti@hotmail.com, alllives@live.com

บทคัดย่อ

การทำธุรกรรมผ่านบัตรเครดิตนั้นจะทำอย่างไรให้มีความปลอดภัยและยืนยันได้ว่าผู้ที่ทำธุรกรรมเป็นเจ้าของบัตรตัวจริง ซึ่งการซื้อสินค้าผ่านบัตรเครดิตนั้นมีความสะดวกสบายอย่างมาก แต่ก็แฝงไปด้วยภัยต่างๆ ที่ตามมา และปัจจุบันความสามารถของโทรศัพท์สมาร์ทโฟนที่เหนือกว่าโทรศัพท์มือถือพื้นฐานทั่วไป ทำให้โทรศัพท์สมาร์ทโฟนกลายเป็นอุปกรณ์สื่อสารที่มีผู้คนนิยมใช้อย่างมาก ภายในโทรศัพท์สมาร์ทโฟนจะมีเครื่องรับสัญญาณดาวเทียมหรือจีพีเอส ซึ่งสามารถนำมาประยุกต์ใช้ประโยชน์ได้มากมาย หนึ่งในนั้นคือการระบุตำแหน่งเพื่อยืนยันตัวตนของผู้ใช้โดยจีพีเอส โดยจะใช้ประกอบกับการทำธุรกรรมทางการเงินผ่านบัตรเครดิต ทำให้ผู้ใช้มีความปลอดภัยจากผู้ไม่ประสงค์ดีที่จะทำการบิดเบือนข้อมูลที่มีความสำคัญไปหรือโจรกรรมบัตรเครดิตเพื่อนำไปใช้โดยผิดกฎหมาย

คำสำคัญ-- โทรศัพท์สมาร์ทโฟน; จีพีเอส; ธุรกรรมบัตรเครดิต

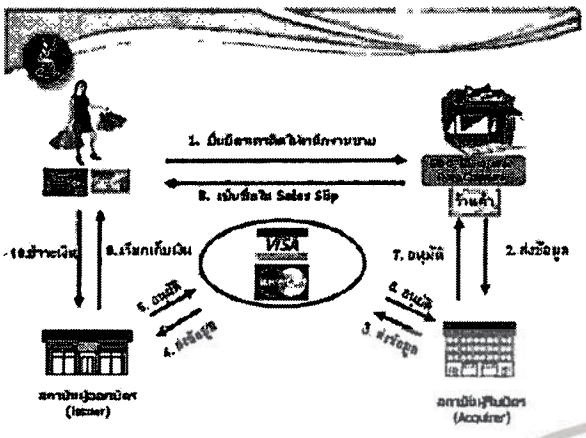
1. บทนำ

บัตรเครดิตได้เข้ามามีบทบาทในการทำธุรกรรมทางการเงินของผู้บริโภคมากขึ้น เพราะมีความสะดวกสบายในการซื้อสินค้าต่างๆ โดยไม่จำเป็นต้องพกเงินสดจำนวนมาก ทั้งนี้ยังได้รับสิทธิในรายการส่งเสริมการขายมากกว่าการซื้อด้วยเงินสด ซึ่งในปัจจุบันมีบัตรเครดิตและบัตรเดบิตรวมกันทั้งสิ้นกว่า 72 ล้านใบ [1] และมีเครื่องรูดบัตรมากกว่าสองแสนเครื่อง [2] นอกจากนั้นบัตรเครดิตยังสามารถซื้อสินค้าออนไลน์ซึ่งมีให้เลือกมากมายและสะดวกกว่าเดินไปซื้อตามร้านค้า ทำให้การทำธุรกรรมทางการเงินในปัจจุบัน บัตรเครดิตจะเป็นสื่อกลางหลักที่ผู้บริโภคนิยมใช้และได้รับการตอบรับอย่างดีจากร้านค้า ในส่วนของโทรศัพท์มือถือได้กลายมาเป็นปัจจัยสำคัญในการดำเนินชีวิตมนุษย์ในปัจจุบัน ต่อมาเมื่อโทรศัพท์มือถือได้รับการพัฒนาอย่างก้าวกระโดดจนกลายเป็นโทรศัพท์สมาร์ทโฟนที่มีความสามารถหลากหลาย เช่นการเชื่อมต่ออินเตอร์เน็ต ดาวน์โหลดแอพพลิเคชัน หรือการใช้งาน GPS ซึ่งสามารถรับพิกัดตำแหน่งของผู้ใช้ได้ว่าอยู่ส่วนใดบนแผนที่โลก จากการที่เทคโนโลยีของการซื้อขายแลกเปลี่ยนสินค้าและเทคโนโลยีของโทรศัพท์สมาร์ทโฟนมีการพัฒนาไปอย่างต่อเนื่อง แต่ความปลอดภัยในการซื้อขายนั้นยังไม่มีการเพิ่มประสิทธิภาพมากนัก โครงการนี้จึงจะทำการเพิ่มความปลอดภัยในการซื้อสินค้าผ่านบัตรเครดิต โดยมีการนำ GPS ของสมาร์ทโฟนมาประยุกต์ใช้ในการยืนยันและระบุตัวตนว่าบุคคลผู้เป็นเจ้าของบัตรเครดิตนั้นอยู่ในสถานที่นั้นจริงขณะทำธุรกรรม

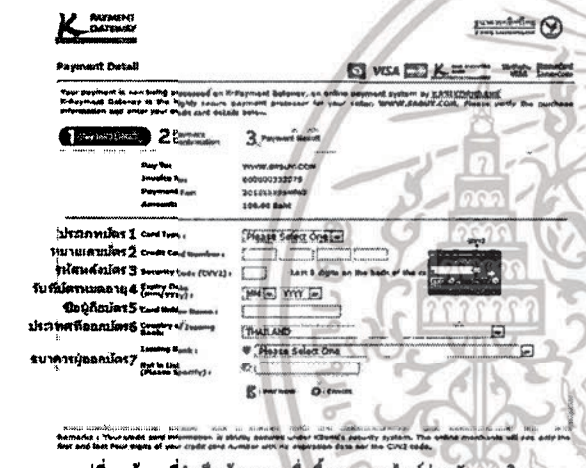
2. ทฤษฎีและงานที่เกี่ยวข้อง

กระบวนการซื้อสินค้าผ่านบัตรเครดิต[3][4] ผู้ซื้อต้องทำการยื่นบัตรเครดิตให้กับพนักงานขาย จากนั้นพนักงานขายจะนำบัตรเครดิตไปรูดที่เครื่องรูดบัตร (Electronic Data Capture: EDC) ซึ่งอาจเป็นของธนาคาร หรือ Non-bank แห่งอื่น ๆ ซึ่งเรียกว่า สถาบันผู้รับบัตร หรือ Acquirer จากนั้น เครื่อง EDC จะส่งข้อมูลกลับไปยังสถาบันผู้รับบัตร สถาบันผู้รับบัตรจะส่งข้อมูลต่อไปยังศูนย์เครือข่ายบัตรเครดิต (เช่น VISA หรือ MASTER CARD เป็นต้น) จากนั้นศูนย์เครือข่ายบัตรเครดิตจะส่งข้อมูลไปยังธนาคาร หรือ Non-bank ที่เป็นผู้ออกบัตรเครดิตนั้น ซึ่งเรียกว่า สถาบันผู้ออกบัตร หรือ Issuer เพื่อขออนุมัติการใช้บัตรเครดิต สถาบันผู้ออกบัตรจะตรวจสอบวงเงินว่ามีเพียงพอหรือไม่ และแจ้งการอนุมัติกลับไปยังศูนย์เครือข่ายบัตรเครดิต ศูนย์เครือข่ายบัตรเครดิตจะแจ้งการอนุมัติกลับไปยังสถาบันผู้รับบัตร สถาบันผู้รับบัตรจะแจ้งการอนุมัติกลับไปยังร้านค้าเพื่อพิมพ์ใบบันทึกการขาย (Sales Slip) จากนั้นผู้ซื้อต้องทำการตรวจสอบความถูกต้องของใบบันทึกรายการขาย (Sales Slip) ก่อนที่จะเซ็นชื่อ ซึ่งการเซ็นชื่อเป็นการยืนยันตัวตนเพียงอย่างเดียวเท่านั้น ซึ่งมีความเสี่ยงที่จะมีการปลอมแปลงลายเซ็นได้ เพราะบัตรเครดิตจะไม่ปรากฏภาพของเจ้าของบัตร เมื่อเซ็นเสร็จเรียบร้อยแล้วให้เก็บ Sales Slip ไว้เป็นหลักฐานการชำระเงินเพื่อตรวจสอบกับใบแจ้งหนี้การชำระเงิน สถาบันผู้ออกบัตรจะจัดส่งใบแจ้งหนี้ให้ผู้ซื้อก่อนครบกำหนดชำระเงิน โดยผู้ซื้อควรชำระค่าใช้จ่ายตามยอดหนี้ที่ระบุในใบแจ้งหนี้ให้แก่สถาบันผู้ออกบัตรภายในเวลาที่กำหนด ไม่เช่นนั้น ต้องเสียค่าดอกเบี้ยและค่าบริการต่าง ๆ โดยกระบวนการทำงานทั้งหมดสามารถสรุปเป็นแผนภาพได้ดังรูปที่ 1.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 1. ขั้นตอนการทำงานของบัตรเครดิต



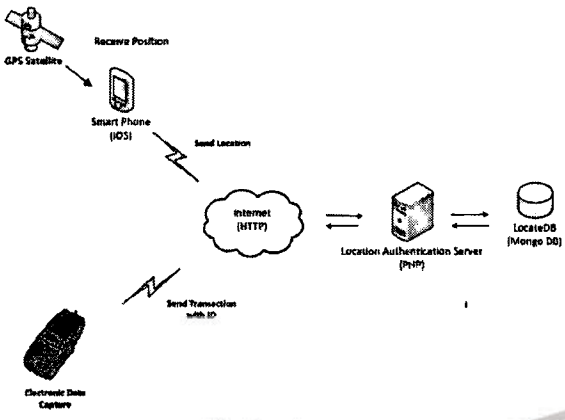
รูปที่ 2. ข้อมูลที่จำเป็นต้องกรอกเมื่อซื้อของออนไลน์ผ่านบัตรเครดิต

จากรูปที่ 2. จะเป็นรายละเอียดที่ต้องกรอกข้อมูลเมื่อมีการซื้อสินค้าออนไลน์ผ่านบัตรเครดิต[5] เว็บไซต์ส่วนมากจะใช้หมายเลขบัตรเครดิต 16 หลัก รหัสหลังบัตร (Security Code) 3 หลัก วันที่บัตรหมดอายุและชื่อผู้ถือบัตรประกอบกันเพื่อยืนยันตัวตนของผู้ซื้อ ซึ่งข้อมูลทั้งหมดที่กล่าวไว้ข้างต้นจะปรากฏอยู่บนบัตรเครดิตทั้งหมด ผู้ใดที่มีข้อมูลดังกล่าวสามารถซื้อสินค้าออนไลน์ได้

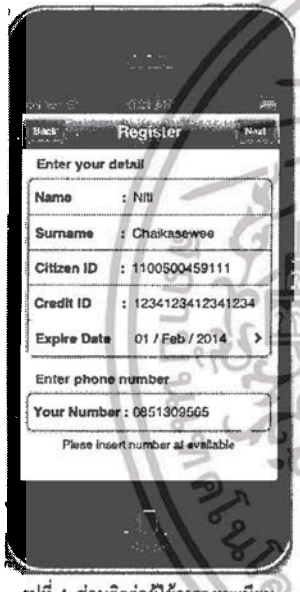
3. แนวคิดการดำเนินงาน

การทำงานโดยรวมนั้นสามารถสรุปเป็นใจความสาคัญได้คือ "ไม่มีสมาร์ทโฟน ไม่มีการซื้อขาย" โดยจะใช้โทรศัพท์สมาร์ทโฟนเป็นเครื่องมือหลักในการระบุตำแหน่งของผู้ใช้ ซึ่งจะไปซื้อสินค้า ณ ร้านค้าต่างๆ ที่มีเครื่องรูดบัตรเครดิต โดยในขั้นแรกผู้ใช้ต้องลงทะเบียนบัตรเครดิต โดยใช้ข้อมูลพื้นฐานที่ปรากฏบนบัตรเครดิต เพื่อให้บัตรเครดิตกับสมาร์ทโฟนมีความสัมพันธ์กันและเมื่อต้องการซื้อสินค้ากับบัตรเครดิตที่ทำการลงทะเบียนไว้แล้ว ให้ทำการเปิดแอพพลิเคชันในโทรศัพท์สมาร์ทโฟนขึ้นมา และกดปุ่ม "Send Location" เพื่อส่งตำแหน่งปัจจุบันของผู้ใช้ (สามารถใช้ได้ 30 นาที โดยไม่ต้องกดทุกครั้งที่มีการซื้อ) และเมื่อมีข้อมูลตำแหน่งปัจจุบันของผู้ซื้อจึงสามารถซื้อสินค้าตามปรกติ แต่หากไม่สะดวกที่จะต้องเข้ามาอัพเดทข้อมูลทุกๆ 30 นาที ผู้ใช้สามารถตั้งค่าให้แอพพลิเคชันส่งข้อมูลพิกัดโดยอัตโนมัติแทนได้ แต่การส่งข้อมูลอัตโนมัติจะสูญเสียพลังงานมากเมื่อเปรียบเทียบกับการกดอัพเดทข้อมูลทีละครั้งเมื่อต้องการซื้อสินค้า เมื่อมีการรูดบัตรเครื่องรูดบัตรจะทำการส่งพิกัดและข้อมูลเกี่ยวกับการซื้อไปยังเครื่องเซิร์ฟเวอร์ แต่เนื่องจากเครื่องรูดบัตรเครดิตไม่สามารถที่จะส่งข้อมูลพิกัดบนแผนที่ไปยังเครื่องเซิร์ฟเวอร์ได้โดยตรง เพราะไม่มีจีพีเอสติดตั้งอยู่ภายในเครื่อง ซึ่งระบบจะใช้วิธีการเก็บข้อมูลพิกัดเครื่องรูดบัตรตั้งแต่ที่ร้านค้าขอเครื่องรูดบัตรไปติดตั้งที่ร้าน โดยนำตำแหน่งร้านไปค้นหาพิกัดและเก็บข้อมูลพิกัดไว้ในฐานข้อมูล เมื่อข้อมูลจากเครื่องรูดบัตรส่งมาถึงเครื่องเซิร์ฟเวอร์ เครื่องเซิร์ฟเวอร์จะเปรียบเทียบกับพิกัดของผู้ใช้ที่ส่งมาก่อนว่าอยู่ในระยะใกล้เคียงหรือไม่ สำหรับการซื้อขายออนไลน์นั้นมีลักษณะเดียวกัน คือเมื่อต้องการซื้อสินค้าให้ทำการส่งข้อมูลพิกัดปัจจุบันไปก่อน และเมื่อกรอกข้อมูลที่หน้าเว็บไซต์ที่ทำการซื้อสินค้า จะต้องกรอกชื่อเมือง อำเภอ(เขต) และตำบล(แขวง) โดยใช้ AJAX เข้ามาช่วยในการหาชื่อเมืองให้ไวขึ้น หากพิมพ์ "S" ภายในช่องที่ให้กรอก จะขึ้นคำว่า "Samutprakarn" "Samutsakorn" "Samutsongkram" เพื่อให้ผู้ใช้ไม่พิมพ์ชื่อต่างๆ ผิด การตรวจสอบพิกัดในการซื้อสินค้าผ่านเครื่องรูดบัตรและซื้อสินค้าออนไลน์จะมีความเหมือนกันคือหากพิกัดของผู้ซื้อไม่ได้อยู่ในบริเวณที่ผู้ใช้ซื้อสินค้า เซิร์ฟเวอร์จะส่งการแจ้งเตือนไปยังโทรศัพท์สมาร์ทโฟนเพื่อให้ยืนยันคำสั่งซื้อหรือสามารถกดยกเลิกเพื่อไม่ให้เกิดการซื้อขายขึ้น การอิมพลิเมนท์ระบบจำเป็นต้องเพิ่มเครื่องเซิร์ฟเวอร์และระบบฐานข้อมูลลงไปเพื่อเก็บข้อมูลที่จำเป็น โดยเซิร์ฟเวอร์ที่เพิ่มเข้ามาจะเชื่อมต่อกับสถาบันผู้รับบัตร (Acquirer) โดยเป็นจุดแรกที่เครื่องรูดบัตรส่งข้อมูลมาถึง ทำให้ลดการส่งข้อมูลตั้งแต่ต้นทาง กระบวนการทำงานของระบบที่สร้างขึ้นมาใหม่แสดงดังรูปที่ 3. โครงสร้างของระบบ ในส่วนของระบบปฏิบัติที่ใช้ในโทรศัพท์สมาร์ทโฟนคือ iOS[6] โดยมีเครื่องเซิร์ฟเวอร์ที่ใช้ภาษา PHP และฐานข้อมูลจะใช้ NOSQL ในการอิมพลีเมนท์ ซึ่งสาเหตุที่ใช้ NOSQL นั้นเพราะว่ามีความรวดเร็วในการทำงานและสามารถขยายฐานข้อมูลต่อไปในอนาคตได้โดยมีข้อจำกัดไม่มากเมื่อเทียบการฐานข้อมูลแบบมี Relation ที่จำเป็นต้องมีแบบ ER Model และทำการ Normalize เพื่อให้ตารางมีความซ้ำซ้อนน้อยที่สุด และในส่วนของส่วนติดต่อผู้ใช้ในโทรศัพท์สมาร์ทโฟนจะออกแบบให้เรียบง่าย และสื่อความหมายชัด จากรูปที่ 4. คือการลงทะเบียนโทรศัพท์สมาร์ทโฟนให้เชื่อมโยงกับบัตรเครดิต และหลังจากลงทะเบียนเมื่อเปิดแอพพลิเคชันจะปรากฏปุ่ม "Send Location" ดังปรากฏในรูปที่ 5. ในส่วนของมีการแจ้งเตือนแบบพุชโนทิฟิเคชันจะแจ้งเตือนเมื่อตำแหน่งของโทรศัพท์สมาร์ทโฟนและบริเวณที่ทำการซื้อขายไม่ใกล้เคียงกัน ดังปรากฏในรูปที่ 6. ในส่วนของเซิร์ฟเวอร์จะสามารถ เพิ่ม ลบ และแสดงข้อมูลของผู้ใช้แต่ละคนได้ โดยการเข้าสู่ระบบจำเป็นต้องมีการ Log in ก่อน เพื่อความปลอดภัยของข้อมูลผู้ใช้ ซึ่งเป็นข้อมูลที่มีความสำคัญมาก

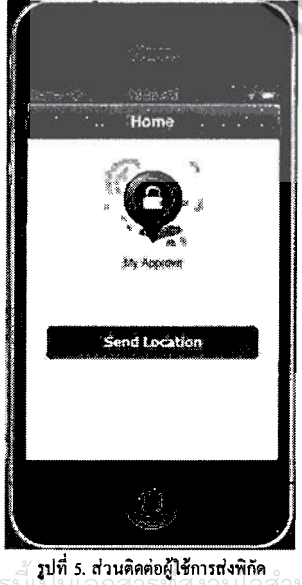
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



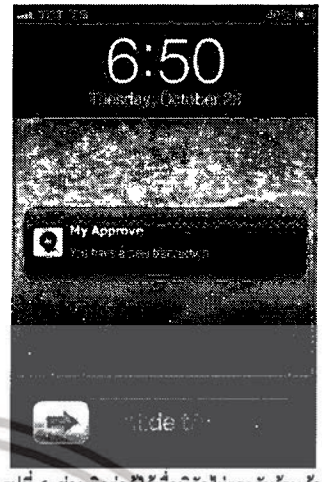
รูปที่ 3. โครงสร้างของระบบ



รูปที่ 4. ส่วนติดต่อผู้ใช้การลงทะเบียน



รูปที่ 5. ส่วนติดต่อผู้ใช้การส่งพิกัด



รูปที่ 6. ส่วนติดต่อผู้ใช้เมื่อพิกัดไม่ตรงกับร้านค้า



รูปที่ 7. ส่วนติดต่อผู้ใช้ของเซิร์ฟเวอร์

4. วิเคราะห์การทำงานและประเมินผล

การทำงานจะเริ่มขึ้นเมื่อผู้ใช้กดส่งข้อมูลพิกัดไปยังเครื่องเซิร์ฟเวอร์โดยข้อมูลพิกัดนี้มีระยะการใช้งานได้เพียง 30 นาทีเท่านั้น โดยภายในระยะเวลา 30 นาที ลูกค้าจะสามารถซื้อสินค้าร้านใดก็ได้ภายในบริเวณที่กดส่งข้อมูลพิกัดไป แต่หากหมดเวลา 30 นาทีจะมีการแจ้งเตือนว่าหมดเวลาและให้ส่งเข้าไปใหม่หากต้องการซื้อสินค้าเพิ่มเติม หากไม่ส่งข้อมูลพิกัดใหม่จะไม่สามารถซื้อสินค้าใดๆ ได้อีก หรือผู้ใช้อาจจะเลือกการส่งพิกัดอัตโนมัติ สามารถซื้อสินค้าได้ตลอดเวลาโดยไม่ต้องกดส่งใหม่ทุกครั้ง แต่อาจส่งผลกระทบต่อระดับพลังงานภายในโทรศัพท์สมาร์ทโฟนได้ ในส่วนของเครื่องเซิร์ฟเวอร์ซึ่งต้องคอยรับข้อมูลจากโทรศัพท์สมาร์ทโฟนและจากเครื่องรูดบัตรเพื่อนำมาประมวลผลข้อมูล โดยข้อมูลที่เข้ามาจะมีจำนวนมากเพราะการซื้อขายจะเกิดขึ้นตลอดเวลา จำนวนข้อมูลที่เข้าไปในเซิร์ฟเวอร์จะมีจำนวนมาก ซึ่งจำเป็นต้องใช้เซิร์ฟเวอร์จำนวนมาก เพื่อช่วยในการประมวลผลและจัดเก็บเซสชันที่เข้ามา ดังนั้นหากนำแอพพลิเคชันนี้ไปใช้ร่วมกับการซื้อขายจริงผ่านบัตรเครดิตจะลดปัญหาต่างๆ มากมายอาทิ เช่น การโจรกรรมบัตรเครดิตเพื่อนำบัตรเครดิตนั้นไปซื้อสินค้าต่างๆ โดยที่เจ้าของบัตรไม่รู้ เพราะผู้โจรกรรมจะไม่สามารถซื้อสินค้าได้เลย หากไม่มีโทรศัพท์สมาร์ทโฟน เสมือนนำบัตรเครดิตที่หมดอายุแล้วไปใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. บทสรุป

แอพพลิชันนี้สามารถเพิ่มความปลอดภัยให้กับการใช้บัตรเครดิตให้ไม่สามารถที่จะรูดซื้อสินค้าโดยที่เจ้าของบัตรนั้นไม่ยินยอม โดยการใช้ข้อมูลจีพีเอสผ่านโทรศัพท์สมาร์ทโฟนมายืนยันตัวตนร่วมกับการใช้บัตรเครดิตในการทำธุรกรรมทางการเงิน ในส่วนของแอพพลิเคชันจะมีลักษณะเรียบง่าย เพียงกดส่งข้อมูลเท่านั้น โดยอาจจะส่งผลต่อเวลาในการทำธุรกรรมทางการเงินที่อาจจะเพิ่มขึ้นเล็กน้อย แต่สามารถเพิ่มความปลอดภัยให้กับบัตรเครดิตอย่างมาก หรือผู้ใช้อาจจะเลือกการส่งพิกัดอัตโนมัติ โดยสามารถสรุปได้ในตาราง 1. และตาราง 2.

ตาราง 1. เปรียบเทียบการซื้อด้วยบัตรเครดิตผ่านเครื่องรูดบัตรกับการใช้แอพพลิเคชันใหม่

	ระบบเดิม	แอพพลิเคชันใหม่
การยืนยันตัวตนเจ้าของบัตรเครดิต	ตรวจดูลายเซ็นต์ที่ใบเสร็จเปรียบเทียบกับหลังบัตรเครดิต	ใช้พิกัดข้อมูลจีพีเอสเปรียบเทียบกับตำแหน่งของร้าน
ช่องโหว่	ทุกคนสามารถใช้บัตรเครดิตได้ เพียงแต่เซ็นต์ชื่อให้มีความคล้ายกับเจ้าของบัตร	หากโทรศัพท์สมาร์ทโฟนหายหรือแบตเตอรีหมดจะไม่สามารถซื้อสินค้าได้
ภัย (Threat)	อาจมีผู้ไม่ประสงค์ดีนำบัตรเครดิตไปใช้โดยเจ้าของบัตรเครดิตไม่อนุญาต	-
จุดเด่น	รวดเร็ว	ปลอดภัย

ตาราง 2. เปรียบเทียบการซื้อด้วยบัตรเครดิตแบบออนไลน์กับการใช้แอพพลิเคชันใหม่

	ระบบเดิม	แอพพลิเคชันใหม่
การยืนยันตัวตนของเจ้าของบัตรเครดิต	รหัสบัตรเครดิต ข้อมูลหน้าบัตร และ Security Code 3 หลัก	ใช้พิกัดข้อมูลจีพีเอสเปรียบเทียบกับชื่อเมือง อำเภอและตำบลที่กำลังทำธุรกรรมปัจจุบัน
ช่องโหว่	ทุกคนสามารถซื้อสินค้าผ่านบัตรเครดิตได้ เพียงมีบัตรเครดิตและกรอกข้อมูลลงไป	หากโทรศัพท์สมาร์ทโฟนหายหรือแบตเตอรีหมดจะไม่สามารถซื้อสินค้าได้
ภัย (Threat)	อาจมีผู้ไม่ประสงค์ดีนำบัตรเครดิตไปใช้โดยเจ้าของบัตรเครดิตไม่อนุญาต	-
จุดเด่น	-	ปลอดภัย

เอกสารอ้างอิง

[1] ธนาคารแห่งประเทศไทย. "จำนวนบัตรพลาสติก". HTTP://WWW2.BOT.OR.TH/STATISTICS/DOWNLOAD/PS_PT_006_TH_ALL.XLS.

[2] ธนาคารแห่งประเทศไทย. "จำนวนเครื่องรับบัตร (EFTPOS TERMINAL)".HTTP://WWW2.BOT.OR.TH/STATISTICS/DOWNLOAD/PS_PT_007_TH_ALL.XLS

[3] ธนาคารแห่งประเทศไทย. "ขั้นตอนการใช้บัตรเครดิต". http://www.bot.or.th/Thai/FinancialLiteracy/creditcard/Pages/creditcard_4.aspx

[4] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอกนิกส์(องค์การมหาชน). "Focus Group Seminar เรื่อง Payment Card Standard". http://standard.etda.or.th/wp/?p=1

[5] บริษัท สนุก ช้อปปิ้ง จำกัด. "ชำระเงินผ่านบัตรเครดิตออนไลน์ (Credit Card)". http://sabuy.sanook.com/sites/help/seller/detail/30098

[6] Vandad Nahavandipoor. **"iOS 5 Programming Cookbook,"**. 1 st ed. New York : O'REILLY, 2011.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารแนบ

ผลงานที่ได้รับการเผยแพร่

โครงการจัดตั้งห้องปฏิบัติการวิจัยและพัฒนา Mobile Computing and Sensor Networks

โดย ดร.สุเมธ ประภาวัต

ด้วยเงินรายได้คณะเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2556 (งบยุทธศาสตร์ 5%)



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Load Distribution using Modified RED for Multipath TCP Communication

Sumet Prabhavat[1] Ruttikorn Varakulsiripunth[2] Satoshi Utsumi[3] Yasushi Kato[4]

[1]Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
[2]Faculty of Information Technology, Thai-Nichi Institute of Technology, Bangkok, Thailand
[3,4]Tsuruoka National College of Technology, Yamagata, Japan
[1]sumet@it.kmitl.ac.th, [2]kvruttik@gmail.com, [3]u.satoshi0215@gmail.com, [4]president@tsuruoka-nct.ac.jp

***Abstract*— Demand for large bandwidth network connections is growing continuously while network connections via multiple paths can exist because of high degree of connectivity. Utilization of the multiple paths is an economical solution for provisioning large network capacity to meet the users' requirements but it brings about key issues such as load imbalance (causing a large queue and buffer overflow at a gateway) and packet reordering problems that have significant impacts on TCP connections. In this paper, we propose a load distribution model for TCP transmission, called Load Distribution over Multipath with Extended Drop Slope Random Early Detection (LDM/ExRED). LDM/ExRED takes advantages of RED mechanism to maintain a small queue, avoid buffer overflow at a gateway, and mitigate packet reordering problem. In addition, it reduces peak buffer occupancy by using our modified RED (i.e., ExRED). Our work will be evaluated and compared to the other existing models by simulations under realistic traffic conditions.**

Keywords—Load Distribution; Load Balancing; Multipath TCP

I. INTRODUCTION

A wide variety of network service requirements demanded by users has been an important driving force for development of networking technologies [1]. By using today's technologies, multipath configurations can be established in various ways [2]. Their primary objectives are to improve network reliability by increasing network availability and reducing network downtime. A main path was used for data transmission while the others were backups which would be activated when the main path became unavailable. Currently, applications of multiple paths aims not only at avoiding a single point of failure but also at facilitating network provision [1–4] where its effectiveness is essential to quality of network services and Quality of Service (QoS) guarantee. Using multiple paths as a single path with aggregate bandwidth is a practical solution which is preferable rather than provisioning a large-bandwidth path because it offers a possibility to establish a very large-bandwidth connection. This improves scalability to support the future growth in bandwidth demand and affordability for network users. It also provides flexibility in bandwidth management within the communication protocol over the multipath network. Bandwidth aggregation and network-load balancing are important issues having been attractive research topics, and a large amount of load distribution approaches have been proposed. The rest of this paper is organized as follows. Section II briefly describes existing load distribution models, some studies on packet reordering problems, and an active queue management for TCP networks. Section III presents a new load distribution model with our modified active queue management mechanism. Section IV discusses performance evaluation under real traffic conditions. Conclusions are then given in Section V.

II. RELATED WORKS

A. Load Distribution Models

Load distribution can be classified into packet-based model and flow-based models. Packet-based models can be further classified into non-adaptive and adaptive models. Surplus Round Robin (SRR) [5] is a simple non-adaptive load distribution model. SRR is an enhanced version of round robin family model which is widely used schemes in the Internet because it can achieve starvation-free and acceptable load balancing efficiency. Least-loaded first (LLF) [6–8] is an adaptive load distribution model. LLF is a well-known load-sharing approach introduced to manage task loads with heavy-tailed distribution, where a task is assigned to the least-loaded server. In multipath load balancing with this scheme, a path having the smallest load or the shortest queue will be selected for an arrived packet. The most important drawback is that they do not consider task sequence, which can result in the packet reordering problem [9].

On the other hand, Direct Hashing (DH) [10], Table-based Hashing (TH) [11], and Fast Switching (FS) [12] are flow-based models which can prevent packet reordering but they can cause load imbalance problem due to inability to cope with variance of the flow size distribution. This problem can cause a large buffer occupancy leading to a high risk of buffer overflow [2]. Adaptive load distribution models, e.g., Load Distribution over Multipath (LDM) and Load Balancing for Parallel Forwarding (LBPF) [13–15] were introduced to mitigate the load imbalance problem. However, there is trade-off between balancing load and maintaining a low risk of packet reordering. This depends on the respective algorithms as well as their set parameters.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

978-1-4799-0425-9/13/$31.00 ©2013 IEEE

B. Packet Reordering Problem

Several works have studied on packet reordering problem [16–22]. Packet reordering can occur with high probabilities of splitting a flow and switching a path [18], [19]. On the other hand, the possibility of packet reordering will decrease if the interarrival time of two consecutive packets belonging to the same flow is longer than the longest time required to deliver a packet via the parallel paths [23]. The packet interarrival time must be greater than the difference between the longest and the shortest delays among parallel paths to ensure packet order preservation. If the load is not properly distributed among the parallel paths, some paths may experience congestion (leading to large queues) while the others are idle; consequently, the delay difference can be very large.

C. Active Queue Management for TCP Gateway

Random Early Detection (RED) [24] is a well-known active queue management mechanism introduced to improve performance of TCP communication. RED itself consists of two main parts, i.e., the estimation of an average queue size and the decision of whether or not to drop an incoming packet. An average queue size is calculated by a current queue size using an exponentially weighted moving average (EWMA). Based on the average queue size, RED decides whether or not to drop an incoming packet. Packet arrival rate of a flow plays an important role in determining packet drop probability. The higher the packet arrival rate, the higher the packet drop rate. This feature of RED is to prevent two major problems that have a significant impact on TCP connections: buffer overflow and synchronization of TCP flows [25] due to burst traffic. In LDM/RED [26], we uses RED for sensing congestion and marking a packet arriving at the time congestion occurs. The marked packet will be switched to a less congested path.

III. Load Distribution (over Multipath Networks) with Extended Drop Slope Random Early Detection

Figure 1 describes our approach called Load Distribution over Multipath with Extended Drop Slope Random Early Detection (LDM/ExRED), which is developed from LDM/RED [26] and our modified RED algorithm (i.e., ExRED) [27]. Assume that multiple and parallel connections are established between a source and a destination before data transmission is started. For each path p, bandwidth is μ_p. The other parameters, e.g., hop counts and path delay, are assumed reflected by a measured queue length q_p. The input traffic is split into flows, each of which independently takes a path determined by a path selection component. LDM/ExRED is a variant version of FS [12] and LDM [13], a table-based model which selects paths based on the flow-path mapping table. A packet belonging to an existing flow is sent via the same path as its previous ones. When a new flow appears, a packet belonging to the new flow will be sent via a new path having the shortest queue.

In LDM/ExRED, a mapping table is modified and the path for an existing flow will be changed. The existing flow is switched (to a new path having the shortest queue) with probability π_s which is determined by ExRED mechanism, as illustrated in Fig. 2. Based on an average queue length $\hat{q}_p$,

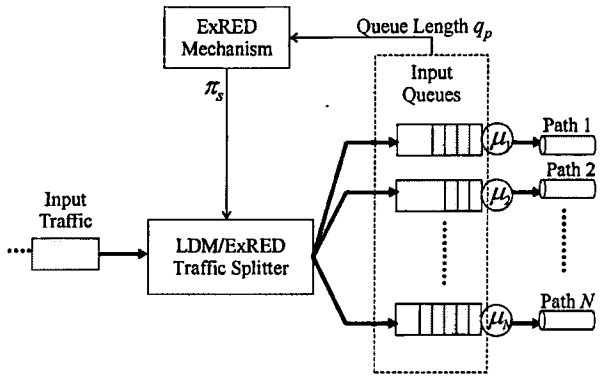


Figure 1. Description of the proposed model, LDM/ExRED

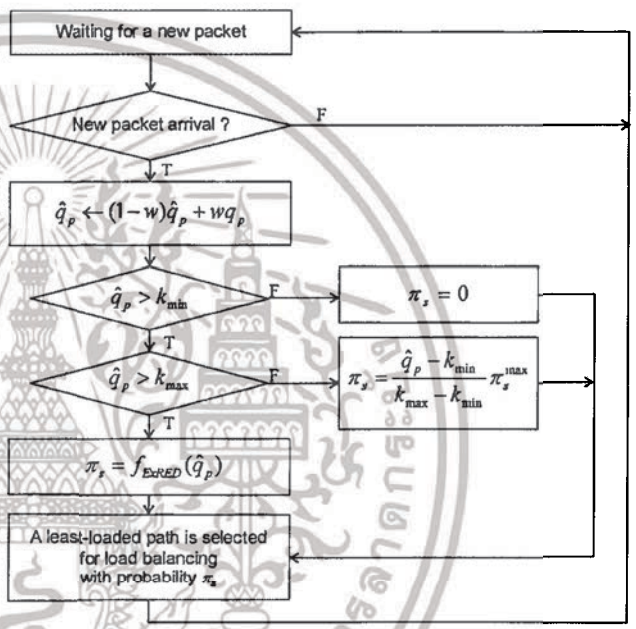


Figure 2. Flowchart to calculate π_s in traffic splitting algorithm

LDM/ExRED makes a decision of whether or not to split the flow. There are two queue thresholds: minimum and maximum thresholds, i.e., k_{min} and k_{max}. When $\hat{q}_p > k_{min}$, the flow is split with probability $\pi_s > 0$. The larger the average queue size $\hat{q}_p$, the higher the probability π_s. When $\hat{q}_p > k_{max}$, π_s increases according to polynomial function in (1) until $\pi_s = \pi_s^{max}$ (which is a desired maximum value of splitting probability). When $\pi_s^{max} = 1$ and $\pi_s = \pi_s^{max}$, all flows are always moved to a new path.

$$f_{ExRED}(\hat{q}) = a_2\hat{q}^2 + a_1\hat{q} + a_0 \quad (1)$$

where coefficients of the positive increasing function are

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$a_2 = \frac{(k_{max} - k_{min}) - (K - k_{min})\pi_s^{max}}{(k_{max} - k_{min})(K - k_{max})^2}$$

$$a_1 = \frac{(k_{max}^2 + K^2 - 2k_{max}k_{min})\pi_s^{max} - 2k_{max}^2 + 2k_{max}k_{min}}{(k_{max} - k_{min})(K - k_{max})^2}$$

$$a_0 = \frac{k_{max}^3 - k_{max}^2 k_{min} - (k_{max}^2 + 2k_{max}k_{min} + k_{min}K)K\pi_s^{max}}{(k_{max} - k_{min})(K - k_{max})^2}$$

Equation (1) shows that ExRED provides flexible increasing of path-switching probability. It can prevent a consecutive path-switching in case of the average queue size is over maximum threshold and not exceeds limit of buffer size (K). We expect that this will allow us to utilize a particular path as much as possible while not causing overload on the path.

IV. Performance Evaluation

In this section, comparative performance under different conditions of real traffics is demonstrated.

A. Simulation model and parameters

Three simulation scenarios are conducted to compare the performance of load distribution models, by using 1-hour long real traffic traces [28], i.e., DSet1, DSet2, and DSet3, which are captured from primary Internet access point between Digital Equipment Corporation and the Internet. Characteristics of the traces are listed in Table I. Three paths exist between a pair of source and destination. Bandwidth capacities (or mean service rates) of path 1, path 2, and path 3 are 1, 4, and 7 Mbps, respectively; the total bandwidth capacity is 12 Mbps. As compared to the total bandwidth capacity, traffics generated from trace DSet1 and DSet2 incur heavy load and some load-spikes. Moreover, we use trace DSet3 to generate extremely heavy traffic which peak load is much higher than the total bandwidth capacity, thus incurring network overload.

With the set-up simulation environment, LDM/ExRED, LDM, LLF, and SRR are evaluated. In LDM/RED and LDM/ExRED, the parameters are chosen: EWMA parameter w=0.02, k_{min}=10, k_{max}=30, and π_s^{max}=0.1. These parameters setting are recommended in [24], [27], and [29]. In SRR, weights assigned for path 1, path 2, and path 3 are 1, 4, and 7, respectively, which are used for specifying desired forwarding rates on each path [5]. In LBPF, the size of the table is 20, W=1000, and P=20, where W is window size for detecting aggressive flows and P is period for splitting the aggressive flows. LBPF's parameters can be further read at [14].

B. Load Balancing Efficiency

Tables II shows that LDM/ExRED can achieve load balancing, as compared to the others since probabilities of buffer occupancy of all paths are almost equal. This can be implied that all paths are fairly utilized. Moreover, Table III shows that LDM/RED and LDM/ExRED can prevent buffer overflow; maximum queue sizes incurred by both of them are significantly smaller than those incurred by SRR and LDM. This is because burst traffic (which can cause a large queue) is detected by RED and then distributed over multiple paths.

TABLE I. Profile of Traffic Traces

Trace ID	# Packets x10^6	Traffic Rate (Mbps:)			# Different Flows	Flow Size (Packets)		Flow Rate (Flows/Second)		
		Mean	Min.	Max.		Mean	CV	Mean	Min.	Max.
DSet 1	2.66	5.91	2.07	13.65	5865	453.87	7.52	137.89	77	204
DSet 2	2.87	6.38	0.46	12.24	12903	222.71	5.98	175.32	44	247
DSet 3	3.86	8.58	1.86	15.45	12710	303.88	7.11	184.50	90	269

TABLE II. Probability of Buffer Occupancy

Load Distribution Model	Dset 1			Dset 2			Dset 3		
	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3
LDM/ExRED	0.71	0.66	0.65	0.73	0.68	0.65	0.86	0.82	0.80
LDM/RED	0.70	0.66	0.65	0.73	0.67	0.65	0.87	0.82	0.80
LDM	0.86	0.71	0.59	0.89	0.73	0.58	0.95	0.85	0.77
LLF	0.77	0.53	0.47	0.80	0.55	0.48	0.91	0.74	0.70
SRR	0.35	0.66	0.66	0.37	0.68	0.68	0.61	0.81	0.82

TABLE III. Maximum Queue Size (Packets)

Load Distribution Model	Dset 1			Dset 2			Dset 3		
	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3
LDM/ExRED	83	81	82	85	83	82	319	318	317
LDM/RED	100	98	100	104	97	102	376	375	375
LDM	1685	422	180	3845	378	76	5976	2780	522
LLF	92	92	93	83	83	83	293	293	293
SRR	43	86	185	33	88	165	110	350	557

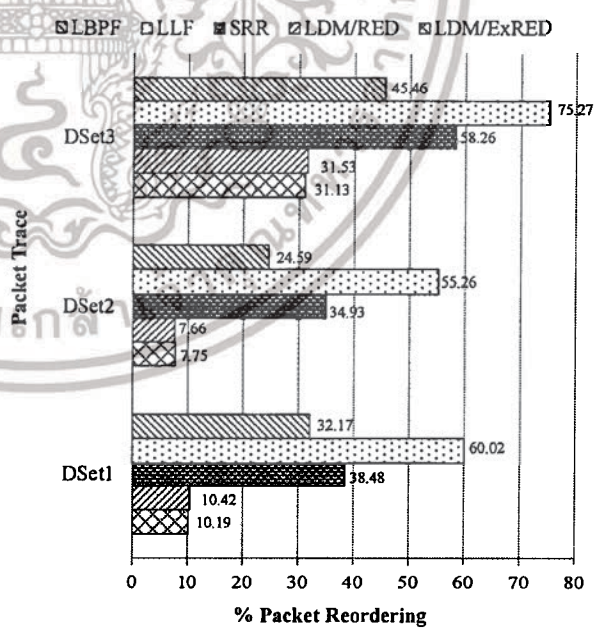


Figure 3. Risk of Packet Reordering

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

However, when buffer is highly utilized, RED causes consecutive marked packets while ExRED can prevent such problem. Therefore, LDM/ExRED can reduce peak buffer occupancy. A gateway device requires only a small buffer.

C. Packet Order Preservation

Fig. 3 illustrates that LDM/ExRED and LDM/RED can efficiently alleviate packet reordering inherently existing in packet-based models such as SRR and LLF. LDM is a flow-based model which can perfectly prevent packet reordering. SRR sends packets in a round robin manner. It can cause a risk of packet reordering. LLF choosing only the path with the shortest queue size can cause a high risk of packet reordering. LBPF splits a group of largest flows, thus leading to the risk of packet reordering. The discussion on this issue can be found in [2], [23], and [30]. As compared to LDM/RED, LDM/ExRED has a potential to maintain low risk of packet reordering because of a smaller path-switching probability. However, difference between delay on high congested path and that on a less congested path is also a factor of the risk of packet reordering [2], [23]. This is an open issue for further studies.

V. Concluding Remarks

This paper proposes a load distribution model for TCP transmission. LDM/ExRED takes advantages from RED mechanism in traffic splitting and distribute load subject to necessary condition to prevent packet reordering. With a modified RED, i.e., ExRED, it can prevent buffer overflow (due to burstiness of TCP flows) at a gateway and maintain low risk of packet reordering. The superiority of LDM/ExRED is presented by comparative performance among LDM/ExRED and the current existing load distribution models by simulations under variety of real traffic conditions.

References

[1] L. Golubchik, J. Lui, T. Tung, A. Chow, W. Lee, G. Franceschinis, and C. Anglano, "Multi-path continuous media streaming: What are the benefits?," *Performance Evaluation*, vol. 49, pp. 429–449, Sep. 2002.

[2] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "On Load Distribution over Multipath Networks," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 3, pp. 662–680, 2012.

[3] M. Menth, R. Martin, A. Koster, and S. Orlowski, "Overview of resilience mechanisms based on multipath structures," in *Proc. the 6th International Workshop on Design and Reliable Communication Networks (DRCN)*, La Rochelle, France, Oct. 2007.

[4] N. Wang, K. Ho, G. Pavlou, and M. Howarth, "An overview of routing optimization for Internet traffic engineering," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 1, pp. 36–56, 2008.

[5] H. Adiseshu, G. Parulkar, and G. Varghese, "A reliable and scalable striping protocol," *ACM SIGCOMM Computer Communication Review*, vol. 26, no. 4, pp. 131–141, Oct. 1996.

[6] K. G. Shin and C. J. Hou, "Design and Evaluation of Effective Load Sharing in Distributed Real-Time Systems," *IEEE Trans. Parallel and Distributed Systems*, vol. 5, no. 7, pp. 704–719, Jul. 1994.

[7] O. Kremien and J. Kramer, "Methodical analysis of adaptive load sharing algorithms," *IEEE Trans. Parallel Distribution Systems*, vol. 3, no. 6, pp. 747–760, Nov .1992.

[8] C. C. Hui and S. T. Chanson, "Hydrodynamic load balancing," *IEEE Trans. Parallel and Distributed Systems*, vol. 10, no. 11, pp. 1118–1137, Nov. 1999.

[9] Z. Tari, J. Broberg, A. Zomaya, and R. Baldoni, "A least flow-time first load sharing approach for distributed server farm," *Journal of Parallel and Distributed Computing*, vol. 65, no. 7, pp. 832–842, Jul. 2005.

[10] C. Villamizar, "OSPF optimized multipath (OSPF-OMP)," Internet draft draft-ietf-ospf-omp-02.txt, Feb. 1999.

[11] D. Thaler and C. Hopps, "Multipath issues in unicast and multicast next-hop selection," RFC 2991, Nov. 2000.

[12] A. Zinin, Cisco IP Routing, packet forwarding and intra-domain routing protocols. Reading, MA: Addison Wesley, 2002.

[13] J. Song, S. Kim, M. Lee, H. Lee, and T. Suda, "Adaptive load distribution over multipath in MPLS networks," in *Proc. IEEE ICC*, Anchorage, Alaska, May 2003, pp. 233–237.

[14] W. Shi, M. H. MacGregor, and P. Gburzynski, "Load balancing for parallel forwarding," *IEEE/ACM Trans. Networking*, vol. 13, no. 4, pp. 790–801, Aug. 2005.

[15] S. Kandula, D. Katabi, S. Sinha, and A. Berger, "Dynamic load balancing without packet reordering," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 2, pp. 53–62, Apr. 2007.

[16] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis, "Framework for IP performance metrics," RFC 2330, May. 1998.

[17] C. Demichelis and P. Chimento, "IP packet delay variation metric for IP performance metrics (IPPM)," RFC 3393, Nov. 2002.

[18] N. M. Piratla, A. P. Jayasumana, A. A. Bare, and T. Banka, "Reorder buffer-occupancy density and its application for measurement and evaluation of packet reordering," *Computer Communications*, vol. 30, no.9, pp.1980–1993, Jun. 2007.

[19] N. M. Piratla and A. P. Jayasumana, "Reordering of packets due to multipath forwarding – An analysis," in *Proc. IEEE ICC*, Istanbul, Turkey, Jun. 2006, pp. 829–834.

[20] A. Morton, L. Ciavattone, G. Ramachandran, S. Shalunov, and J. Perser, "Packet reordering metrics," RFC 4737, Nov. 2006.

[21] A. Jayasumana, N. Piratla, T. Banka, and R. Whitner, "Improved packet reordering metrics," RFC 5236, Jun. 2008.

[22] S. Jaiswal, G. Iannaccone, C. Diot, J. Kurose, and D. Towsley, "Measurement and classification of out-of-sequence packets in a tier-1 IP backbone," *IEEE/ACM Trans. Networking*, vol. 15, no. 1, pp. 54–66, Feb. 2007.

[23] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "On the Performance Analysis of Traffic Splitting on Load Imbalancing and Packet Reordering of Bursty Traffic," in *Proc. IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC 2009)*, Beijing, China, Nov. 2009.

[24] S. Floyd and V. Jacobsan, "Random Early Detection Gateways for Congestion Avoidance," *IEEE/ACM Trans. Networking*, vol. 1, no. 4. pp. 397-413, Aug. 1993.

[25] S. Floyd and V. Jacobson, "On traffic phase effects in packet-switched gateways," *Internetworking: Research & Experience*, vol. 3, no. 3, Sep. 1992, pp.115-56, UK.

[26] S. Prabhavat, N. Kato, and R. Varakulsiripunth, "Load Distribution Mechanism for Multipath TCP Communication," in *Proc. International Symposium on Technology for Sustainability (ISTS 2011)*, Bangkok, Thailand, Jan. 2012, pp. 321–324.

[27] S. Prabhavat and R. Varakulsiripunth, "Performance Improvement on RED Based Gateway in TCP Communication Network," in *Proc. International Conference on Control, Automation and Systems (ICCAS 2004)*, Bangkok, Thailand, Aug. 2004, pp. 782–787.

[28] (Online Sources) P. Danzig, J. Mogul, V. Paxson, and M. Schwartz. (1995, Mar.). *The Internet Traffic Archive*. Available: http://ita.ee.lbl.gov/index.html.

[29] (Online Sources) S. Floyd (1967, Nov.), "RED: Discussions of Setting Parameters," Available: http://www.icir.org/floyd/REDparameters.txt.

[30] S. Prabhavat, H. Nishiyama, N. Ansari, and N. Kato, "Effective Delay-Controlled Load Distribution over Multipath Networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 10, pp. 1730–1741, Oct. 2011.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

International Symposium on Technology for Sustainability
November 21 – 24, 2012, Swissôtel Le Concorde, Bangkok, Thailand

Mark-Reverse Explicit Congestion Notification for Satellite IP Networks: Simulation and Analysis Results

Masato Inoue*, Pakapol Tangdumrongrat**, Sumet Prabhavat**, Satoshi Utsumi*,
Salahuddin Muhammad Salim Zabir*** and Norio Shiratori****

*Tsuruoka National College of Technology, Yamagata, Japan
**King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
***France Telecom Japan, Tokyo, Japan
****Tohoku University/Waseda University, Sendai/Tokyo, Japan
e-mail: u-satoshi@tsuruoka-nct.ac.jp

***Abstract*—In this paper, we propose a new congestoin notification scheme, named as Mark-Reverse ECN (Explicit Congestion Notification) for satellite IP networks. Simulation and analysis are conducted for performance evaluation. This analytical model takes the packet drop ratio and the packet mark ratio into account. We show that the results from the analytical model and the simulation match quite closely.**

Primary Categories — Informatics.
Secondary Categories — Computer System/Network.
Keywords — ECN (Explicit Congestion Notification), Congestion Control, Satellite IP Network, Analytical Model.

I. Introduction

Explicit Congestion Notification (ECN) has been proposed for the Internet as a means for detecting an incipient congestion before it actually occurs and notifying that explicitly to the corresponding end hosts. This has the potential to improve the network performance under congestion scenarios than conventional packet dropping mechanisms [1]. Random Early Detection (RED) with ECN gives definite improvement in time delays for interactive traffic. In [1], they examined use of a Backward Explicit Congestion Notification (BECN) mechanism to inform the sender of the congestion situation in the network. Because this mechanism uses ICMP Source Quenches (ISQs) for backward notification, the TCP senders would be attacked by the blind throughput-reduction attack [2].

In this paper, we propose a new congestion notification scheme, we name as Mark-Reverse ECN for satellite IP networks. Contrary to the conventional ECN mechanisms, rather then marking the packets in the forward direction, our proposed scheme marks the packets containg the ACKs in the reverse direction bound for the source nodes. The ACKs eventually notify congestion to the source nodes. As such, this mechanism leads to a faster notification of an incipent congestion.

The rest of this paper is organized as follows. In section II, we propose our novel marking scheme, Mark-Reverse ECN following a brief outline of existing schemes. In section III, we evaluate our scheme by comparing with the conventional scheme through simulations. Section IV describes a new analytical model for ECN. Finally, we conclude this paper in section V.

II. Our Proposal: Mark-Reverse ECN

Before presenting our novel mechanism, we first provide a brief outline of the conventional marking schemes.

A. Conventional ECN Schemes

Fig. 1 demonstrates Mark-Tail ECN [3]. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. It will be marked before forwarded to its destination. Source S will be notified about the congestion after this packet arrives at destination D and its ACK packet returns (at time t_2). Notification delay is almost RTT (Round Trip Time).

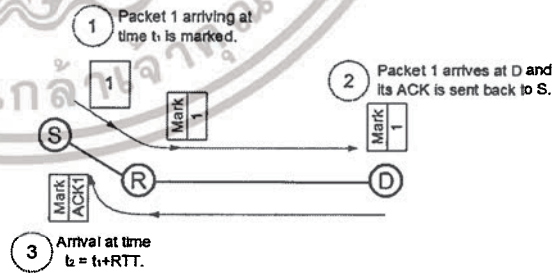


Fig. 1. Mark-Tail ECN Scheme.

B. Mark-Reverse ECN

Fig. 2 shows how our proposal Mark-Reverse ECN works. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. When an ACK packet of any previous packet arrives at the router, e.g., at time t_1^+,

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

it will be marked before being forwarded to its destination (i.e., Source S).Assume that the ACK packet acknowledges the successful delivery of packet 0 which is previously sent at time t_0. Notification delay $\Delta t = t_1^+ - t_1$ is very small.

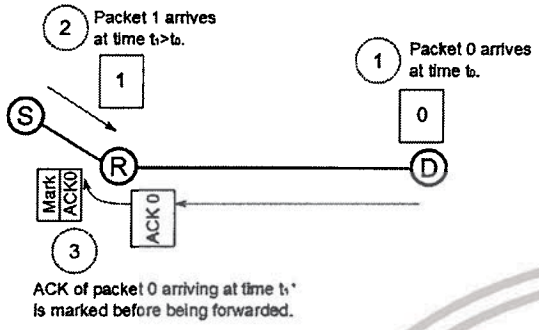


Fig. 2. Mark-Reverse ECN Scheme.

III. Simulation

We use ns-2 [4] for our simulations with respect to the simulation scenario as shown in Fig. 3. We set the packet size 1,000bytes, the maximum window size 1000 segments, the capacity of the satellite link between senders and receivers 10Mbps (about 1,300 packets/sec), round trip time of the satellite link 550ms, and the link error ratio 0%. We changed the number of TCP flows. We set RED for ECN on the forwarding node of the satellite link. We observed the throughput, the packet drop ratio and the packet marking ratio. The simulation time is 500s. Simulation results are in Fig. 4, Fig. 5, and Fig. 6.

IV. Analytical Models for ECN

Our proposed model is composed of four parts according to a typical short-lived flow evolution: the start of the connection (three-way-handshake), the initial slow-start phase, the first loss (or mark) part, and the subsequent losses or marks.

A. The Connection Start-Up Phase

Every TCP connection starts with the three-way-handshake process. Assuming that no ACK packets can get lost, this process can be well modeled as follows [5]:

$$E[T_{twhs}] = RTT + T_s(\frac{1-p}{1-2p} - 1), \quad (1)$$

where T_s is the duration of SYN time-out and p is the packet loss ratio.

B. The Initial Slow-Start Phase

In order to derive the latency for this phase, $E[Y^{SS}]$, the expected number of packets sent until a loss or a mark occurs is given by following enhanced equation (based on the one given in [5]):

$$E[Y^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q))}{p+q}, \quad (2)$$

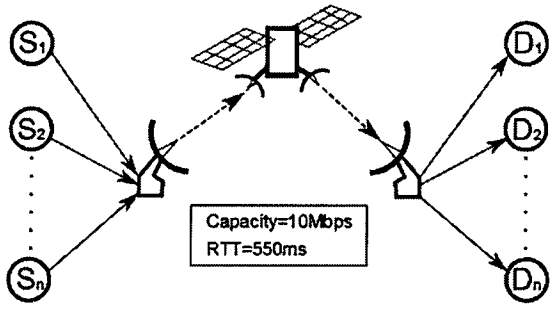


Fig. 3. Simulation scenario.

where d is the total file size measured in packets that must be transmitted and q is the packet marking ratio.

Substituting the value of $E[Y^{SS}]$ in the Equation (2), we get the expected size of congestion window at the end of the low-start phase due to the packet losses or the packet marks:

$$E[W^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q)) + 2(p+q)}{(p+q)g^2}, \quad (3)$$

where $g = 1.61804$ [5].

The expected slow-start latency is calculated as follows [5]:

$$E[n] = \begin{cases} \lceil log_g(\frac{W_m}{C_1}) \rceil \\ +\frac{1}{W_m}(E[Y^{ss}] - g^2 W_m - 2), when\ E[W^{ss}] > W_m \\ \lceil log_g(\frac{E[Y^{SS}]+2}{C_1}) \rceil - 2, when\ E[W^{SS}] \le W_m \end{cases} \quad (4)$$

C. The First Loss

Assume that the first indication to detect congestion is a packet loss. In the round where a TD (triple-duplicate) occurs, let W^{SS} be the current size of *cwnd*, which has a value w. In this round, w packets were sent. Among them, k packets are assumed to be ACKed. Since the connection is still in the slow-start phase, *cwnd* increases to $w + k$ and another $2k$ packets are sent in the next round. If more then three packets from these $2k$ packets get ACKed, then a TD would occur; otherewise, a TO would take place. Let

$$A(w,k) = \frac{(1-p)^k p}{1-(1-p)^w}, \quad (5)$$

be the probability that the first k packets have been successfully transmitted and ACKed in a round of w packets, provided that there might be one or more packets got lost. Now, let

$$h(m) = \sum_{i=0}^{2}(1-p)^i p, for\ m \ge 3, \quad (6)$$

be the probability that no more than 2 packets have been transmitted successfully in a round of m packets. We the

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

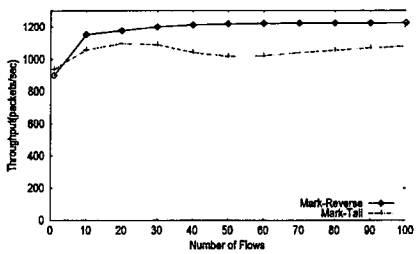


Fig. 4. Throughput comparisons between Mark-Reverse ECN and Mark-Tail ECN.(simulation results)

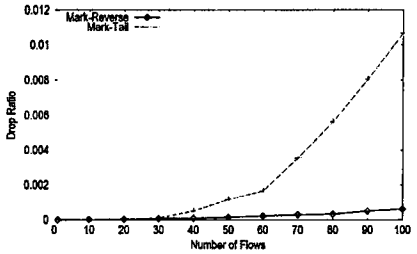


Fig. 5. Drop ratio comparisons between Mark-Reverse ECN and Mark-Tail ECN.(simulation results)

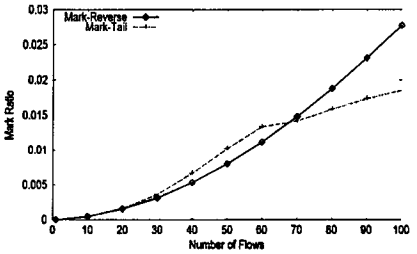


Fig. 6. Mark ration cmparisons between Mark-Reverse ECN and Mark-Tail ECN.(simulation results)

obtain $Q(w)$, the probability that a loss in a window size w is a TO (Timeout), is given by

$$Q(w) = \begin{cases} 1 & ,when\ w \leq 3 \\ \sum_{k=0}^{2} A(w,k) + \sum_{k=3}^{w-1} A(w,k)h(k) & ,otherwise \end{cases} \quad (7)$$

The expected time that TCP spends in the RTOs is given in [7] as:

$$E[Z^{TO}] = T_0 \frac{f(p)}{1-p}, \quad (8)$$

where T_0 is the average duration of the first time-out, and

$$f(p) = 1 + p + 2p^2 + 4p^3 + 8p^4 + 16p^5 + 32p^6. \quad (9)$$

Finally, the expected latency that this loss would incur is

$$T_{loss} = \frac{p}{p+q} \times (1-(1-(p+q))^d) \times (Q(W^{SS})E[Z^{TO}] + (1-Q(W^{SS}))RTT). \quad (10)$$

D. Sending the Rest of the Packets

After the first packet loss or the first packet mark, the transmission latency of the rest $(d - E[Y_{init}])$ packets is obtained as follows:

$$T_{rest} = \frac{d - E[Y^{SS}]}{H}, \quad (11)$$

where H is the throughput of a steady-state flow.

The expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = E[\alpha] + E[W^{TDM}] - 1, \quad (12)$$

where $E[\alpha]$ is the expected number of packets sent in a TDMP (triple-duplicate or marking period) up to and including the first packet that is lost or marked. Given our loss and mark model, the probability that $\alpha_i = k$ is equal to the probability that exactly $k-1$ packets are successfully acknowkedged before a loss or a mark occurs is

$$P[\alpha = k] = (1-(p+q))^{k-1}(p+q), k = 1, 2, \ldots. \quad (13)$$

The mean of α is thus,

$$E[\alpha] = (1-(p+q))^{k-1}(p+q)k = \frac{1}{p+q}. \quad (14)$$

From (12) and (14) it follows that

$$E[Y] = \frac{1-(p+q)}{p+q} + E[W^{TDM}]. \quad (15)$$

From [8] the expected round where the first loss or the first mark occurs, $E[X]$, is

$$E[X] = b(\frac{E[W^{TDM}]}{2} + 1). \quad (16)$$

From [8] the expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) + E[\beta]. \quad (17)$$

Then, from Equations (15) and (17), we get the following expression which involves $E[W^{TDM}]$:

$$\frac{1-(p+q)}{p+q} + E[W^{TDM}] = \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) + E[\beta]. \quad (18)$$

For simplicity, we assume β_i to be uniformly distributed between 1 and $W_i - 1$. Thus, $E[\beta] = E[W^{TDM}]/2$.

Combining (16) and (18), we get:

$$E[W^{TDM}] = -\frac{2(b-1)}{3b} + \sqrt{\frac{4(b(p+q)+2(1-(p+q)))}{3b(p+q)} + (\frac{2(b-1)}{3b})^2}. \quad (19)$$

From [8], the expected value of duration of a round, $E[A]$, is

$$E[A] = RTT(\frac{p}{p+q}(E[X]+1) + \frac{q}{p+q}E[X]). \quad (20)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

E. Impact of Window Limitation

At the beginning of TCP flow establishment, the receiver advertises a maximum buffer size which determines a maximum congestion window size, W_m. As a consequence, during a period without loss indications, the window size can grow up to W_m, but will not grow further beyond this value. During the first TDMP, the window grows linearly up to W_m for U rounds, then remains constant for V rounds, and then a triple-duplicate or marking indication occurs. The expected U rounds, $E[U]$, is as follows [7]:

$$E[U] = \frac{b}{2}W_m. \tag{21}$$

Since Y_i, the number of packets in the ith TDMP, does not depend on window limitation, $E[Y]$ is given by (12):

$$E[Y] = E[\alpha] + W_m - 1. \tag{22}$$

From [7],

$$E[Y] = \frac{3}{4}W_m E[U] + W_m E[V]. \tag{23}$$

Then,

$$\frac{1-(p+q)}{p+q} + W_m = \frac{3b}{8}W_m^2 + W_m E[V]. \tag{24}$$

Thus,

$$E[V] = \frac{1-(p+q)}{(p+q)W_m} + 1 - \frac{3b}{8}W_m. \tag{25}$$

Finally, since $X_i = U_i + V_i$ in ith TDMP, we have

$$E[X] = E[U] + E[V] = \frac{b}{8}W_m + \frac{1-(p+q)}{(p+q)W_m} + 1. \tag{26}$$

The expected number of packets that have been received in a TDMP, $E[Y']$, is

$$\begin{aligned} E[Y'] &= \frac{p}{p+q}(E[\alpha] + E[\beta] - 1.0) \\ &\quad + \frac{q}{p+q}(E[\alpha] + E[W^{TDM}] - E[\beta] - 1.0) \\ &= E[\alpha] + \frac{E[W^{TDM}]}{2} - 1.0. \end{aligned} \tag{27}$$

The expected number of packets received in the time-out phase,

$$E[R] = 1. \tag{28}$$

Thus, the throughput can be formulated as:

$$H = \frac{E[Y'] + \frac{p}{p+q}Q(W^{TDM}) * E[R]}{E[A] + \frac{p}{p+q}Q(W^{TDM}) * E[Z^{TO}]}. \tag{29}$$

From [5], the total expected latency is

$$T_{latency} = E[T_{twhs}] + E[n]RTT + T_{loss} + T_{rest} - \frac{RTT}{2}. \tag{30}$$

Here, the delay caused by the delayed acknowledgment for the first packet is 0ms. That is, the option of delayed acknowledgment is off.

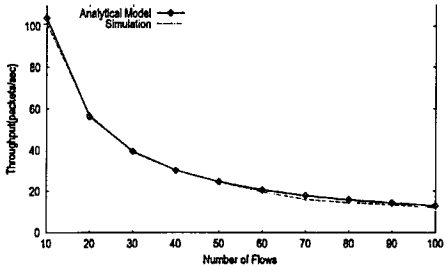


Fig. 7. Throughput comparisons between analytical model and simulation for Mark-Reverse ECN.

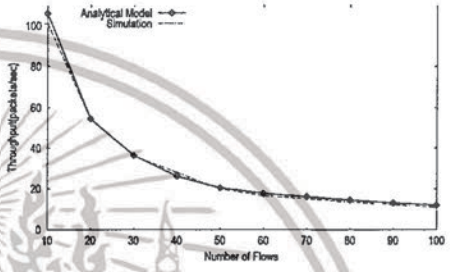


Fig. 8. Throughput comparisons between analytical model and simulation for Mark-Tail ECN.

F. Verification

Fig. 7 and Fig. 8 show the results of this analytical model comparing with simulation results.

V. Conclusion

In this paper, we propose a novel congestion notification scheme, that we name as Mark-Reverse ECN for satellite IP networks. Simulation results show that Mark-Reverse can ensure higher throughput and lower packet drop ratio. In addition, we propose an analytical model for ECN. Analytical results also verify that Mark-Reverse ECN yields better performance than conventional or Mark-Tail mechanisms.

References

[1] F. Akujobi, I. Lambadaris, R. Makkar, N. Seddigh, and B. Nandy, "BECN for Congestion Control in TCP/IP Neworks: Study and Comparative Evaluation," *IEEE Globecom 2002,* Nov. 2002.
[2] RFC 5927, "ICMP Attacks against TCP," July 2010.
[3] S. Floyd, "TCP and Explicit Congestion Notification," Computer Communications Review, vol. 24, no. 5, Oct. 1994.
[4] UCB/LBNL/VINT Nework Simulatior (NS).
[5] D. Zheng, G. Y. Lazarou, and R: Hu, "A Stochastic Model for Short-lived TCP Flows," IEEE International Conference on Communications 2003 (ICC 2003), May 2003, pp.11-15.
[6] N. Cardwell, S. Savage, and T. Anderson, "Modeling TCP Latency," in Proc. *IEEE INFOCOM 2000,* vol. 3, Mar. 2000, pp.1742-1751.
[7] J. Padhye, V. Firouiu, D. F. Towsley, and J. F. Kurose, "Modeling TCP Reno Performance: A Simple Model and Its Empirical Validation," *IEEE/ACM Trans. Networking,* vol. 8, no. 2, pp.133-145, Apr. 2000.
[8] D. Zheng, "On the modeling of TCP latency and throughput," Master's thesis Mississippi State University, 2002.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

Mark-Reverse Explicit Congestion Notification: Concept, Analysis and Evaluation

Masato INOUE†, Pakapol TANGDUMRONGRAT††, Sumet PRABHAVAT††, Satoshi UTSUMI†,
Salahuddin MUHAMMAD SALIM ZABIR†††, and Norio SHIRATORI††††

† Tsuruoka National College of Technology 104 Sawada, Inooka, Tsuruoka, Yamagata, 997–8511 Japan
†† King Mongkut's Institute of Technology Ladkrabang Chalongkrung Rd., Ladkrabang, Bangkok 10520, Thailand
††† France Telecom Japan Co., Ltd Keio Shinjuku Oiwake Bldg. 9F, 3–1–13 Shinjuku, Shinkjuku-ku, Tokyo, 160–0022 Japan
†††† Tohoku University 2-1-1 Katahira, Aoba-ku, Sendai, 980–8577 Japan

Abstract In this paper, we propose a new congestion notification scheme, named as Mark-Reverse ECN (Explicit Congestion Notification) for satellite IP networks. When congestion is beginning to occur on a link, our scheme notifies a source node more quickly than a conventional scheme, i.e., Mark-Tail ECN. Instead of a packet on forwarding path, we marks an acknowledge (ACK) packet on backwarding path which is heading for the source node. We expect that latency time for congestion notification will be reduced and congestion control will thus work more accurately and effectively. Simulation and analysis are conducted for performance evaluation. Through simulation, we compare and evaluate performance of Mark-Reverse ECN and Mark-Tail ECN. Mark-Reverse ECN shows high throughput and low packet drop ratio in satellite IP networks. In analysis, we propose a new analytical model of TCP NewReno supporting ECN. This analytical model takes the packet drop ratio and the packet mark ratio into account for computing delay time and throughput. Analytical results also show superiority of our scheme, correspondingly. A considerably small discrepancy between the results verify our simulation and analysis.

Key words ECN (Explicit Congestion Notification), Congestion Control, Satellite IP Network, Analytical Model.

1. Introduction

Explicit Congestion Notification (ECN) was proposed for the Internet as a means of explicitly notifying end-hosts of network congestion by marking, instead of dropping packets [1]. Random Early Detection (RED) [2] with ECN gives definite improvement in time delays for interactive traffic. In [1], they examined use of a Backward Explicit Congestion Notification (BECN) mechanism to inform the sender of the congestion situation in the network. Because this mechanism uses ICMP Source Quenches (ISQs) for backward notification, the TCP senders would be attacked by the blind throughput-reduction attack [3].

In this paper, we propose a new congestoin notification scheme, named as Mark-Reverse ECN for satellite IP networks. Our proposal, i.e., Mark-Reverse ECN is a scheme that marks ACKs in the opposite direction of the same path when congestion is beginning to occur on the link. The ACKs notifies congestion to the distination node.

The rest of this paper is organized as follows: In section 2., we describe a conventional ECN scheme, i.e., Mark-Tail ECN. In section 3., we propose a new ECN scheme, i.e., Mark-Reverse ECN. In section 4., we evaluate our scheme comparing with the conventional scheme through simulations. Section 5. describes a new analytical model for ECN. Finally, section 6. concludes ths paper.

2. Conventional Scheme: Mark-Tail ECN [4]

Fig. 1 demonstrates Mark-Tail ECN [4]. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. It will be marked before forwarded to its destination. Source S will be notified about the congestion after this packet arrives at destination D and its ACK packet returns (at time t_2). Notification delay is almost RTT.

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย ห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

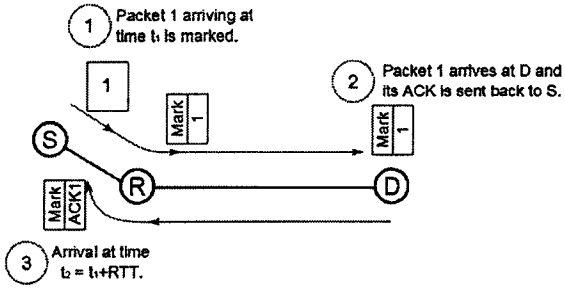


Fig. 1 Mark-Tail ECN Scheme.

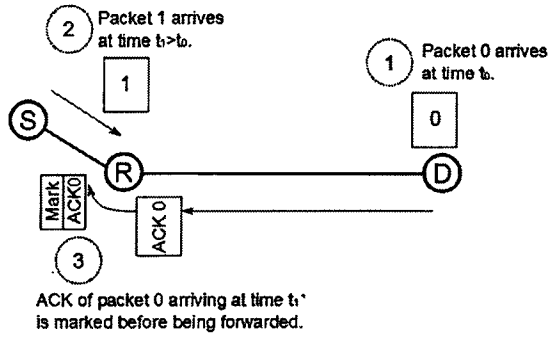


Fig. 2 Mark-Reverse ECN Scheme.

3. Our Proposal: Mark-Reverse ECN

Our proposal Mark-Reverse ECN scheme needs Mark-Reverse ECN-Capable Transport (MR-ECT) bit on IP packets. (MR-ECT bit should not be on at once with ECN-Capable Transport (ECT) bit.) Also, Mark-Reverse ECN scheme needs Congestion Experienced (CE) bit on IP packets. According to Random Early Detection (RED) mechanisms on the queue of the positive direction, the CE bit on the packet whose MR-ECT bit is on in the reverse direction of the same link supporting Mark-Reverse ECN becomes on when the packet is passing in the reverse direction. Mark-Tail ECN scheme and Mark-Front ECN scheme [5] need about RTT to notify congestion to the source node. Mark-Reverse ECN scheme needs about 0 msec to notify congestion to the source node, if the congestion link is near the source node. Because of the fast notification, the number of packet losses due to congestion can be minimized. Especially, it is very useful when the bottleneck link is satellite one. Because Mark-Reverse ECN scheme uses the packets of the same connection for congestion notification differing with Backward Explicit Congestion Notification (BECN), Mark-Reverse ECN scheme can avoid the blind throughput-reduction attack. That is, ICMP Source Quench (ISQ) message of BECN can be transmitted from an arbitrary node to the source node, the Mark-Reverse ECN is notified only from the nodes passed through by the flow using the connection. Moreover, there is no overhead by notifying messages as ISQ messages.

Fig. 2 shows how our proposal Mark-Reverse ECN works. At time t_1, packet 1 arrives at router R and suddenly causes the router to experience congestion. When an ACK packet of any previous packet arrives at the router, e.g., at time t_1^+, it will be marked before being forwarded to its destination (i.e., Source S). Assume that the ACK packet acknowledges the successful delivery of packet 0 which is previously sent at time t_0. Notification delay $\Delta t = t_1^+ - t_1$ is very small.

4. Simulation

4.1 Evaluation of Throughput, Drop ratio and Mark ratio

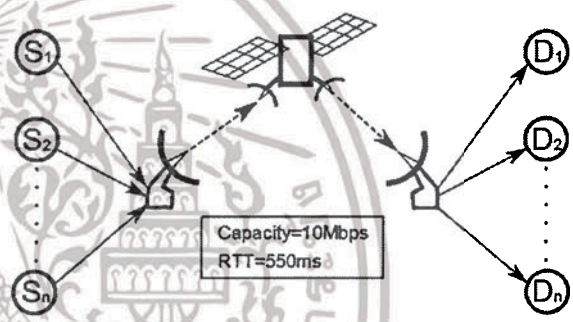


Fig. 3 Simulation scenario.

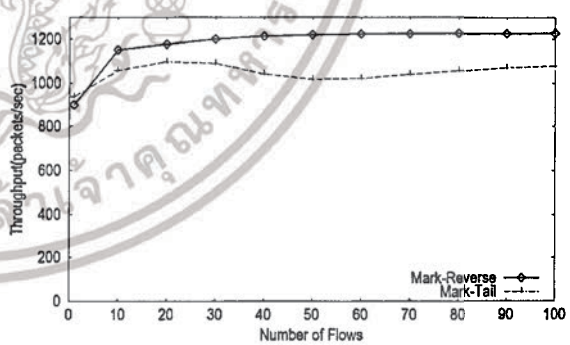


Fig. 4 Throughput comparisons between Mark-Reverse ECN and Mark-Tail ECN. (simulation results)

We use ns-2 [6] for network simulations. We evaluate throughput, drop ratio and mark ratio in the simulation scenario as shown in Fig. 3. We set the packet size 1,000bytes, the maximum window size 1,000 segments, the capacity of the satellite link between senders and receivers 10Mbps (about 1,300 packets/sec), round trip time of the satellite link 550ms, and the link error ratio 0%. We changed the number of TCP flows. We set RED for ECN on the forwarding node of the satellite link. We observed the throughput,

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

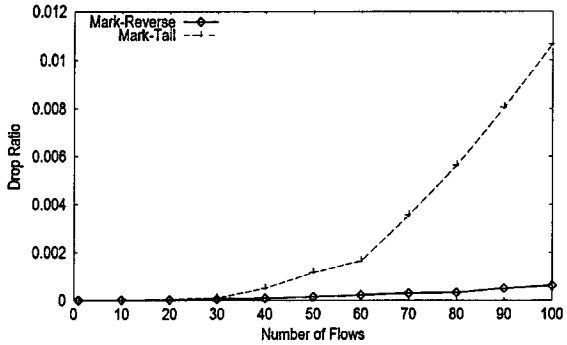


Fig. 5 Drop ratio comparisons between Mark-Reverse ECN and Mark-Tail ECN. (simulation results)

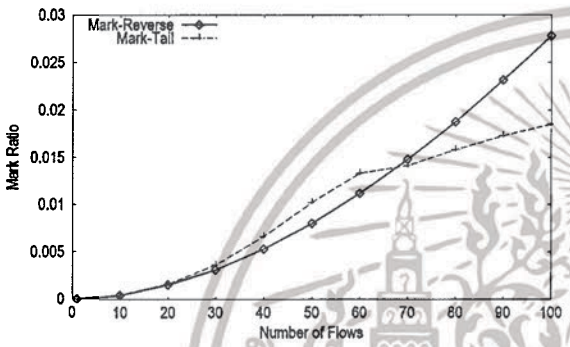


Fig. 6 Mark ratio cmparisons between Mark-Reverse ECN and Mark-Tail ECN. (simulation results)

the packet drop ratio and the packet mark ratio. The simulation time is 500s. Simulation results are in Fig. 4, Fig. 5, and Fig. 6.

5. Analytical Models for ECN

Our proposed model is composed of four parts according to a typical short-lived flow evolution: the start of the connection (three-way-handshake), the initial slow-start phase, the first loss (or mark) part, and the subsequent losses or marks.

5.1 The Connection Start-Up Phase

Every TCP connection starts with the three-way-handshake process. Assuming that no ACK packets can get lost, this process can be well modeled as follows [7]:

$$E[T_{twhs}] = RTT + T_s(\frac{1-p}{1-2p} - 1), \quad (1)$$

where T_s is the duration of SYN time-out and p is the packet loss ratio.

5.2 The Initial Slow-Start Phase

In order to derive the latency for this phase, $E[Y^{SS}]$, the expected number of packets sent until a loss or a mark occurs is given by following enhanced equation (based on the one given in [7]):

$$E[Y^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q))}{p+q}, \quad (2)$$

where d is the total file size measured in packets that must be transmitted and q is the packet mark ratio.

Substituting the value of $E[Y^{SS}]$ in the Equation (2), we get the expected size of congestion window at the end of the low-start phase due to the packet losses or the packet marks:

$$E[W^{SS}] = \frac{(1-(1-(p+q))^d)(1-(p+q)) + 2(p+q)}{(p+q)g^2}, \quad (3)$$

where $g = 1.61804$ [7].

The expected slow-start latency is calculated as follows [7]:

$$E[n] = \begin{cases} \lceil log_g(\frac{W_m}{C_1})\rceil + \frac{1}{W_m}(E[Y^{ss}] - g^2 W_m - 2) \\ \qquad , when\ E[W^{ss}] > W_m \\ \lceil log_g(\frac{E[Y^{SS}]+2}{C_1})\rceil - 2 \\ \qquad , when\ E[W^{SS}] \leqq W_m \end{cases} \quad (4)$$

5.3 The First Loss

Assume that the first indication to detect congestion is a packet loss. In the round where a TD (triple-duplicate) occurs, let W^{SS} be the current size of *cwnd*, which has a value w. In this round, w packets were sent. Among them, k packets are assumed to be ACKed. Since the connection is still in the slow-start phase, *cwnd* increases to $w+k$ and another $2k$ packets are sent in the next round. If more then three packets from these $2k$ packets get ACKed, then a TD would occur; otherewise, a TO would take place. Let

$$A(w,k) = \frac{(1-p)^k p}{1-(1-p)^w}, \quad (5)$$

be the probability that the first k packets have been successfully transmitted and ACKed in a round of w packets, provided that there might be one or more packets got lost. Now, let

$$h(m) = \sum_{i=0}^{2}(1-p)^i p, \ for\ m \geqq 3, \quad (6)$$

be the probability that no more than 2 packets have been transmitted successfully in a round of m packets. As [7], we obtain $Q^{SS}(W^{SS})$, the probability that a loss in a window size W^{SS} of slow-start phase is a TO (Timeout), is given by

$$Q^{SS}(W^{SS}) = \begin{cases} 1 & , when\ w \leqq 2 \\ \sum_{k=0}^{1} A(W^{SS},k) & \\ + \sum_{k=2}^{w-1} A(W^{SS},k)h(2k) & , otherwise \end{cases} \quad (7)$$

The expected time that TCP spends in the RTOs is given in [9] as:

$$E[Z^{TO}] = T_0 \frac{f(p)}{1-p}, \quad (8)$$

where T_0 is the average duration of the first time-out, and

$$f(p) = 1 + p + 2p^2 + 4p^3 + 8p^4 + 16p^5 + 32p^6. \quad (9)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Finally, the expected latency that this loss would incur is

$$T_{loss} = \frac{p}{p+q}(1-(1-(p+q))^d) \times (Q(W^{SS})E[Z^{TO}] + (1-Q(W^{SS}))RTT). \quad (10)$$

5.4 Sending the Rest of the Packets

After the first packet loss or the first packet mark, the transmission latency of the rest $(d - E[Y_{init}])$ packets is obtained as follows:

$$T_{rest} = \frac{d - E[Y^{SS}]}{H}, \quad (11)$$

where H is the throughput of a steady-state flow.

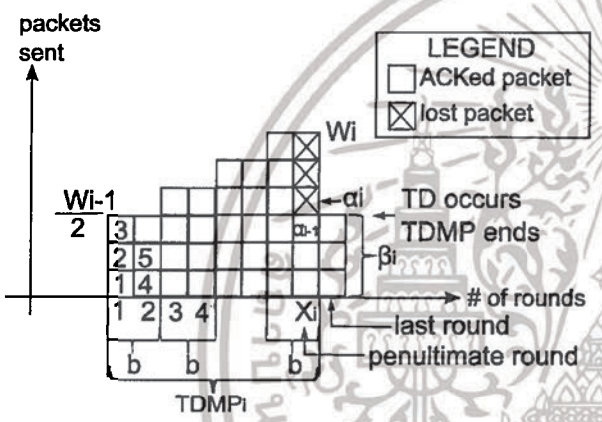


Fig. 7 Pacekts sent during a TDMP when a packet loss occurs.

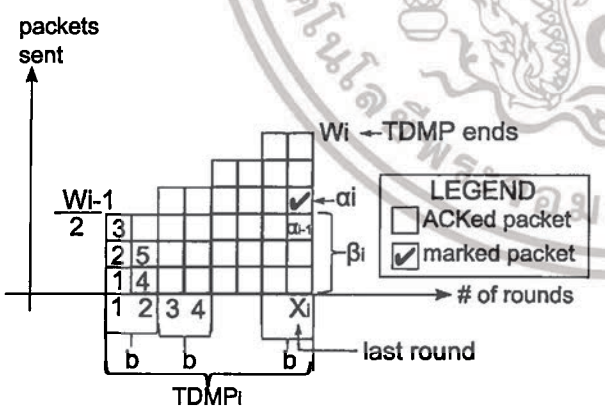


Fig. 8 Packets sent during a TDMP when a marking occurs.

We define TDMP (triple-duplicate or marked period) to be the period between tow triple-duplicate (TD) losses or receipts of marked ACKs. With reference to Fig. 7 when a packet loss occur, and with reference to Fig. 8 when receiving a marked ack, the following enhanced equations are given baesd on [8].

$$Y_i = \begin{cases} \alpha_i + W_i^{TDM} - 1 & ,when\ a\ packet\ loss \\ \alpha_i - (\beta_i + 1) + W_i^{TDM} & ,when\ a\ marked\ ack \end{cases} \quad (12)$$

$$A_i = \begin{cases} \Sigma_{j=1}^{X_i+1} r_{ij} & ,when\ a\ packet\ loss \\ \Sigma_{j=1}^{X_i} r_{ij} & ,when\ a\ marked\ ack \end{cases} \quad (13)$$

$$W_i^{TDM} = \frac{W_{i-1}^{TDM}}{2} + \frac{X_i}{b} - 1, \quad (14)$$

$$Y_i = \begin{cases} \frac{X_i}{2}(\frac{W_{i-1}^{TDM}}{2} + W_i^{TDM} - 1) + \beta_i & \\ \qquad ,when\ a\ packet\ loss & \\ \frac{X_i}{2}(\frac{W_{i-1}^{TDM}}{2} + W_i^{TDM} - 1) & \\ \qquad ,when\ a\ marked\ ack & \end{cases} \quad (15)$$

where X_i is the penultimate round in the TDMP which experiences packet losses, r_{ij} is the round trip tim, W_i^{TDM} is the window size at the end of a TDMP, α_i is the number of packets sent in a TDMP until the first loss or the first receipt of a marked ACK happens, and β_i is the number of packets sent before the loss or the receipt of a marked ack in the round.

The expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = \begin{cases} E[\alpha] + E[W^{TDM}] - 1 & \\ \qquad ,when\ a\ packet\ loss & \\ E[\alpha] - E[\beta] - 1 + E[W^{TDM}] & \\ \qquad ,when\ a\ marked\ ack & \end{cases} \quad (16)$$

where $E[\alpha]$ is the expected number of packets sent in a TDMP up to and including the first packet that is lost or marked. Given our loss and mark model, the probability that $\alpha_i = k$ is equal to the probability that exactly $k-1$ packets are successfully acknowkedged before a loss or a mark occurs is

$$P[\alpha = k] = (1-(p+q))^{k-1}(p+q), k = 1, 2, \ldots. \quad (17)$$

The mean of α is thus,

$$E[\alpha] = (1-(p+q))^{k-1}(p+q)k = \frac{1}{p+q}. \quad (18)$$

From (16) and (18) it follows that

$$E[Y] = \begin{cases} \frac{1-(p+q)}{p+q} + E[W^{TDM}] & \\ \qquad ,when\ a\ packet\ loss & \\ \frac{1-(p+q)}{p+q} - E[\beta] + E[W^{TDM}] & \\ \qquad ,when\ a\ marked\ ack & \end{cases} \quad (19)$$

From [10] the expected round where the first loss or the first mark occurs, $E[X]$, is

$$E[X] = b(\frac{E[W^{TDM}]}{2} + 1). \quad (20)$$

From [10] the expected value of the number of packets sent in a round when a packet loss occurs, $E[Y]$, is

$$E[Y] = \begin{cases} \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) + E[\beta] & \\ \qquad ,when\ a\ packet\ loss & \\ \frac{E[X]}{2}(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1) & \\ \qquad ,when\ a\ marked\ ack & \end{cases} \quad (21)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ ดัดแปลง เผยแพร่ หรือแสวงหาประโยชน์ทางการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Then, from Equations (20), (19) and (21), we get the following expression which involves $E[W^{TDM}]$:

$$\frac{1-(p+q)}{p+q} + E[W^{TDM}] = \frac{E[X]}{2}\left(\frac{E[W^{TDM}]}{2} + E[W^{TDM}] - 1\right) + E[\beta]. \quad (22)$$

For simplicity, we assume β_i to be uniformly distributed between 1 and $W_i - 1$. Thus, $E[\beta] = E[W^{TDM}]/2$.

Combining (20) and (22), we get:

$$E[W^{TDM}] = -\frac{2(b-1)}{3b} + \sqrt{\frac{4(b(p+q)+2(1-(p+q)))}{3b(p+q)} + \left(\frac{2(b-1)}{3b}\right)^2}. \quad (23)$$

From [10], the expected value of duration of a round, $E[A]$, is

$$E[A] = \begin{cases} RTT \cdot (E[X]+1) & ,when\ a\ packet\ loss \\ RTT \cdot E[X] & ,when\ a\ marked\ ack \end{cases} \quad (24)$$

That is,

$$E[A] = \frac{p}{p+q} RTT \cdot (E[X]+1) + \frac{q}{p+q} RTT \cdot E[X] \quad (25)$$

5.5 Impact of Window Limitation

At the beginning of TCP flow establishment, the receiver advertises a maximum buffer size which determines a maximum congestion window size, W_m. As a consequence, during a period without loss indications, the window size can grow up to W_m, but will not grow further beyond this value. During the first TDMP, the window grows linearly up to W_m for U rounds, then remains constant for V rounds, and then a triple-duplicate or marking indication occurs. The expected U rounds, $E[U]$, is as follows [9]:

$$E[U] = \frac{b}{2} W_m. \quad (26)$$

Since Y_i, the number of packets in the ith TDMP, does not depend on window limitation, $E[Y]$ is given by (16):

$$E[Y] = E[\alpha] + W_m - 1. \quad (27)$$

From [9],

$$E[Y] = \frac{3}{4} W_m E[U] + W_m E[V]. \quad (28)$$

Then,

$$\frac{1-(p+q)}{p+q} + W_m = \frac{3b}{8} W_m^2 + W_m E[V]. \quad (29)$$

Thus,

$$E[V] = \frac{1-(p+q)}{(p+q)W_m} + 1 - \frac{3b}{8} W_m. \quad (30)$$

Finally, since $X_i = U_i + V_i$ in ith TDMP, we have

$$E[X] = E[U] + E[V] = \frac{b}{8} W_m + \frac{1-(p+q)}{(p+q)W_m} + 1. \quad (31)$$

The expected number of packets that have been received in a TDMP, $E[Y']$, is

$$E[Y'] = \begin{cases} E[\alpha] + E[\beta] - 1.0 & \\ & ,when\ a\ packet\ loss \\ E[\alpha] + E[W^{TDM}] - E[\beta] - 1.0 & \\ & ,when\ a\ marked\ ack \end{cases} \quad (32)$$

That is,

$$E[Y'] = \frac{p}{p+q}(E[\alpha] + E[\beta] - 1.0) + \frac{q}{p+q}(E[\alpha] + E[W^{TDM}] - E[\beta] - 1.0) = E[\alpha] + \frac{E[W^{TDM}]}{2} - 1.0. \quad (33)$$

As [9], we obtain $Q(w)$, the probability that a loss in a window size w of congestion-avoidance phase is a TO, is given by

$$Q(w) = \begin{cases} 1 & ,when\ w \leq 3 \\ \sum_{k=0}^{2} A(w,k) + \sum_{k=3}^{w} A(w,k)h(k) & \\ & ,otherwise \end{cases} \quad (34)$$

The expected number of packets received in the time-out phase,

$$E[R] = 1. \quad (35)$$

Thus, the throughput can be formulated as:

$$H = \frac{E[Y'] + \frac{p}{p+q} Q(W^{TDM}) * E[R]}{E[A] + \frac{p}{p+q} Q(W^{TDM}) * E[Z^{TO}]}. \quad (36)$$

From [7], the total expected latency is

$$T_{latency} = E[T_{twhs}] + E[n]RTT + T_{loss} + T_{rest} - \frac{RTT}{2}. \quad (37)$$

Here, the delay caused by the delayed acknowledgment for the first packet is 0ms. That is, the option of delayed acknowledgment is off.

5.6 Verification

We evaluate our proposal Mark-Reverse ECN scheme by the analytical model of Section 5. and by the network simulator ns-2 using the parameters used and given in the Section 4.1. Fig. 11 and Fig. 12 show that the results of this analytical model are very close to simulation results.

6. Conclusion

In this paper, we proposed a new congestoin notification scheme, named as Mark-Reverse ECN for satellite IP networks. Simulation results show that our scheme acheives

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

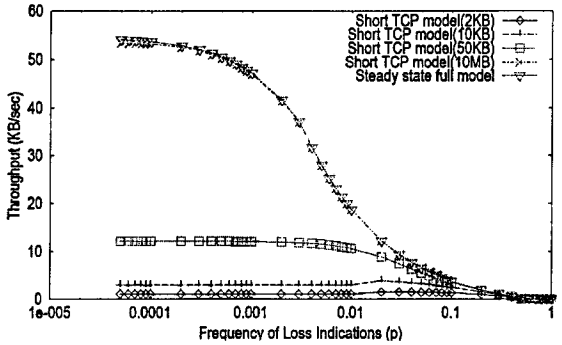


Fig. 9 Throughput predictions given by the short TCP model and the steady state model when drop ratio p is changing and mark ratio is constant $q = 0$. The conditions are: $RTT = 550ms$, $MSS = 1,000bytes$, $T_S = T_0 = 1sec$, $W_m = 30segments$, $b = 1$.

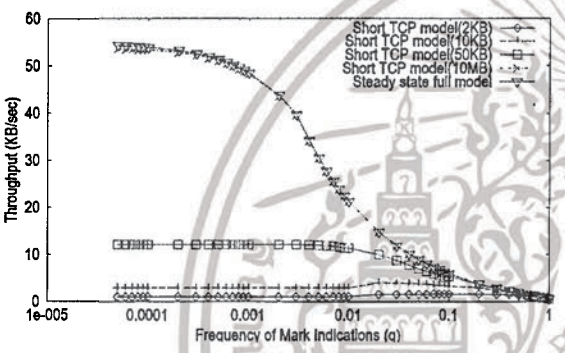


Fig. 10 Throughput predictions given by the short TCP model and the steady state model when drop ratio is constant $p = 0$ and mark ratio is changing. The conditions are: $RTT = 550ms$, $MSS = 1,000bytes$, $T_S = T_0 = 1sec$, $W_m = 30segments$, $b = 1$.

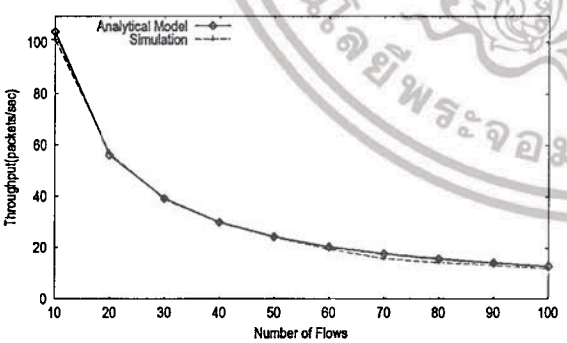


Fig. 11 Throughput comparisons between analytical model and simulation for Mark-Reverse ECN.

higher throughput than the conventional scheme. Analytical results also shows our superiority, correspondingly. A good match between analysis and simulation curves can be observed and validates our results.

REFERENCES

[1] F. Akujobi, I. Lambadaris, R. Makkar, N. Seddigh, and B. Nandy, "BECN for Congestion Control in TCP/IP Neworks: Study and Comparative Evaluation", *IEEE Globecom 2002*, Nov. 2002.

[2] S. Floyd, V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance", *IEEE/ACM Trans. Networking*, vol.1, no.4, August 1993.

[3] RFC 5927, "ICMP Attacks against TCP", July 2010.

[4] S. Floyd, "TCP and Explicit Congestion Notification", Computer Communications Review, vol. 24, no. 5, Oct. 1994.

[5] C. Liu, R. Jain, "Improving Explicit Congestion Notification with the Mark-Front Strategy", Computer Networks (elsevier), vol.35, issue 2-3, Feb. 2001.

[6] UCB/LBNL/VINT Nework Simulatior (NS).

[7] D. Zheng, G. Y. Lazarou, and R. Hu, "A Stochastic Model for Short-lived TCP Flows", IEEE International Conference on Communications 2003 (ICC 2003), May 2003, pp.11-15.

[8] N. Cardwell, S. Savage, and T. Anderson, "Modeling TCP Latency", in Proc. *IEEE INFOCOM 2000*, vol. 3, Mar. 2000, pp.1742-1751.

[9] J. Padhye, V. Firouiu, D. F. Towsley, and J. F. Kurose, "Modeling TCP Reno Performance: A Simple model and its Empirical Validation", *IEEE/ACM Trans. Networking*, vol. 8, no. 2, pp.133-145, Apr. 2000.

[10] D. Zheng, "On the modeling of TCP latency and throughput", Master's thesis Mississippi State University, 2002.

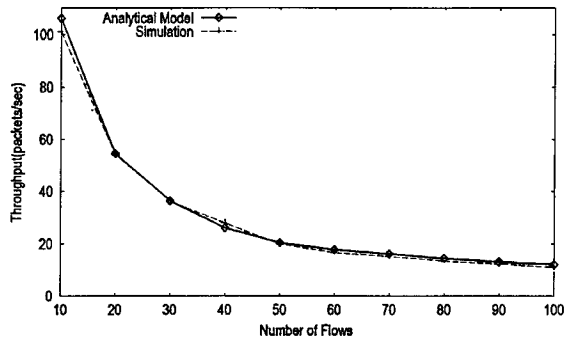


Fig. 12 Throughput comparisons between analytical model and simulation for Mark-Tail ECN.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การปรับปรุงการแบ่งโหลดเพื่อกระจายข้อมูลหลายทางบนเครือข่ายเฉพาะกิจเคลื่อนที่
Multipath Load-balancing Improvement on Mobile Ad-hoc Network

ศุภโชค พงษ์ขวัญ (Supachoke Pongquan) วรวัชร ณรงคะชวนะ (Worrawat Narongkhachavana)
และ สุเมธ ประภาวัต (Sumet Prabhavat)
คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ
aquarix38425@gmail.com, worrawat@gmail.com, sumet@it.kmitl.ac.th

บทคัดย่อ

ความล้มเหลวของการสื่อสารบนเครือข่ายเฉพาะกิจ มักมีสาเหตุมาจากเส้นทางที่ใช้งานอยู่ถูกตัดขาด อันเนื่องมาจากการสูญหายของโมบายล์โหนด เช่น การเคลื่อนที่ของโมบายล์โหนด พลังงานที่จำกัดของโมบายล์โหนด เป็นต้น งานวิจัยนี้จึงพัฒนารูปแบบวิธีการส่งข้อมูลโดยใช้การส่งข้อมูลหลายเส้นทาง และวิธีการเลือกเส้นทางของโปรโตคอลซึ่งส่งผลให้สามารถใช้งานเส้นทางที่ถูกเลือกได้อย่างมีประสิทธิภาพ จากผลการจำลองการส่งข้อมูลระหว่างโมบายล์โหนด แสดงให้เห็นถึงการเพิ่มขึ้นของอัตราสำเร็จในการส่งข้อมูล และเวลาที่ใช้ในการทำงานลดลง

คำสำคัญ: เครือข่ายสื่อสารเฉพาะกิจ การส่งข้อมูลหลายเส้นทาง การกระจายโหลดของเครือข่าย

Abstract

Mobile Ad-hoc network has been popularly focused in recent years. Major problem of Mobile Ad-hoc network is the mobility of mobile nodes which could bring packet delivery failure into the network. This paper aims to develop multipath load-balancing algorithm into multipath routing protocol based on Dynamic Source Routing Protocol (DSR). The algorithm use multiple routes found from route discovery process and utilize that routes by using per-packet allocation scheme. We use extensive simulation to show the result which increase success ratio and reduce overall worktime.

Keyword: Mobile Ad-hoc Network, Dynamic Source Routing Load Balancing, Multipath Routing.

1. บทนำ

เทคโนโลยีการสื่อสารคือหัวใจสำคัญของระบบเครือข่าย ซึ่งมีทั้งระบบเครือข่ายแบบ Infrastructure ที่จำเป็นต้องพึ่งพาอุปกรณ์ที่ทำหน้าที่รับ-ส่ง ข้อมูล โดยหากเกิดเหตุไม่คาดฝันที่ทำให้ระบบ Infrastructure ไม่สามารถทำงานได้ ก็จะทำให้การสื่อสารขัดข้อง เป็นที่มาของระบบเครือข่ายไร้สายเฉพาะกิจ (Ad Hoc Network) ซึ่งเป็นระบบเครือข่ายแบบที่ไม่จำเป็นต้องมีอุปกรณ์ที่ทำหน้าที่รับ-ส่งข้อมูล เป็นตัวกลาง (Infrastructureless) เพื่อที่จะให้การติดต่อสื่อสารเป็นไปได้ในเวลาที่เกิดเหตุขัดข้องจนระบบ Infrastructure ไม่สามารถทำงานได้

Mobile Ad Hoc Network (MANET) [1] เป็นระบบเครือข่ายแบบ Infrastructureless ที่ทำงานด้วยเทคโนโลยีเครือข่ายไร้สาย โดยเทคโนโลยีที่แพร่หลายที่สุดก็คือเทคโนโลยี IEEE 802.11 หรือ Wi-Fi ซึ่งมีอยู่ในสมาร์ทโฟนทั่วไป ดังนั้นการนำเทคโนโลยี Wi-Fi มาใช้สำหรับสร้างเครือข่ายเฉพาะกิจของสมาร์ทโฟนจึงเป็นทางเลือกที่ดีในการทำให้เกิดเครือข่ายสื่อสารในสถานการณ์วิกฤตดังกล่าวได้

แต่ปัญหาของการสร้างเครือข่าย MANET ด้วยเทคโนโลยี Wi-Fi ก็คือ โมบายล์โหนดในเครือข่าย MANET มีโอกาสสูงที่จะขาดการเชื่อมต่อจากกัน เพราะเทคโนโลยี Wi-Fi ไม่เหมาะสมกับการใช้งานกับเครือข่ายที่โมบายล์โหนดมีการเคลื่อนที่ เนื่องจากเทคโนโลยีดังกล่าวมีระยะการเชื่อมต่อค่อนข้างสั้น ทำให้มีโอกาสที่โมบายล์โหนดจะเคลื่อนที่ออกนอกจากระยะการเชื่อมต่อ ส่งผลให้มีโอกาสเกิดการขาดการเชื่อมต่อระหว่างโมบายล์โหนดต้นทางและปลายทาง ซึ่งนำไปสู่ปัญหาความยั่งยืนทนทานของเครือข่าย ดังนั้นการมีการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หาเส้นทางหลายเส้นในเครือข่าย MANET สามารถลดโอกาสเกิดการขาดการเชื่อมต่อระหว่างโมบายล์โหนดต้นทางและปลายทางได้ จึงเป็นทางเลือกที่เป็นไปได้ในการแก้ปัญหาดังกล่าว

ในส่วนที่ 2 จะกล่าวถึงทฤษฎีพื้นฐานที่เกี่ยวข้องและนำมาพัฒนา, ส่วนที่ 3 มีการอธิบายรายละเอียดอัลกอริทึมที่นำมาใช้พัฒนาระบบเครือข่าย, ส่วนที่ 4 เป็นการประเมินผลการทดลองของอัลกอริทึมที่พัฒนาขึ้นมา โดยเปรียบเทียบกับโปรโตคอลหลักที่นำมาพัฒนา และส่วนที่ 5 เป็นการสรุปผลการทดลองของงานวิจัยนี้

2. วิจารณ์วรรณกรรม

2.1 Mobile Ad-hoc Network

ระบบเครือข่ายเฉพาะกิจไร้สาย (MANET) เป็นระบบที่ถูกออกแบบมาเพื่อรองรับการเชื่อมต่อระหว่างโมบายล์โหนดโดยไม่จำเป็นต้องพึ่งพาอุปกรณ์เชื่อมต่อพื้นฐาน เช่น แอคเซสพอยท์ สวิทช์ หรือ เราท์เตอร์ โดยตัวอุปกรณ์ (End-device) สามารถสร้างเครือข่ายขึ้นมาได้เอง และทำการติดต่อกันระหว่างโมบายล์โหนดด้วยกันเอง เพื่อให้ข้อมูลส่งไปถึงปลายทาง โดยที่จุดเด่นของ MANET คือ สามารถจัดการกับอุปกรณ์ต่างๆ ที่มีการเคลื่อนที่อยู่ได้อย่างอิสระ (Node Mobility)

โปรโตคอลการค้นหาเส้นทางของระบบเครือข่ายเฉพาะกิจไร้สาย หากจัดแบ่งตามลักษณะการทำงานของโปรโตคอล [2], [3] จะแบ่งเป็น 2 กลุ่ม ได้แก่ 1) โปรโตคอลค้นหาเส้นทางแบบโปรแอคทีฟ ซึ่งในโปรโตคอลประเภทนี้โมบายล์โหนดทุกๆ ตัวในเครือข่ายจะมีตารางข้อมูลของโมบายล์โหนดต่างๆ (Routing Information) ภายในระบบ และมีการอัพเดทข้อมูลนั้นทุกๆ ช่วงเวลาที่กำหนด 2) โปรโตคอลค้นหาเส้นทางแบบรีแอคทีฟ จะไม่มีการกำหนดเวลาในการอัพเดทข้อมูลภายในช่วงเวลาที่กำหนด แต่จะทำการหาเส้นทางของทั้งระบบเฉพาะเวลาที่จะมีการส่งข้อมูลระหว่างโมบายล์โหนดตั้งแต่ต้นทางจนถึงปลายทาง

2.2 Dynamic Source Routing Protocol (DSR)

DSR [4] เป็นโปรโตคอลในการหาเส้นทางการส่งข้อมูลแบบรีแอคทีฟ โดยเมื่อโมบายล์โหนดต้องการที่จะส่งข้อมูลโมบายล์โหนดต้นทางจะมีการบรอดแคสท์แพ็คเก็ตชนิดพิเศษที่เพิ่ม DSR Header เข้าไปในแพ็คเก็ตแบบปกติ เพื่อทำการเก็บข้อมูลของโมบายล์โหนดต่างๆ ภายในเครือข่าย ซึ่งตัวแพ็คเก็ตที่มี DSR Header จะเก็บข้อมูลไอพีแอดเดรส ของโมบายล์โหนดที่ส่งผ่านเข้าไปในส่วนหัวของแพ็คเก็ต และเมื่อพบโมบายล์โหนดปลายทางแล้วก็จะส่งข้อความตอบกลับมายังต้นทาง จากนั้นก็จะเริ่มทำการสร้างเส้นทางเพื่อทำการส่งแพ็คเก็ตปกติตามเส้นทางที่ได้ทำการบันทึกไว้

โปรโตคอล DSR มีกลไกการทำงานหลักสองกลไก คือ 1) กลไกการค้นหาเส้นทาง (Route Discovery) จะเริ่มต้นทำงานเมื่อโมบายล์โหนดต้องการส่งแพ็คเก็ตไปยังปลายทางแต่ไม่มีข้อมูลเส้นทางที่จะทำการส่งแพ็คเก็ตนั้นๆ ไปยังปลายทาง จึงเริ่มทำการค้นหาเส้นทาง โดยโหนดต้นทางจะทำการบรอดแคสต์แพ็คเก็ตร้องขอเส้นทาง (Route Request: RREQ) ออกไป โดยมีหมายเลข RREQ ID กำหนดไว้และเมื่อโมบายล์โหนดภายในเครือข่ายได้รับก็จะทำการตรวจสอบแพ็คเก็ตว่ามีปลายทางเป็นของตนหรือไม่ หากไม่ใช่ก็จะทำการบรอดแคสต์แพ็คเก็ตนั้นต่อออกไป และหากมีปลายทางเป็นตนเองก็จะทำการส่งแพ็คเก็ตตอบรับ (Route Reply: RREP) กลับมายังโหนดต้นทาง 2) กลไกการปรับปรุงเส้นทาง (Route Maintenance) จะถูกเรียกใช้เมื่อโมบายล์โหนดภายในเครือข่ายทำการส่งข้อมูลอยู่และเส้นทางที่ถูกใช้มีโมบายล์โหนดขาดหายออกไปจากเส้นทาง ทำให้การส่งข้อมูลหยุดชะงักลง โมบายล์โหนดระหว่างทางที่เชื่อมต่อกับโหนดที่หายไปจะทำการส่งแพ็คเกตแจ้งกลับมายังต้นทาง (Route Error: RERR) ว่าเส้นทางที่ใช้อยู่ได้ขาดลงไป และโมบายล์โหนดต้นทางก็จะทำการเรียกใช้เส้นทางอื่นๆ ที่อยู่ภายในแคชของตน หรืออาจเรียกกลไก Route Discovery เพื่อทำการหาเส้นทางใหม่

2.3 Multiple Source Routing Protocol (MSR)

โปรโตคอล MSR [5] พัฒนาขึ้นโดยใช้หลักการของ Dynamic Source Routing Protocol และนำหลักการของการส่งแบบหลายเส้นทางมาประยุกต์ใช้ได้ง่าย เนื่องจากในการทำงานปกติของ DSR เป็นแบบ Source Routing ซึ่งมีกลไกในการหา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เส้นทางก่อนส่งข้อมูลและมีการเก็บข้อมูลเส้นทางที่หามาได้ไว้กับโมบายล์โหนดที่ทำการส่งข้อมูล ทำให้การประมวลผลการส่งแบบหลายเส้นทางมีความเป็นไปได้ที่จะนำมาใช้กับโปรโตคอล DSR

กลไกการค้นหาเส้นทางในโปรโตคอล MSR มีการทำงานเหมือนในโปรโตคอล DSR แต่จะมีการนำข้อมูลเส้นทางที่ได้รับกลับมาจากโหนดปลายทางมาเก็บไว้ในแคชของตน และนำข้อมูลเส้นทางต่างๆ ที่ได้รับออกมาใช้ในการส่งแพ็คเก็ตโดยใช้รูปแบบการส่งแพ็คเก็ตแบบ Round Robin [6] ซึ่งจะมีการวนใช้งานแต่ละเส้นทางไปเรื่อยๆ

3. ขั้นตอนการดำเนินงานวิจัย

จากการศึกษาทบทวนวรรณกรรมในส่วนที่ 2 เกี่ยวกับเครือข่ายเฉพาะกิจเคลื่อนที่, โปรโตคอล DSR และโปรโตคอล MSR ผู้วิจัยได้เล็งเห็นว่าโปรโตคอล DSR ที่มีการใช้เส้นทางเพียงเส้นทางเดียวที่ได้รับจากกระบวนการ Route Discovery นั้นมีโอกาสทำให้เกิดปัญหา Single-point-of-failure ซึ่งมีผลต่อความน่าเชื่อถือของโปรโตคอล โดยชี้วัดได้จากอัตราสำเร็จในการส่งแพ็คเก็ต นอกจากนี้การเลือกใช้เส้นทางเพียงเส้นทางเดียว ยังมีโอกาสทำให้เกิดความกับคั่งภายในเส้นทางนั้น ในขณะที่ยังมีเส้นทางอื่นที่ได้รับมาสามารถใช้ในการส่งข้อมูลได้อีก ส่งผลให้ใช้เวลานานในการส่งข้อมูลสำเร็จ

ผู้วิจัยจึงทำการนำเสนอแนวคิดการพัฒนาโปรโตคอล MSR ที่มีอยู่เดิมโดยจะปรับปรุงรูปแบบการส่งแพ็คเก็ตเดิมที่ใช้แบบ Round Robin ผู้วิจัยนำเสนอรูปแบบการส่งแพ็คเก็ตแบบ Weight-Round Robin (WRR) แทนการใช้รูปแบบการส่งแบบเดิม เนื่องจากในการส่งแพ็คเก็ตแบบ Round Robin นั้นมีการกระจายโหลดของเส้นทางเท่าๆ กัน จึงมีโอกาสที่เส้นทางที่มีดีเลย์สูงจะถูกเรียกใช้งานเท่ากับเส้นทางที่มีดีเลย์ต่ำ ซึ่งค่าดีเลย์วัดได้จากกการจับเวลาตั้งแต่ส่งแพ็คเก็ต Route Request ออกไปและได้รับ Route Reply กลับมาผ่านเส้นทางนั้นๆ

ผู้วิจัยได้ทำการนำค่าบิทเรทจากดาต้าลิงค์เลเยอร์ ขึ้นมาเป็นตัวแปรในการกำหนดน้ำหนักให้กับเส้นทางบนเน็ตเวิร์คเลเยอร์ ทั้งนี้ ผู้วิจัยคาดว่าค่าบิทเรทดังกล่าวสามารถประเมินคุณภาพของเส้นทางได้โดยประมาณ และมีการใช้จำนวนฮอปของเส้นทางเป็นตัวกำหนดน้ำหนักรองในกรณีที่ค่าบิทเรทของเส้นทางเท่ากันดังที่แสดงให้เห็นจากโค้ดเทียมในภาพที่ 1

```
1  struct route
2  {
3      path
4      bitrate
5      num_hop
6  };
7  new vector srt_vector
8  new vector weight_vector
9  if (srt_vector.size() = 0)
10 {
11     srt_vector.pushback(route);
12 }
13 else
14 {
15     for(int i=0; i<srt_vector.size();i++)
16     {
17         if (srt_vector.at(i).bitrate < route.getBitrate()
18             OR srt_vector.at(i).num_hop < route.num_hop)
19         {
20             srt_vector.insert(srt_vector.at(i-1), route);
21             weight_vector.insert(weight_vector.at(i-1), i);
22         }
23     if(n==srt_vector.size())
24     {
25         srt_vector.pushback(route);
26         weight_vector.pushback(srt_vector.size());
27     }
28 }
29 return srt_vector;
```

ภาพที่ 1: แสดงโค้ดเทียมของกระบวนการหาเส้นทาง

การกำหนดค่าตัวแปรต่างๆ ดังนี้

route = โครงสร้างของเส้นทาง ประกอบไปด้วย

- *path* = เส้นทาง
- *bitrate* = บิทเรทของดาต้าลิงค์เลเยอร์
- *num_hop* = จำนวนฮอป

srt_vector = เวกเตอร์ที่เก็บเส้นทางต่างๆ ไว้

weight_vector = เวกเตอร์ที่เก็บน้ำหนักของเส้นทาง

n = ขนาดของเวกเตอร์

การทำงานของโค้ดข้างต้นจะเริ่มทำงานเมื่อเริ่มกระบวนการค้นหาเส้นทางโดย กำหนดค่าจำนวนเต็ม *n* ให้เท่ากับขนาดของเวกเตอร์เส้นทาง เมื่อเริ่มต้นค้นหาเส้นทางหากพบเส้นทางที่ใช้ได้ก็จะทำการเพิ่ม *route* เข้าไปในเวกเตอร์ และหากพบเส้นทางต่อมาก็จะทำการเปรียบเทียบค่าบิทเรท (*bitrate*) และจำนวนฮอป (*num_hop*) ของเส้นทางภายในเวกเตอร์ โดยจะกำหนดให้เส้นทางที่มีค่าบิทเรทสูงกว่าอยู่ด้านหน้าของเวกเตอร์ และหากมีค่าบิทเรทเท่ากันก็จะทำการเปรียบเทียบจำนวนฮอป โดยให้เส้นทางที่ใช้จำนวนฮอปน้อยกว่าอยู่ด้านหน้า พร้อมกับเพิ่มน้ำหนักให้กับเส้นทางเข้าไปยัง *weight_vector* ที่ตำแหน่งเดียวกับเส้นทางนั้นๆ เมื่อทำงานเสร็จสิ้นก็จะทำการส่งค่า *srt_vector* ที่เก็บเส้นทางต่างๆ ออกไปใช้งานต่อ

ในงานวิจัยนี้ ผู้วิจัยทำการคำนวณน้ำหนักของเส้นทางโดยกำหนดน้ำหนักสูงสุดตามจำนวนเส้นทางที่สามารถใช้ได้ ลดลง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มาจนถึงเส้นทางที่มีน้ำหนักต่ำสุดคือ 1 และมีการกระจายโหลดโดยใช้การกระจายตามแต่ละแพ็คเก็ต โดยจะส่งแพ็คเก็ตออกไปยังเส้นทางที่มีน้ำหนักสูงสุดเป็นจำนวนตามค่าน้ำหนักของเส้นทางนั้นๆ จากนั้นจึงส่งแพ็คเก็ตออกไปยังเส้นทางถัดไปตามค่าน้ำหนักของเส้นทางเช่นกัน

ผู้วิจัยเล็งเห็นว่าการส่งแพ็คเก็ตแบบ WRR สามารถแก้ปัญหาดังกล่าวได้โดยใช้ค่าดีเลย์ของเส้นทางเป็นตัวกำหนดอัตราการถ่วงน้ำหนักของการส่งแพ็คเก็ตทำให้สามารถแบ่งโหลดของการส่งแพ็คเก็ตไปยังเส้นทางที่มีดีเลย์น้อยกว่าได้ดี ทั้งนี้เพื่อลดเวลาการทำงานโดยรวมของระบบตั้งแต่เริ่มส่งแพ็คเก็ตจนกระทั่งส่งแพ็คเก็ตทั้งหมดสำเร็จโดยจะมีการนำเสนอผลของการทดลองในส่วนถัดไป

4. ผลการทดลอง

จากการนำเสนอการปรับปรุงโปรโตคอลในส่วนที่ 3 ผู้วิจัยได้ทำการทดลองโดยใช้โปรแกรมจำลองระบบเครือข่าย และนำผลการจำลองเครือข่ายมาเปรียบเทียบกับอัลกอริทึม DSR และ MSR โดยมีข้อกำหนดควบคุม และผลการทดลองดังนี้

4.1 การควบคุมข้อกำหนดระบบเครือข่ายของแต่ละโปรโตคอล

การทดลองมีการกำหนดการควบคุมโดยมีการกำหนดให้โมบายล์โหนดมีการเคลื่อนที่อยู่เสมอด้วยความเร็วคงที่ โดยที่ความเร็วของแต่ละโหนดมีการสุ่มแบบยูนิฟอร์ม มีกระจายตัวของโหนดแบบสุ่มภายในพื้นที่กว้าง 1500 เมตร ยาว 1000 เมตร กำหนดให้โหนดต้นทางส่งข้อมูลไปยังโหนดปลายทางด้วยโปรโตคอล UDP และให้ระบบหยุดทำงานเมื่อโหนดปลายทางได้รับข้อมูลจำนวน 1000 แพ็คเก็ต โดยมีการแสดงข้อมูลจำเพาะอื่นๆ ภายในตารางที่1 ต่อจากนี้

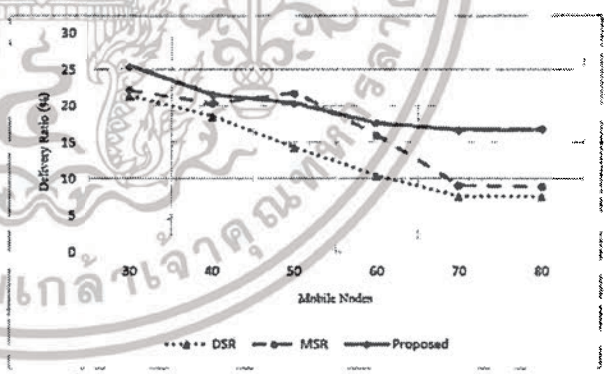
ตารางที่ 1: แสดงข้อมูลจำเพาะของการจำลองการทำงาน

พื้นที่จำลอง	1500 เมตร × 1000 เมตร
รัศมีการทำงานของโหนด	250 เมตร
จำนวนแพ็คเก็ตที่ปลายทางได้รับ	1000 แพ็คเก็ต
จำนวนโหนดในเครือข่าย	30, 40, 50, 60, 70, 80
อัตราการส่งแพ็คเก็ต	4 แพ็คเก็ต/วินาที
โปรโตคอลที่ใช้ส่งข้อมูล	UDP
ความเร็วในการเคลื่อนที่เฉลี่ย	2.5, 5, 7.5, 10 เมตร/วินาที
จำนวนรอบที่ใช้ในการทดลอง (ต่อหนึ่งรูปแบบจำลอง)	40 รอบ

4.2 ตัวชี้วัดและผลการทดลอง

จากการควบคุมข้อกำหนดต่างๆ ในส่วนที่ 4.1 และทำการทดลองจำลองการทำงานของอัลกอริทึมการค้นหาเส้นทางของโปรโตคอล DSR โปรโตคอล MSR และอัลกอริทึมที่ผู้วิจัยนำเสนอ ผู้วิจัยได้เสนอผลการจำลองระบบออกมาในรูปแบบกราฟโดยมีตัวชี้วัดต่างๆ ที่ใช้ในการเปรียบเทียบผลการทำงานคือ ผลสำเร็จของการส่งแพ็คเก็ต และเวลาการทำงานตั้งแต่เริ่มส่งแพ็ตเก็ตจนโมบายล์โหนดปลายทางได้รับแพ็คเก็ตเป็นจำนวน 1,000 แพ็ตเก็ต

การทดลองควบคุมการทำงานโดยกำหนดความเร็วในการเคลื่อนที่เฉลี่ยเป็น 7.5 และ 10 เมตร/วินาที พบว่าอัตราสำเร็จในการส่งแพ็ตเก็ตของระบบที่มีจำนวนโมบายล์โหนดที่เพิ่มขึ้นจะส่งผลให้อัตราสำเร็จในการส่งแพ็ตเก็ตลดลง โดยในอัลกอริทึมของ MSR และอัลกอริทึมที่ผู้วิจัยนำเสนอ สามารถทำงานได้ดีกว่าอัลกอริทึมการค้นหาเส้นทางของ DSR ตามภาพที่ 1 และภาพที่ 2 ซึ่งจะเห็นได้ว่าเมื่อมีจำนวนโมบายล์โหนดเยอะ อัลกอริทึมที่นักวิจัยได้นำเสนอจะสามารถทำงานได้ดีกว่าอัลกอริทึม MSR และ DSR ที่ยังมีค่าใกล้เคียงกัน ทั้งนี้เนื่องจากกลไกการกระจายโหลดที่ทำให้สามารถใช้งานเส้นทางที่มีอยู่ได้อย่างมีประสิทธิภาพ

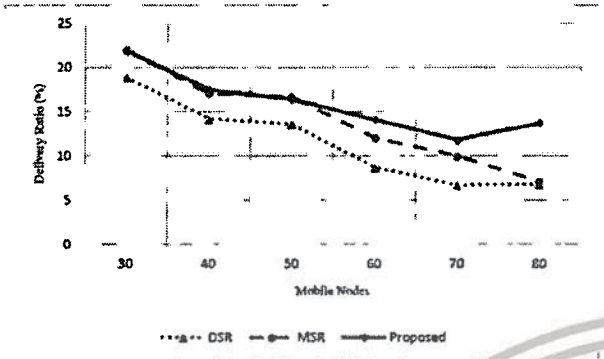


ภาพที่ 1: แสดงผลการทดลองอัตราสำเร็จต่อจำนวนโมบายล์โหนดที่ความเร็ว 7.5 เมตร/วินาที

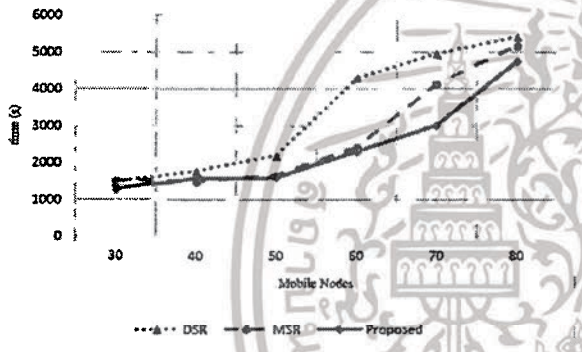
ในการทดลองเพื่อหาเวลาการทำงานด้วยการกำหนดความเร็วในการเคลื่อนที่เฉลี่ยเป็น 7.5 และ 10 เมตร/วินาที ตามภาพที่ 3 และภาพที่ 4 แสดงให้เห็นว่าที่จำนวนโหนดตั้งแต่ 30 – 50 โหนด แต่ละอัลกอริทึมจะใช้เวลาในการทำงานใกล้เคียงกัน แต่เมื่อจำนวนโหนดเพิ่มขึ้น อัลกอริทึมที่นักวิจัยนำเสนอมาสามารถทำงานได้ดีกว่าโปรโตคอล MSR และ DSR อย่างเห็นได้ชัด ทั้งนี้เพราะว่ามีการกำหนดน้ำหนักให้กับเส้นทาง ทำให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

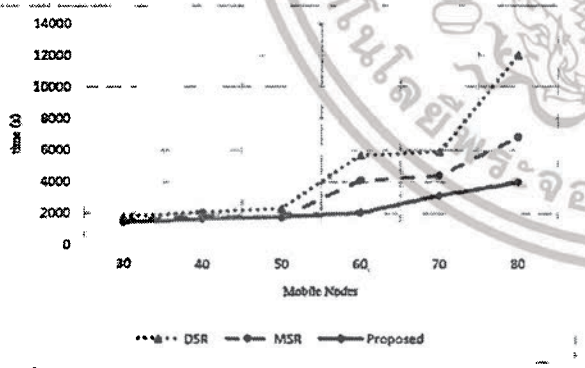
สามารถกระจายโหลดออกไปยังเส้นทางที่มีบิทเรทสูงกว่า สามารถระบายการไหลของแพ็คเก็ตได้และไม่เกิดความคับคั่งภายในเส้นทางที่มีบิทเรทต่ำ



ภาพที่ 2: แสดงผลการทดลองอัตราสำเร็จต่อจำนวนโมบายล์โหนดที่ความเร็ว 10 เมตร/วินาที

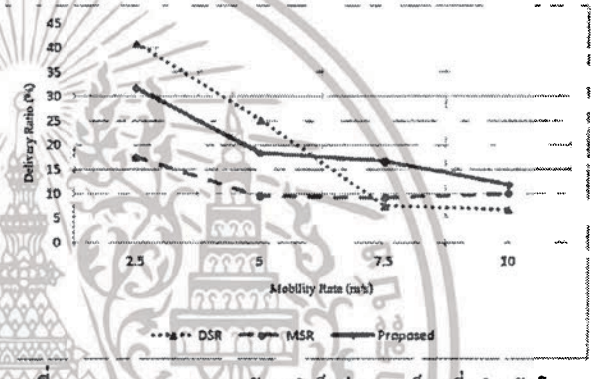


ภาพที่ 3: แสดงผลการทดลองเวลาการทำงานต่อจำนวนโมบายล์โหนดที่ความเร็ว 7.5 เมตร/วินาที

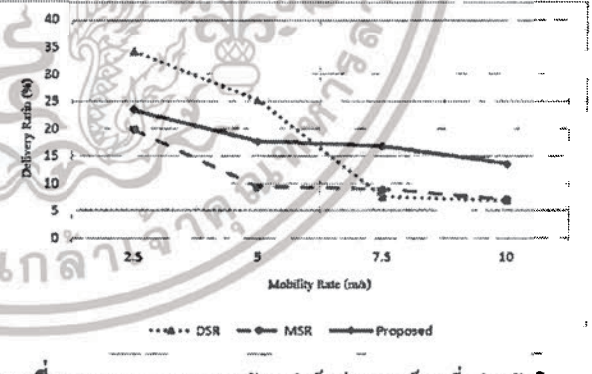


ภาพที่ 4: แสดงผลการทดลองเวลาการทำงานต่อจำนวนโมบายล์โหนดที่ความเร็ว 10 เมตร/วินาที

ภาพที่ 5 และภาพที่ 6 แสดงการเปรียบเทียบการทำงานที่มีจำนวนโมบายล์โหนดภายในเครือข่ายสูง เช่น 70 และ 80 โหนด ระหว่างความเร็วเฉลี่ยในการเคลื่อนที่ของโมบายล์โหนด ต่ออัตราสำเร็จในการส่งแพ็ตเก็ตของโหนด จะเห็นได้ว่าเมื่อโหนดมีการเคลื่อนที่ด้วยความเร็วต่ำ ประสิทธิภาพการทำงานของอัลกอริทึม DSR จะทำงานได้ดีกว่าอัลกอริทึม MSR และอัลกอริทึมที่นักวิจัยนำเสนอ แต่เมื่อโมบายล์โหนดเคลื่อนที่ด้วยความเร็วสูงขึ้น อัตราสำเร็จในการส่งแพ็คเก็ตของ DSR จะลดลงอย่างมาก ในขณะที่อัลกอริทึมของผู้วิจัยมีการลดลงค่อนข้างน้อย ทำให้สามารถทำงานได้ดีกว่าอัลกอริทึม DSR และ MSR ที่ความเร็ว 7.5 และ 10 เมตร/วินาที ทั้งนี้เป็นผลมาจากการเคลื่อนที่ของโมบายล์ด้วยความเร็วสูง ทำให้มีโอกาสสูงที่เส้นทางแพ็คเก็ตจะถูกตัดขาด ทำให้การแพ็คเก็ตในเครือข่ายที่ใช้อัลกอริทึม DSR หยุดชะงักลง ในขณะที่ MSR และอัลกอริทึมที่นำเสนอยังสามารถส่งแพ็คเก็ตได้อยู่เนื่องจากมีการใช้เส้นทางการส่งแพ็คเก็ตหลายเส้นทาง



ภาพที่ 5: แสดงผลการทดลองอัตราสำเร็จต่อความเร็วเฉลี่ยสำหรับโหนดจำนวน 70 โหนด

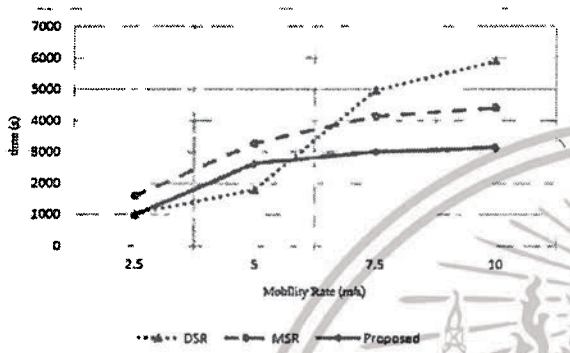


ภาพที่ 6: แสดงผลการทดลองอัตราสำเร็จต่อความเร็วเฉลี่ยสำหรับโหนดจำนวน 80 โหนด

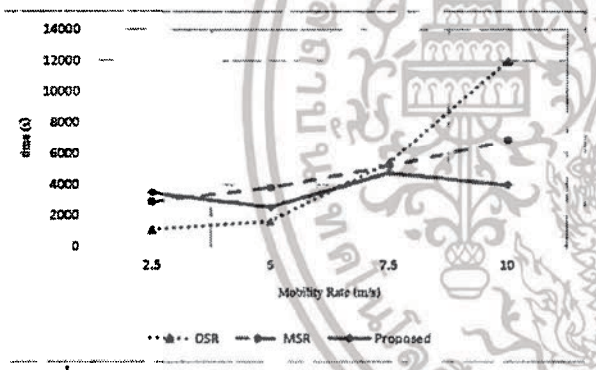
ภาพที่ 7 และภาพที่ 8 เป็นการเปรียบเทียบเวลาการทำงานต่อความเร็วในการเคลื่อนที่ของโมบายล์โหนด ของเครือข่ายที่มีโมบายล์โหนดจำนวน 70 และ 80 โหนดตามลำดับ อัลกอริทึมของ DSR สามารถทำงานได้ดีกว่าในความเร็ว 2.5 และ 5 เมตร/วินาที แต่เมื่อความเร็วเพิ่มขึ้นเป็น 7.5 และ 10 เมตร/วินาที อัลกอริทึม DSR จะใช้เวลาทำงานเพิ่มขึ้นอย่างมาก ส่วนอัลกอริทึม MSR และอัลกอริทึมที่นำเสนอมีการใช้เวลา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพิ่มขึ้นน้อยกว่าอัลกอริทึม DSR เป็นผลมาจากการที่เส้นทางที่ส่งแพ็คเก็ตอยู่ถูกตัดขาด ทำให้อัลกอริทึม DSR ที่ทำงานโดยการส่งแพ็คเก็ตเส้นทางเดียว ต้องเริ่มกระบวนการค้นหาเส้นทางใหม่ จึงใช้เวลาเพิ่มขึ้นเป็นอย่างมาก ในขณะที่อัลกอริทึม MSR และอัลกอริทึมที่นำเสนอยังมีเส้นทางอื่นๆ ที่สามารถใช้ได้มารองรับการส่งแพ็คเก็ตไปยังโมบายล์โหนดปลายทาง



ภาพที่ 7: แสดงผลการทดลองเวลาการทำงานต่อความเร็วเฉลี่ยของโมบายล์โหนดจำนวน 70 โหนด



ภาพที่ 8: แสดงผลการทดลองเวลาการทำงานต่อความเร็วเฉลี่ยของโมบายล์โหนดจำนวน 80 โหนด

5. สรุปผลการทำงานของระบบ

นักวิจัยได้นำเสนอการพัฒนาอัลกอริทึมในการค้นหาเส้นทางของเครือข่ายเฉพาะกิจเคลื่อนที่ โดยมีโปรโตคอล DSR เป็นหลัก และนำโปรโตคอล MSR ที่พัฒนาต่อมาจาก DSR มาเป็นพื้นฐานในการพัฒนาอัลกอริทึม ซึ่งได้ทำการเพิ่มอัลกอริทึมการค้นหาเส้นทางโดยใช้ค่าบิทเรทจากดาต้าลิงค์เลเยอร์ และจำนวนฮอปของเส้นทางมาเป็นตัวกำหนดน้ำหนักให้กับเส้นทาง

จากผลการทดลองในส่วนที่ 4 สามารถบอกได้ว่าอัลกอริทึมที่นักวิจัยนำเสนอนั้น สามารถทำงานได้ดีกว่าอัลกอริทึม DSR และ MSR ในสถานการณ์ที่มีจำนวนโมบายล์โหนดสูง หรือมีการเคลื่อนที่ด้วยความเร็วมาก เป็นผลมาจากการเพิ่มอัลกอริทึมค้นหาเส้นทางให้มีการกำหนดน้ำหนักให้กับเส้นทาง ทำให้ไม่เกิดความคับคั่งในเส้นทางใดเส้นทางหนึ่ง และสามารถดึงประสิทธิภาพของโมบายล์โหนดออกมาใช้งานได้อย่างเต็มที่

เอกสารอ้างอิง

[1] T. S. Rappaport. **"Wireless Communications Principles & Practice."** Upper Saddle River, New Jersey: Prentice-Hall, Inc.1996

[2] T. Lin. **"Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications."** Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the Ph.D. in Computer Engineering. 2004

[3] K.Gorantala. **"Routing Protocols in Mobile Ad-hoc Networks"** Master's Thesis in Computing Science at Ume°a University. June 15, 2006

[4] D. B. Johnson and D. A. Maltz, **"Dynamic Source Routing in Ad Hoc Wireless Networks."** Computer Science Department, Carnegie Mellon University. 1996

[5] L. Wang, Y. Shu, M. Dong and L. Zhang, **"Adaptive Multipath Source Routing in Ad Hoc Networks."** Department of Computer Science, Tianjin University, Tianjin, China

[6] S. Prabhavat, H. Nishiyama, N. Ansari and N. Kato **"On Load Distribution over Multipath Networks."** *IEEE Communications Survey & Tutorials*, vol. 14, no. 3, pp. 662-680, 2012.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กลไกค้นหาเกตเวย์ที่มีโอเวอร์เฮดจากการแลกเปลี่ยนข้อความต่ำ สำหรับเครือข่ายเคลื่อนที่เฉพาะกิจ

Gateway Discovery Mechanism with Low Message Exchange Overhead for Mobile Ad Hoc Networks

สุเมธ ประภาวัต(Sumet Prabhavat) สารัช ศรีสวัสดิ์พงษ์ (Sarach Sriswadpong)

ทะนง ชูวณิชชานนท์ (Tanong Chuvanitchanon) วรวัชร ฉรงคะชวนะ(Worrawat Narongkhachavana)

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

sumet@it.kmitl.ac.th, acecharmil@gmail.com, tanong3200@hotmail.com, worravat@gmail.com

บทคัดย่อ

ในการค้นหาเกตเวย์เพื่อให้เครือข่ายเคลื่อนที่เฉพาะกิจติดต่อกับเครือข่ายภายนอกหรืออินเตอร์เน็ตได้ โอเวอร์เฮดที่เกิดจากการแลกเปลี่ยนข้อมูลระหว่างโหนดเพื่อการค้นหาเกตเวย์ และเวลาที่ต้องใช้ในการค้นหาเป็นปัจจัยที่ลดทอนประสิทธิภาพเครือข่ายอย่างหลีกเลี่ยงไม่ได้ ในงานวิจัยก่อนหน้านี้พยายามแก้ไขปัญหาดังกล่าว เช่น กลไกในโพรโทคอล AODV ที่ใช้เวลาในการค้นหาเกตเวย์น้อย แต่ก็ทำให้เกิดโอเวอร์เฮดมาก เมื่อเทียบกับกลไกในโพรโทคอล OLSR ที่มีโอเวอร์เฮดต่ำ แต่ก็ใช้เวลาในการค้นหานาน บทความนี้จึงเสนอกลไกที่สามารถค้นหาเกตเวย์ได้โดยมีโอเวอร์เฮดต่ำ และใช้เวลาในการค้นหาน้อย ซึ่งพิสูจน์ได้โดยการจำลองการทำงานและเปรียบเทียบกับกลไกค้นหาเกตเวย์จากงานวิจัยก่อนหน้าในสภาวะที่โหนดเคลื่อนที่แบบสุ่ม และมีพารามิเตอร์การจำลองที่แตกต่างกันออกไป

คำสำคัญ: เครือข่ายเคลื่อนที่เฉพาะกิจ การค้นหาเกตเวย์ โอเวอร์เฮด การแลกเปลี่ยนข้อมูลเพื่อหาเกตเวย์

Abstract

A gateway discovery mechanism on mobile ad hoc network (MANET) is applicable for connecting MANET to other networks or the Internet. However, it causes message exchange overhead and gateway discovery time (leading to network delay), which degrade network performance significantly. These issues have been addressed by previous works: A gateway discovery mechanism in a modified AODV takes short time to find a gateway but causes high overhead whereas that in a modified version of OLSR needs only a few number of message exchanges but requires long discovery time. This paper proposes an improved gateway discovery mechanism that can reduce message exchange overhead while maintains low gateway discovery time. Performance evaluations are conducted using simulations with different parameters and random waypoint mobility model.

Keyword: Mobile Ad Hoc Network, Gateway Discovery, Message Exchange Overhead

1. บทนำ

จากเทคโนโลยีด้านการสื่อสารที่มีการพัฒนาไปอย่างรวดเร็วอันส่งผลให้เกิดนวัตกรรมใหม่ ๆ เกิดขึ้น เช่น การสื่อสารแบบไร้สาย และมีการใช้งานกันอย่างแพร่หลายซึ่งการสื่อสารกลายเป็นสิ่งสำคัญในการดำเนินชีวิตของมนุษย์ไปแล้ว ทั้งนี้เองหากเกิดสถานการณ์ที่เกิดภัยพิบัติหรือเหตุการณ์ไม่คาดฝันซึ่งทำให้การติดต่อสื่อสารระหว่างโมบายล์โหนดกับโครงสร้างพื้นฐานถูกตัดขาด ส่งผลให้ไม่สามารถติดต่อสื่อสารและขอความช่วยเหลือจากบุคคลอื่น ๆ ได้ จากปัญหาดังกล่าวจึงมีนักวิจัยหลายกลุ่มพยายามพัฒนาเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด (MANET : Mobile Ad-hoc Network) [1] ซึ่งทำให้โมบายล์โหนดสามารถติดต่อสื่อสารกันได้โดยไม่ต้องพึ่งพาโครงสร้างพื้นฐาน

แต่การเชื่อมต่อกันเพียงในเครือข่ายเฉพาะกิจดังกล่าวทำให้เกิดปัญหาการจำกัดทางด้านขอบเขตของเครือข่าย และจากที่กล่าวมาการที่โมบายล์โหนดทำหน้าที่เป็นผู้ส่งต่อข้อมูลให้โหนดอื่น ๆ นั้นทำให้มีการใช้พลังงานสำหรับทำหน้าที่ดังกล่าวนอกเหนือจากเพื่อการส่งข้อมูลของตนเอง อันส่งผลให้เกิด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ปัญหาในการใช้พลังงานที่มีอยู่อย่างจำกัด (จากแบตเตอรี่) ของโมบายล์โหนด

จากปัญหาที่กล่าวมาผู้จัดทำจึงศึกษารูปแบบการหาเส้นทางให้สามารถหาเส้นทางเชื่อมต่อที่ผ่านเกตเวย์ออกไปยังโครงสร้างพื้นฐานได้บนเครือข่ายเฉพาะกิจของโมบายล์โหนด (อย่างเช่น เครือข่ายอินเตอร์เน็ต) เพื่อแก้ไขปัญหาด้านการจำกัดขอบเขตเครือข่าย ซึ่งทำให้ติดต่อสื่อสารออกไปนอกพื้นที่ได้ และลดการใช้พลังงานที่มีอยู่อย่างจำกัดของโมบายล์โหนดให้ทำงานได้นานขึ้น ไปจนกระทั่งลดโอกาสเกิดความไม่ต่อเนื่องในเครือข่าย

2. ทฤษฎีและงานที่เกี่ยวข้อง

โพรโทคอลค้นหาเส้นทาง (Routing Protocols) ในเครือข่ายสื่อสารเฉพาะกิจถูกแบ่งเป็น 3 กลุ่ม [2] คือ 1) โพรโทคอลค้นหาเส้นทางแบบรีแอกทีฟ (Reactive Routing Protocols) ซึ่งค้นหาเส้นทางเมื่อต้องการส่งข้อมูล เช่น โพรโทคอลเอโอดีวี (AODV : Ad hoc On-Demand Distance Vector) [4] และโพรโทคอลดีเอสอาร์ (DSR : Dynamic Sort Routing) [3] 2) โพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ (Proactive Routing Protocols) ทำการค้นหาเส้นทางไปยังทุกปลายทางที่เป็นไปได้ก่อนที่จะมีการส่งข้อมูล เช่น โพรโทคอลโอแอลเอสอาร์ (OLSR : Optimized Link State Routing) [5] และสุดท้าย 3) โพรโทคอลค้นหาเส้นทางแบบไฮบริดจ์ (Hybrid Routing Protocols) ซึ่งมีการทำงานผสมผสานระหว่างโพรโทคอลค้นหาเส้นทางทั้ง 2 แบบก่อนหน้า

โดยมีงานวิจัยที่ได้ศึกษาการเชื่อมต่อระหว่างเครือข่ายเฉพาะกิจของโมบายล์โหนดกับเครือข่ายอื่น ๆ เช่น เครือข่ายโทรศัพท์ (Cellular Network) [10] เครือข่ายอินเทอร์เน็ต [6],[7],[8] โดยใช้การค้นหาโหนดเกตเวย์ในการเชื่อมต่อระหว่างเครือข่ายสื่อสารเฉพาะกิจและเครือข่ายอินเทอร์เน็ตหรือเครือข่ายอื่น ๆ ซึ่งเกตเวย์มีหน้าที่เป็นตัวกลางในการเชื่อมต่อ

จากการศึกษางานวิจัยที่เกี่ยวข้องกับการค้นหาเกตเวย์ มีการนำโพรโทคอลค้นหาเส้นทาง AODV [6],[8] มาปรับแก้รูปแบบและการส่งของข้อความ (Message) จากที่กำหนดใน RFC [4] โดยแก้ไข HELLO messages ที่ใช้เพื่อบอกถึงการมีตัวตนของตนเองกับโหนดรอบข้างโดยการบรอดแคสต์ซึ่งถูกส่งก็ต่อเมื่อโหนดนั้น ๆ ยังไม่มีการส่งคำร้องขอเส้นทาง (Route Request) การตอบกลับเส้นทาง (Route Reply) โดยในการปรับแก้รูปแบบข้อความนั้นได้ทำการเพิ่มแฟล็ก (Flag) พิเศษ ที่เรียกว่าแฟล็ก I (I-flag) เพื่อระบุว่าเป็น HELLO message ที่ส่งมาจากเกตเวย์ และบันทึกแอดเดรสของเกตเวย์ (Gateway Address) ใน HELLO message ด้วยเพื่อระบุว่าถูกสร้างมาจากเกตเวย์โหนดใด ขั้นตอนในการส่ง HELLO_I นั้นจะเริ่มส่งจากโหนดเกตเวย์เพื่อบอกถึงการมีอยู่ของโหนดเกตเวย์ให้ทุกโหนดที่อยู่ภายในช่วงคลื่นสัญญาณของเกตเวย์รับรู้ผ่านการรับ HELLO_I (จากการบรอดแคสต์ HELLO_I ของเกตเวย์) จากนั้นโหนดที่ได้รับ HELLO_I จะทำการการบันทึกเส้นทางที่สามารถไปยังเกตเวย์ และบรอดแคสต์ (Rebroadcast) HELLO_I ซ้ำออกไป แต่ถ้าโหนดใดไม่ได้รับ HELLO_I ในช่วงระยะเวลาของการส่ง HELLO messages (HELLO interval) โหนดนั้นก็จะทำการส่ง HELLO messages แบบปกติที่ไม่มีการปรับแก้แทน ซึ่งขอเรียกการค้นหาเส้นทางไปยังเกตเวย์นี้ว่า อัลกอริทึม HELLO และภายในงานวิจัยดังกล่าวนักวิจัยได้ทำการเปรียบเทียบอัลกอริทึม HELLO กับอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ และแบบรีแอกทีฟ โดยผลสรุปคือ อัลกอริทึม HELLO มีเวลาที่ใช้ในการค้นหาเกตเวย์ที่น้อยกว่าเมื่อเปรียบเทียบกับอัลกอริทึมทั้งสอง

โดยสำหรับโพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ [8] เมื่อโหนดได้รับข้อมูลเกี่ยวกับเกตเวย์จะตัดสินใจว่าจะรับหรือทิ้งข้อมูลนั้น โดยจะรับข้อมูลนั้นก็ต่อเมื่อโหนดไม่รู้เส้นทางไปยังเกตเวย์หรือข้อมูลนั้นมีเส้นทางที่สั้นกว่าหรือข้อมูลนั้นมาจากแหล่งกำเนิดเดียวกันแต่มีความใหม่กว่า (มี sequence number ที่มากกว่า) และถ้าหากโหนดเลือกรับข้อมูลเส้นทางก็จะหยุดการร้องขอเส้นทาง จากนั้นจึงทำการตั้งค่าหรือปรับปรุงเส้นทางไปยังเกตเวย์ตามข้อมูลที่ได้รับมา และส่งต่อไปยังโหนดอื่น ๆ

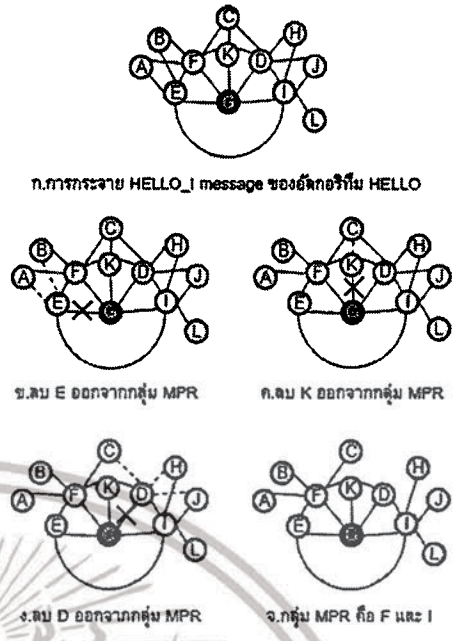
3. แนวคิดและการดำเนินงาน

จากงานวิจัยในส่วนที่ 2 เห็นได้ว่าอัลกอริทึม HELLO มีเวลาในการทำให้แต่ละโหนดรับรู้เส้นทางเชื่อมต่อไปยังเกตเวย์น้อยที่สุดเมื่อเทียบกับอัลกอริทึมอื่นๆ [8] แต่ยังมีข้อเสียเรื่องโอเวอร์เฮดเพราะทุกโหนดต้องทำการบรอดแคสต์ข้อมูล

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
1:   for x in V
2:   assume N = Nx - Nx'
3:        for i in N
4:             for j in N - i
5:                  if Nj ⊆ Ni
6:                       N = N - j
7:                  end
8:             end
9:        end
10:       for i in N
11:            for j in N - i
12:                 Ni,j = Ni,j ∪ (Ni ∩ Nj)
13:            end
14:       end
15:       for i in N
16:            if Ni ⊆ Ni,j
17:                 N = N - i
18:                 Ni,j = Ni,j - Ni
19:            end
20:       end
21:       V = V - (Nx - N)
22:  end
```

ภาพที่ 1: แสดงโค้ดเทียมของอัลกอริทึมในการหาโหนด MPR



ภาพที่ 2: แสดงตัวอย่างการหากลุ่มโหนด MPR

ในงานวิจัยนี้จึงนำอัลกอริทึม HELLO มาเพิ่มกลไกเพื่อลดจำนวนการบรอดแคสต์ข้อมูลเส้นทางที่เกี่ยวข้องกับเกตเวย์ด้วยวิธีการลดจำนวนโหนดที่ทำการบรอดแคสต์ ซึ่งกลไกนี้ถูกใช้ในโพรโทคอลค้นหาเส้นทาง OLSR เรียกว่าการเลือกโหนดเอ็มพีอาร์ (MPR: Multipoint Relays Selection) โดยมีหน้าที่ในการส่งต่อข้อมูล (Retransmission) โดยโหนดที่เริ่มต้นบรอดแคสต์นั้นจะมีทำหน้าที่ในการคัดเลือกโหนด MPR หรือเป็น MPR Selector ซึ่งโหนด MPR จะอยู่ในกลุ่มของโหนดข้างเคียง (Neighbor nodes) แต่ทุกโหนดที่เป็นโหนดข้างเคียงไม่จำเป็นต้องเป็นโหนด MPR ซึ่ง สามารถเปลี่ยนแปลงได้ตลอดตามความเหมาะสม ในการคัดเลือกโหนด MPR นั้น โหนด MPR Selector จะเลือกจากกลุ่มโหนดข้างเคียงในระยะ 1 hop (One Hop Neighbors) ของตนที่สามารถเชื่อมต่อกับโหนดข้างเคียงในระยะ 2 hop (Two Hop Neighbors) ของตนที่มากที่สุด ซึ่งโหนดข้างเคียงในระยะ 1 hop คือ โหนดที่ตนเองสามารถเชื่อมต่อได้ (โหนดที่อยู่ภายในช่วงคลื่นสัญญาณของตนเอง) แต่โหนดข้างเคียงในระยะ 2 hop คือ โหนดที่ตนเองไม่สามารถเชื่อมต่อได้แต่สามารถเชื่อมต่อผ่านโหนดข้างเคียงในระยะ 1 hop ได้ โดยมีงานวิจัยบางส่วนได้นำเอากลไกการเลือกโหนด MPR มาประยุกต์เข้ากับกลไกการแลกเปลี่ยน HELLO messages บนโพรโทคอล AODV [11] ซึ่งมีความแตกต่างกับงานวิจัยของเราเนื่องจากผู้จัดทำได้ทำการออกแบบกลการคัดเลือกโหนด MPR และกลไกการทำงานของโหนด MPR ขึ้นเอง ซึ่งแต่ละกลไกมีการทำงานดังนี้ กลการคัดเลือกโหนด MPR จะทำโดยการแลกเปลี่ยน HELLO message เพื่อเรียนรู้โหนดข้างเคียงในระยะ 1 hop และโหนดข้างเคียงในระยะ 2 hop ของทุกโหนดข้างเคียงในระยะ 1 hop จากนั้นจะนำข้อมูลดังกล่าวที่เรียนรู้มาทำการคัดเลือกโหนด MPR ซึ่งมีการทำงานตามโค้ดเทียมในภาพที่ 1

โดย G = กราฟเชื่อมโยง โดยที่ G = (V,E)

V = เซ็ตของโมบายล์โหนด

E = เส้นทางการเชื่อมโยงของแต่ละโมบายล์โหนด

x' = โหนด MPR ก่อนหน้า (Predecessor node)

$N_x \in V$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ของ x ใดๆใน V

$N'_x \in V$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop ของ x ใดๆที่ไม่มีโหนดที่ก่อให้เกิดเส้นทางที่ซ้ำซ้อน (Redundancy Paths) โดยที่ $N'_x \in V$ เป็นเซ็ตย่อยของ $N_x \in V$ และทำให้ G' = (V',E') โดยที่ $V' = U(x \in V)N'_x$ หรือกล่าวได้ว่า $N'_x \in V$ คือกลุ่มของโหนด MPR

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$N_{i,j}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ร่วมของโหนด i และ j โดย $i,j \in N$ และ $i \neq j$

จากโค้ดเทียมในภาพที่ 1 แสดงถึงอัลกอริทึมที่ใช้ในการคำนวณหาโหนด MPR หรือ $N'_x \in V$ และภาพที่ 2 แสดงตัวอย่างการหาโหนด MPR โดยการทำงานของอัลกอริทึมแบ่งออกได้เป็น 2 ขั้นตอน 1) หาความเป็นเซ็ตย่อย (Subset) คือ หาเซ็ตของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงที่เหลือที่ครอบคลุมโหนดข้างเคียงในระดับ 2 hop ที่เหมือนกันกันหรือน้อยกว่า แสดงอยู่ในภาพที่ 1 บรรทัดที่ 3 ถึง 9 และภาพที่ 2(ข และ ค) และ 2) หาเซ็ตของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงที่เหลือที่ครอบคลุมโหนดข้างเคียงในระดับ 2 hop ของตนมากที่สุด แสดงอยู่ในภาพที่ 1 บรรทัดที่ 10 ถึง 20 และภาพที่ 2(ง) โดยทำขั้นตอนที่ 2) ซ้ำจนกว่าจะไม่สามารถตัดเซ็ตใดออกจากการพิจารณาได้อีกซึ่งจะผลเป็นเซ็ตของโหนด MPR ซึ่งแสดงให้ภาพที่ 2(จ)

และสำหรับกลไกการทำงานของโหนด MPR จะระบุให้โหนดที่กำลังส่งข้อมูลเกตเวย์ขณะนั้นจะเป็นผู้เลือกโหนด MPR โดยใช้กลไกการเลือกโหนด MPR ที่ได้กล่าวไว้ข้างต้น ดังนั้นคำนวณหาโหนด MPR นั้นจึงเริ่มต้นคำนวณจากโหนดเกตเวย์เมื่อคำนวณเสร็จเกตเวย์จะทำการส่ง HELLO_I message ที่บรรจุข้อมูลเพื่อระบุว่าโหนดใดเป็นโหนด MPR ไปยังโหนดข้างเคียงในระยะ 1 hop จากนั้นเมื่อโหนดข้างเคียงที่เป็น MPR ได้รับ HELLO_I message ดังกล่าวก็จะทำการคำนวณหาโหนด MPR ของตนต่อไป และส่ง HELLO_I message ไปยังโหนด MPR ที่คำนวณได้ต่อไปเรื่อยๆ พร้อมทั้งบันทึกเส้นทางไปยังเกตเวย์ตามอัลกอริทึม HELLO ที่ได้กล่าวไว้ในส่วนที่ 2 แต่สำหรับโหนดข้างเคียงที่ได้รับ HELLO_I message ไม่ใช่โหนด MPR ก็จะไม่ส่งต่อ HELLO_I message แต่บันทึกเส้นทางไป ยังเกตเวย์เท่านั้น

ดังนั้นอัลกอริทึมที่ได้พัฒนาได้มีการลดโอเวอร์เฮดจากการแลกเปลี่ยน HELLO_I message ของอัลกอริทึม HELLO คือทุกโหนดที่ทำหน้าที่บรอดแคสต์ HELLO_I message ซึ่งอาจทำให้เกิดความซ้ำซ้อน ดังภาพที่ 2(ก) ที่ทุกโหนดต้องทำหน้าที่บรอดแคสต์ข้อความ แต่สำหรับอัลกอริทึมที่ได้พัฒนาโดยขอเรียกว่า HELLOMPR จะมีเพียงบางโหนดที่ทำหน้าที่ในการบรอดแคสต์ ตัวอย่างเช่น ในภาพที่ 2(ก) ที่ใช้อัลกอริทึม HELLO ที่โหนด A และ B ได้รับ HELLO_I message จากทั้งโหนด E และ F เมื่อเปรียบเทียบกับภาพที่ 2(จ) ที่ใช้อัลกอริทึม HELLOMPR ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด F เท่านั้น

4. การทดลองและการประเมินผล

ในการทดลองได้ทำการจำลองการทำงานของอัลกอริทึมผ่านโปรแกรมจำลอง OMNET++ ซึ่งเป็นการเปรียบเทียบระหว่างอัลกอริทึมในการค้นหาเกตเวย์ทั้ง 3 ได้แก่ 1) อัลกอริทึมโพรแอกทีฟ 2) อัลกอริทึม HELLO และ 3) อัลกอริทึม HELLOMPR ซึ่งในอัลกอริทึมที่ 1) และ 2) อ้างอิงการทำงานทำงานตามงานวิจัยที่ [6] โดยมีข้อกำหนดเกี่ยวกับเหตุการณ์จำลอง และผลการทดลองเปรียบเทียบดังนี้

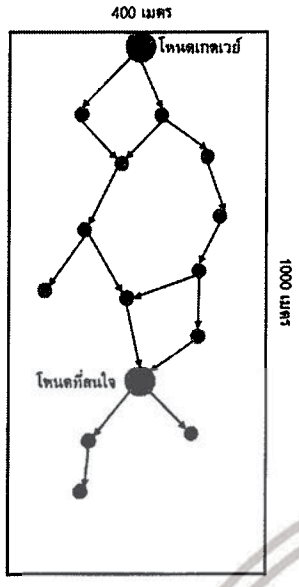
4.1 เหตุการณ์จำลองและตัวแปรต่าง ๆ ที่ใช้ในการจำลอง

กำหนดให้การกระจายตัวของโหนดจะกระจายแบบสุ่มอยู่ในเครือข่ายพื้นที่ขนาดกว้าง 400 เมตร และยาว 1,000 เมตร ดังแสดงในภาพที่ 3 ซึ่งแต่ละโหนดจะเคลื่อนที่ภายใต้ความเร็วสูงสุด 10 เมตร / วินาที โดยในการทดลองแต่ละครั้งใช้การกระจายตัวของโหนดแบบสม่ำเสมอ (Uniform Distribution) เพื่อให้แต่ละการทดลองโหนดมีการกระจายตัวที่แตกต่าง โดยจากภาพที่ 3 กำหนดให้โหนดที่เป็นเกตเวย์ (Gateway node) อยู่บนสุดของเครือข่าย และกำหนดให้โหนดที่สนใจซึ่งคือโหนดที่จะต้องได้รับข้อมูลเส้นทางไปยังเกตเวย์ อยู่ห่างจากเกตเวย์ระยะ 600 เมตร โดยที่ทุกโหนดมีระยะในการส่งข้อมูล 250 เมตรรอบตัวโหนด และมีตัวแปรต่าง ๆ ที่ได้กำหนดและใช้ในการจำลองเพิ่มเติมดังแสดงในตารางที่ 1

ตารางที่ 1: ตัวแปรต่างๆที่กำหนดในการทดลอง

จำนวนโหนดในเครือข่ายสื่อสารเฉพาะกิจ	15, 60
พื้นที่ของเครือข่าย	400 เมตร × 1,000 เมตร
ระยะส่งข้อมูลของโหนด	250 เมตร
เวลาทั้งหมดในการทดลอง	300 วินาที
ช่วงเวลาในการส่ง HELLO message	1, 5, 10, 15, 20, 25, 30
จำนวนรอบที่ใช้ในการทดลอง	100 รอบ (ทั้ง 15,60 โหนด)
รูปแบบการเคลื่อนที่ของโหนด	Random Waypoint
ความเร็วสูงสุดในการเคลื่อนที่	10 เมตร/วินาที

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



ภาพที่ 3: แสดงภาพจำลองทอพอโลยีของเครือข่าย

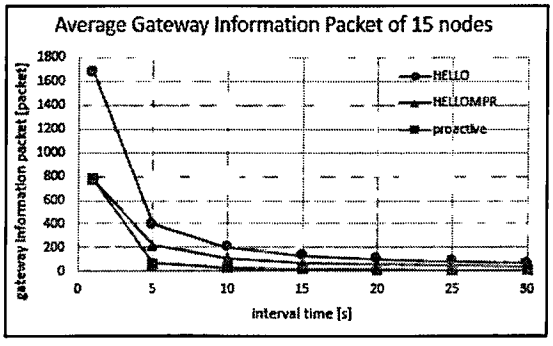
4.2 ผลการทดลองและตัวชี้วัด

สำหรับการทดลองเพื่อเปรียบเทียบระหว่างอัลกอริทึมค้นหาเกตเวย์เราได้เลือกตัวชี้วัดในการทดลองคือ 1) จำนวนของข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบ 2) เวลาที่ใช้ในการค้นหาเกตเวย์

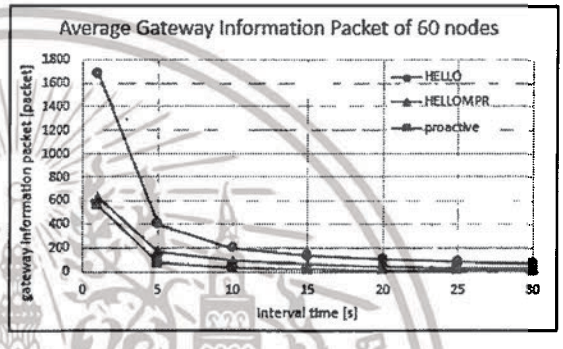
ในภาพที่ 4 ภาพที่ 5 และตารางที่ 2 แสดงให้เห็นถึงผลการทดลองในตัวชี้วัดด้านจำนวนข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ โดยอัลกอริทึม HELLO มีจำนวนข้อความที่ส่งในเครือข่ายมากที่สุด เนื่องจากทุกโหนดต้องทำการบรอดแคสต์ข้อมูลของเกตเวย์ แต่อัลกอริทึม HELLOMPR มีจำนวนน้อยกว่าในอัลกอริทึม HELLO มากเนื่องจากมีกลไกในการลดจำนวนโหนดที่ทำการบรอดแคสต์ แต่อัลกอริทึมแบบโพรแอกทีฟก็ยังมีจำนวนข้อความน้อยที่สุดเนื่องมาจากทุกโหนดจะทราบ topology ของทั้งระบบทำให้สามารถคำนวณหาโหนด MPR ได้อย่างเต็มประสิทธิภาพแต่สำหรับอัลกอริทึมที่ได้พัฒนานั้นทราบเพียงโหนดข้างเคียงในระยะ 1 และ 2 hop

ตารางที่ 2: ผลลัพธ์จำนวนข้อความที่ส่งเพื่อการค้นหาเกตเวย์

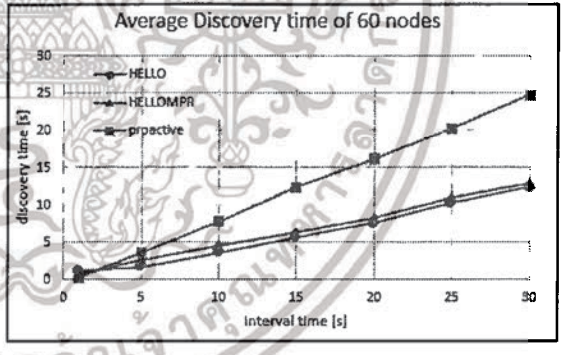
	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	784.443 pkt	31.402 pkt	10 pkt
HELLO	1683.25 pkt	200.39 pkt	66.124 pkt
HELLOMPR	778.248 pkt	110.69 pkt	37.009 pkt
60 nodes			
proactive	558.348 pkt	31.384 pkt	10 pkt
HELLO	1680.24 pkt	192.42 pkt	65.234 pkt
HELLOMPR	628.518 pkt	87.446 pkt	27.771 pkt



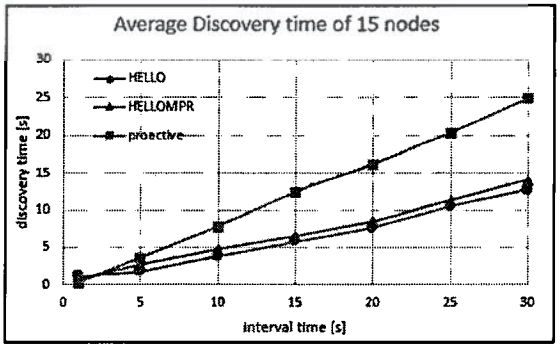
ภาพที่ 4: กราฟจำนวนข้อความที่ใช้เพื่อค้นหาเกตเวย์สำหรับ 15 โหนด



ภาพที่ 5: กราฟจำนวนข้อความที่ใช้เพื่อค้นหาเกตเวย์สำหรับ 60 โหนด



ภาพที่ 6: กราฟเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับจำนวน 15 โหนด



ภาพที่ 7: กราฟเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับจำนวน 60 โหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตารางที่ 3: ผลลัพธ์เวลาเฉลี่ยที่ใช้ในการค้นหาเกตเวย์

	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	0.231s	7.741s	24.83s
HELLO	1.148s	3.757s	12.69s
HELLOMPR	0.717s	4.677s	13.91s
60 nodes			
proactive	0.221s	7.727s	24.74s
HELLO	1.015s	3.532s	12.34s
HELLOMPR	0.621s	4.391s	12.89s

ในภาพที่ 6 ภาพที่ 7 และตารางที่ 3 แสดงผลลัพธ์ในตัวชี้วัดด้านเวลาที่ใช้ในการค้นหาเกตเวย์ (Gateway Discovery Time) โดยจะเริ่มนับตั้งแต่เกตเวย์ประกาศข้อมูลเส้นทางจนกระทั่งโหนดที่สนใจรับรู้เส้นทางไปยังเกตเวย์ โดยอัลกอริทึมแบบโพรแอกทีฟใช้เวลาในการค้นหาเกตเวย์สูง แต่สำหรับอัลกอริทึม HELLO และอัลกอริทึม HELLOMPR ก็มีเวลาที่ใช้ในการค้นหาเกตเวย์เพียงเล็กน้อย แต่อัลกอริทึม HELLO จะใช้เวลาน้อยที่สุดเนื่องจากการเพิ่มกลไกคัดเลือกโหนด MPR ทำให้โหนดที่สนใจอาจได้รับ HELLO_I message ช้ากว่าในกรณีที่โหนดที่สนใจนั้นอยู่ใกล้กับโหนดไม่ใช่ MPR มากกว่าโหนดที่ทำหน้าที่เป็น MPR

5. สรุปผล

ในงานวิจัยนี้ได้พัฒนาอัลกอริทึมในการค้นหาเกตเวย์สำหรับเครือข่ายสื่อสารเฉพาะกิจโดยมีพื้นฐานมาจากโพรโทคอล AODV และได้นำหลักการในการคัดเลือกโหนด MPR จากโพรโตคอล OLSR โดยใช้ทฤษฎีเซ็ตมาช่วยในการคำนวณเพื่อลดจำนวนข้อมูลที่ส่งต่อภายในเครือข่าย

จากผลการทดลองสรุปได้ว่าเครือข่ายที่ใช้อัลกอริทึม HELLOMPR มีการส่งข้อมูลเกี่ยวกับเกตเวย์น้อยกว่าอัลกอริทึม HELLO จนเข้าใกล้อัลกอริทึมแบบโพรแอกทีฟ ซึ่งเป็นผลจากการลดจำนวนโหนดที่ต้องบรอดแคสต์ข้อมูลที่ใช้ในการค้นหาเกตเวย์ ซึ่งส่งผลให้โหนดในเครือข่ายมีพลังงานทำให้โหนดอยู่ในระบบได้นานขึ้น และประสิทธิภาพด้านเวลาที่ใช้ในการทำให้โหนดที่สนใจรู้จักเส้นทางไปยังเกตเวย์ไม่ได้ลดลง ซึ่งในสถานการณ์ภัยพิบัตินั้นมีความจำกัดด้านแหล่งพลังงานของโมบายล์โหนด (จากแบตเตอรี่) และความเร่งด่วนในการสื่อสารนั้นก็มีความสำคัญ ดังนั้นอัลกอริทึมที่มีความเหมาะสมคืออัลกอริทึม HELLOMPR เพราะมีการส่งข้อความเป็นจำนวนน้อย และมีเวลาในการค้นหาเกตเวย์ต่ำ

เอกสารอ้างอิง

[1] T. S. Rappaport. "Wireless Communications Principles & Practice." Upper Saddle River, New Jersey: Prentice-Hall, Inc.1996

[2] T. Lin. "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications." Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the Ph.D. in Computer Engineering. 2004

[3] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)." Internet Engineering Task Force (IETF) draft, February 2007.

[4] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing." Internet Engineering Task Force (IETF) draft, July 2003.

[5] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol (OLSR)." Internet Engineering Task Force(IETF) draft, October 2003.

[6] M. Rosenschon. "Internet Gateway Discovery for Mobile Ad Hoc Networks" Submitted for the Degree of Doctor of Philosophy School of Engineering and Mathematical Sciences CITY University London. 2 October 2007

[7] J. Broch, et al. "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks" International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN99), Workshop on Mobile Computing, Perth, Western Australia. June 1999

[8] M. Rosenschon, T. Manz, J. Habermann, V. Rakocevic. "Gateway Discovery Algorithm for Ad-Hoc networks using HELLO Messages" International Workshop on Wireless Ad Hoc Networks IWWAN 2005, London. May 2005.

[9] M. Rosenschon, V. Rakocevic, J. Habermann "Performance Comparison of Gateway Discovery Algorithms in Ad Hoc Networks with Mobile Nodes" Wireless Conference 2006, 12th European, April 2006.

[10] H. Luo, R. Ramjeey, P. Sinhaz, L. Liy, S. Lu "UCAN: A Unified Cellular and AdHoc Network Architecture" MobiCom'03, San Diego, California, USA, September 2003.

[11] A. Tahar, B. Azeddine. "AODV Extension Using Multi Point Relay for High Performance Routing in VANETS" International Journal of Computer Science Department, 2007.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทความสิ่งประดิษฐ์

การประชุมวิชาการ งานวิจัย และพัฒนาเชิงประยุกต์ ครั้งที่ 6 การพัฒนาเทคโนโลยีเพื่อให้โลกมีสันติสุข

ECTI-CARD Proceedings 2014, Chiang Mai, Thailand

การพัฒนาระบบสื่อสาร สมาร์ทโฟนด้วยเทคโนโลยี WiFi-Direct

Development of Smartphone Networks with WiFi-Direct

ธีรพงษ์ โชคสถิตย์ , เบญจพร ปาวะรีย์ และ สุเมธ ประภาวัต

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

E-mail: TeerapongC@outlook.com , iiniim20421@gmail.com , sumet@it.kmitl.ac.th

บทคัดย่อ

จากการสื่อสารผ่านสายสัญญาณบนเครือข่ายแลน จนถึงการสื่อสารไร้สายผ่านอุปกรณ์พกพาขนาดเล็ก รูปแบบการสื่อสารได้รับการพัฒนาปรับปรุงอย่างต่อเนื่อง ทั้งในเรื่องความสะดวกสบาย ความรวดเร็วในการสื่อสาร ความถูกต้องของข้อความที่ปลายทางได้รับ และความยืดหยุ่นในการใช้งาน ด้วยเหตุนี้ผู้เขียนจึงให้ความสนใจในการพัฒนาศักยภาพของระบบสื่อสารระหว่างสมาร์ทโฟน (Smartphone) เพื่อสนับสนุนกิจกรรมการสื่อสาร ในกรณีที่ระบบสาธารณูปโภคพื้นฐานไม่สามารถใช้การได้ ยกตัวอย่างเช่น การแจ้งเหตุป้องกันหรือการขอความช่วยเหลือ จากเหตุการณ์ภัยพิบัติ เป็นต้น

คำสำคัญ: Smartphone Networks; WiFi-Direct; Ad hoc Network

Abstract

From communication via data signals in LAN network to wireless communication via small portable devices. Form of communication has been developed continuously. In terms comfort and speed of communication. The accuracy of the text has received at destination. And resilience in applications. Thus, this project foresees potential for a study on smartphone ad hoc networks to support the activities communication infrastructures could not rely on it. For example, notifications or requests for assistance from catastrophic events. The ad hoc networks are expected to communicate support for the people who need it when such a situation arises.

Keyword: Smartphone Networks; WiFi-Direct; Ad hoc Network

1. บทนำ

ระบบสื่อสารเป็นสิ่งจำเป็น มีบทบาท และเป็นส่วนสนับสนุนสำคัญของกิจกรรมต่างๆ อย่างเช่น การแจ้งเหตุป้องกันหรือการขอความช่วยเหลือ จากเหตุการณ์ภัยพิบัติ จากการศึกษาพบว่า เหตุการณ์ภัยพิบัติมักจะก่อให้เกิดความเสียหายแก่สาธารณูปโภคพื้นฐานของระบบเครือข่ายสื่อสาร เช่น สถานีฐาน (Base Station) หรือเสากระจายสัญญาณ เป็นเหตุให้ระบบสื่อสารไม่สามารถใช้การได้

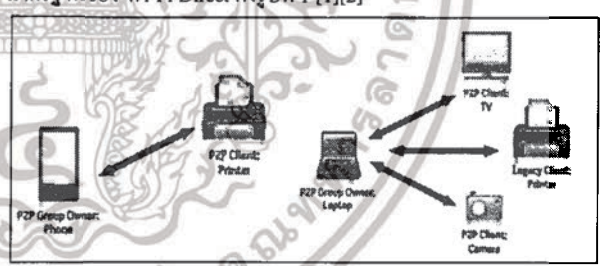
ระบบสื่อสารสำรองจึงมีความสำคัญ การพัฒนาระบบสื่อสารระหว่างสมาร์ทโฟน จึงเป็นการสร้างแอพลิเคชั่นเพื่อเชื่อมต่อระหว่างสมาร์ทโฟนเครื่องหนึ่งไปยังสมาร์ทโฟนอีกเครื่องหนึ่ง ให้สามารถแลกเปลี่ยนข้อมูลข่าวสาร ซึ่งเป็นช่องทางการสื่อสารที่ไม่ต้องพึ่งพาสาธารณูปโภคพื้นฐาน โดยอาศัยเทคโนโลยี Wi-Fi Direct นั่นเอง

2. ทฤษฎีและหลักการ

2.1 Wi-Fi Direct

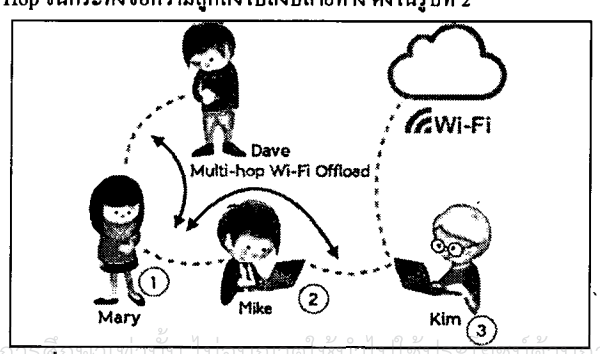
Wi-Fi Direct คือ เทคโนโลยีการสื่อสารตามมาตรฐาน Wi-Fi มีการเชื่อมต่อลักษณะ Peer-to-Peer โดยผู้ใช้สามารถเชื่อมต่อกับอุปกรณ์อื่นๆ ได้โดยตรง ไม่จำเป็นต้องติดต่อกับเครือข่ายโครงสร้างพื้นฐาน (Infrastructure network)

Wi-Fi Direct เริ่มต้นการทำงานโดยอุปกรณ์จะสร้างการเชื่อมต่อไปยังอุปกรณ์ใกล้เคียง เพื่อแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ทั้งสองโดยตรง ซึ่งการส่งสารในลักษณะนี้เรียกว่า 1 Hop ทั้งนี้ผู้ใช้ต้องร้องขอการเชื่อมต่อกับอุปกรณ์ใกล้เคียงผ่าน Wi-Fi Protected Setup ที่รักษาความปลอดภัยในการเชื่อมต่อด้วย industry-standard WPA2 security และเมื่ออุปกรณ์ทั้งสองเชื่อต่อกัน การเชื่อมต่อจะอยู่ในรูปแบบของ Wi-Fi Direct Group เพราะฉะนั้นอุปกรณ์ทั้งสองจะสามารถบริการได้ทุกอย่างที่อยู่บนมาตรฐานของ Wi-Fi Direct ดังรูปที่ 1 [1][2]



รูปที่ 1. ลักษณะการเชื่อมต่อของ Wi-Fi Direct[1]

แต่ Wi-Fi Direct มีข้อจำกัดคือรองรับการเชื่อมต่อเพียง 1 Hop เพราะฉะนั้นจะไม่สามารถนำมาใช้ในสถานการณ์ปกติได้ เพราะการสื่อสารประกอบไปด้วยเส้นทางย่อยหลาย Hop (Multi-Hop) จึงต้องประยุกต์ใช้การส่งต่อจากโหนดหนึ่งไปยังอีกโหนดหนึ่ง ต่อเนื่องหลาย Hop จนกระทั่งข้อความถูกส่งไปถึงปลายทาง ดังในรูปที่ 2

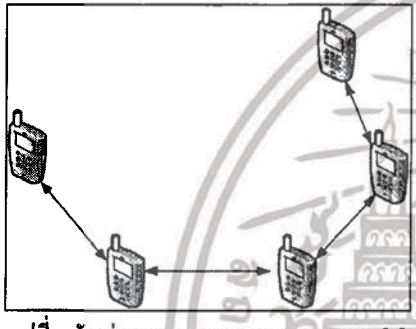


รูปที่ 2. การหาเส้นทางแบบ Multi-Hop Routing ด้วย Wi-Fi Direct[1]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 Mobile Ad hoc Network (MANET)

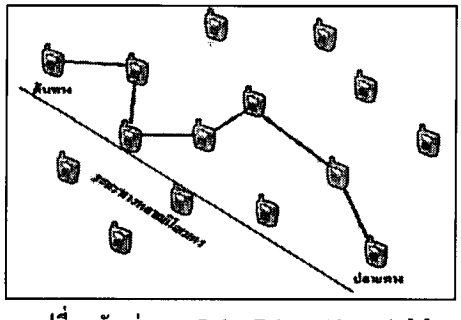
เครือข่ายไร้สายเฉพาะกิจ (Mobile Ad Hoc Network - MANET) ทำให้โหนดเคลื่อนที่แบบไร้สาย (Wireless Mobile Node) สามารถทำการสื่อสาร ในขณะกำลังสื่อสารได้อย่างอิสระ ผ่านการจองเส้นทางล่วงหน้าก่อนการส่งข้อมูลได้ ดังนั้นจึงสามารถนำมาปรุยุกต์ใช้บนเครือข่ายสื่อสารชั่วคราวที่ไม่จำเป็นต้องมีโครงสร้างพื้นฐาน เช่น เสากระจายสัญญาณ (Base Station) และเปลี่ยนการควบคุมของศูนย์กลางการควบคุม (Centralized Administration) เป็นการอาศัยความร่วมมือกันระหว่างโหนดในการส่งต่อข้อมูล โดยโหนดจะปฏิบัติตัวเองเป็นเสมือนเราเตอร์ (Router) ส่งต่อข้อมูลระหว่างจากโหนดหนึ่งไปยังอีกโหนดหนึ่ง ต่อเนื่องไปจนถึงโหนดปลายทางดังรูปที่ 3 [3][4]



รูปที่ 3.ตัวอย่างของ Mobile Ad hoc Networks[3]

2.3 Delay-Tolerant Network (DTNs)

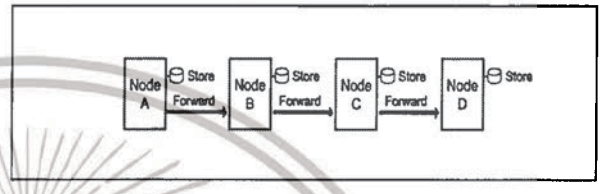
เครือข่ายที่มีความคงทนต่อความหน่วง (เครือข่ายดีทีเอ็น) เป็นเทคโนโลยีที่ทำให้เกิดการติดต่อสื่อสารบนพื้นที่เฉพาะ(Regions) ซึ่งเทคโนโลยีเครือข่ายในปัจจุบันไม่สามารถนำไปใช้ในทางปฏิบัติได้ เนื่องจากการสื่อสารบนพื้นที่เฉพาะนั้น โหนดและช่องทางการเชื่อมต่อระหว่างโหนด(Link) อาจจะมีปัญหาในเรื่องความน่าเชื่อถือ เช่น มีโอกาสในการเชื่อมต่อกันได้ยาก หากเกิดการเชื่อมต่อก็จะเกิดขึ้นเพียงแค่ในช่วงระยะเวลาสั้นๆเท่านั้น อันเป็นสาเหตุให้เกิดความผิดพลาดของข้อมูล ข้อมูลบางส่วนขาดหายระหว่างส่ง หรือการขาดการเชื่อมต่อของเครือข่ายเป็นเวลานาน ซึ่งปัญหาเหล่านี้ก็จะส่งผลกระทบต่อความแปรปรวนของ Hop (ช่องทางการส่งข้อมูลระหว่าง router หนึ่งๆ) หรือช่องทางการส่งข้อมูลของ router [5]



รูปที่ 4. ตัวอย่างของ Delay-Tolerant Networks[5]

ลักษณะเด่นของเครือข่ายดีทีเอ็น คือการสร้างการเชื่อมต่อระหว่างอุปกรณ์ Mobile Device ในสถานการณ์ที่ Network ไม่สามารถสร้าง End to End Connection ได้ เพื่อให้เกิดการติดต่อสื่อสาร ซึ่งจะเป็นการทำให้ Network มีความกว้างขึ้น จากเทคโนโลยี Wire และ Wireless ดังรูปที่ 4

กระบวณการทำงานของดีทีเอ็นนั้น จะมีลักษณะการทำงานโดย ทำการเชื่อมโยงโปรโตคอลของเครือข่าย ที่ยอมให้สามารถเกิดการติดต่อกันระหว่างอุปกรณ์สัญญาณได้ แม้ว่า Network จะไม่ได้มีการเชื่อมต่ออยู่ตลอดเวลาก็ตาม ซึ่งโหนดใด ๆ ที่อยู่ระหว่างโหนดต้นทางกับโหนดปลายทางอาจจะต้องทำหน้าที่ในการช่วยรับข้อมูลแล้วส่งต่อ ทำให้การส่งสามารถส่งถึงปลายทางได้ ดังรูปที่ 5



รูปที่ 5. กระบวณการทำงานของดีทีเอ็น [5]

โดยตัวอย่างกลไกการส่งข้อความบนเครือข่ายดีทีเอ็นเช่น Direct Mail, Gradient Routing และ Epidemic Routing เป็นต้น [8][9]

3. การวิเคราะห์และออกแบบ

3.1 ความต้องการของระบบ

3.1.1 ความต้องการหลักของระบบ

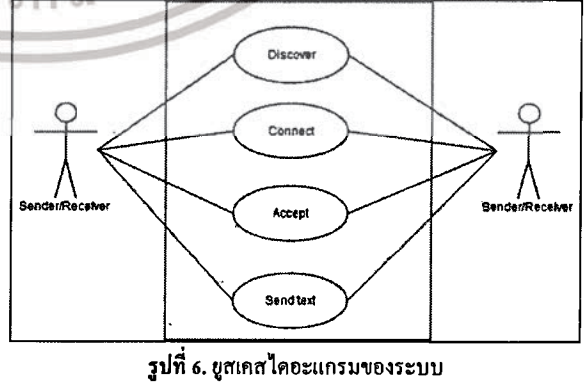
- สามารถค้นหาผู้ใช้อื่น
- เชื่อมต่อเข้ากับผู้ใช้อื่นที่ต้องการ
- สามารถสร้างข้อความและส่งข้อความ
- ยอมรับการเชื่อมต่อจากผู้ขอทำการเชื่อมต่ออื่นได้

3.1.2 ความต้องการของระบบที่ไม่ใช่ หน้าที่หลักของระบบ

- ผู้ใช้งานระบบต้องเปิดสัญญาณ Wi-Fi Direct

3.2 ภาพรวมของระบบ

จากความต้องการของระบบ แสดงภาพรวมของระบบสื่อสารระหว่างสมาร์ทโฟนด้วย WiFi-Direct ได้ ดังรูปที่ 6 ดังนี้

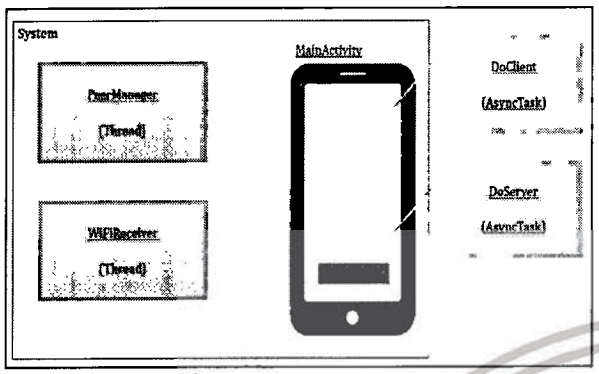


รูปที่ 6. ยูสเคสไดอะแกรมของระบบ

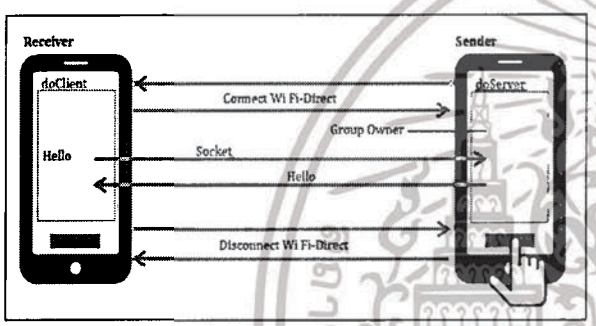
ภายในระบบจะประกอบไปด้วย เทรดสองชนิด ได้แก่ PeerManager ที่ทำหน้าที่ เกี่ยวกับการติดต่อจากผู้ที่เข้ามาร้องขอการเชื่อมต่อ และ WiFiReciever จะทำหน้าที่ดูแลการเชื่อมต่อของเทคโนโลยี WiFi-Direct กับการทำงานของเครื่อง และในส่วนของตัวเครื่อง(MainActivity) มีการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ใช้ AsyncTask เพื่อสลับหน้าที่การทำงานของเครื่องไปมาระหว่าง Client และ Server ดังในรูปที่ 7 และ 8



รูปที่ 7. องค์ประกอบภายในระบบ



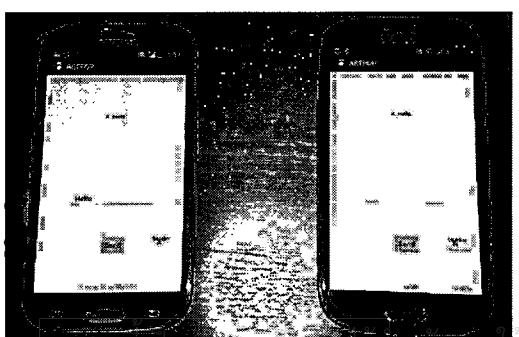
รูปที่ 8. ขั้นตอนการทำงานภายในระบบ

4. ผลการทำงานของระบบ

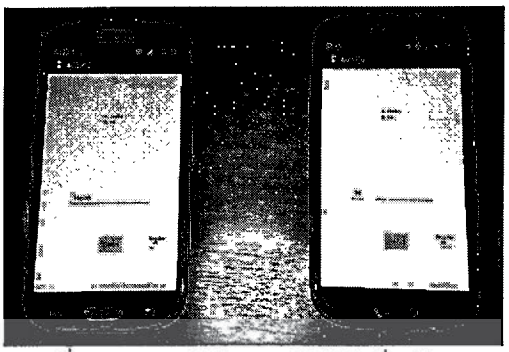
จากการทดลองการใช้งานแอพพลิเคชั่นที่พัฒนาขึ้น เพื่อส่งข้อความระหว่างสมาร์โฟน ด้วยWiFi-Direct แสดงผลดังรูปที่ 9, 10 และ 11



รูปที่ 9. แสดงการตั้งชื่อเครื่อง และพิมพ์ข้อความเพื่อส่งไปให้เครื่องถัดไป



รูปที่ 10. แสดงข้อความที่ได้รับจากการส่งข้อความผ่าน **WiFi-Direct**



รูปที่ 11. แสดงการส่งข้อความกลับไปยังเครื่องต้นทาง

5. สรุปผลทำงานของระบบและแนวทางในการพัฒนาต่อยอด

ระบบสื่อสารระหว่างสมาร์ทโฟนด้วย WiFi-Direct เป็นระบบที่สามารถสร้างช่องทาง เพื่อการสื่อสารหรือส่งข้อมูล โดยไม่ต้องพึ่งพาระบบสาธารณูปโภคพื้นฐาน เหมือนในระบบสื่อสารทั่วไป โดยอาศัยการทำงานของเทคโนโลยี WiFi-Direct ซึ่งจากการทำการทดลองการทำงานของระบบ แสดงให้เห็นว่า สามารถแลกเปลี่ยนข้อความระหว่างสมาร์ทโฟนแบบ 1-Hop ได้

ในการพัฒนาระบบทำให้เล็งเห็นถึงความเป็นไปได้ ในการพัฒนาให้ระบบสามารถส่งข้อมูลแบบ Multi-Hop ซึ่งจะทำให้ระบบมีประสิทธิภาพเกิดความเหมาะสมต่อการนำไปประยุกต์ใช้ได้มากขึ้น จึงมีการเสนอแนวทางการพัฒนาต่อในอนาคต โดยจะศึกษาความท้าทายในการสื่อสารของเครือข่ายไร้สายเคลื่อนที่ ขีดจำกัดการทำงานของเทคโนโลยี WiFi-Direct และศึกษาเทคโนโลยีเครือข่าย ซึ่งปัจจุบันมีเทคโนโลยีเครือข่ายไร้สายเคลื่อนที่ ที่ได้รับความสนใจคือ เทคโนโลยีเครือข่ายมาเน็ต (MANET : Mobile Ad-hoc Network) และเทคโนโลยีเครือข่ายดีทีเอ็น (DTN : Delay Tolerant Network) ซึ่งจะใช้ในการศึกษาเพื่อสร้างเครือข่ายเฉพาะกิจเพื่อนำมาใช้ในการพัฒนาระบบต่อไป[7]

โดยได้มีการวิเคราะห์ประสิทธิภาพของเครือข่ายที่มีความเหมาะสมต่อการนำมาใช้งานแล้ว สรุปได้โดยย่อว่า การนำสมาร์ทโฟนมาสร้างการเชื่อมต่อกันโดยตรง เป็นช่องทางการสื่อสารสำรอง แทนการเชื่อมต่อเข้าระบบสื่อสารหลักที่ล้มเหลว อันเนื่องมาจากสถานีฐานหรือเสากระจายสัญญาณได้รับความเสียหาย จำเป็นต้องอาศัยเทคโนโลยีการสื่อสารแบบไร้สาย (Wi-Fi) เพื่อสร้างเป็นเครือข่ายสื่อสารเฉพาะกิจของสมาร์ทโฟน ทำให้ผู้ใช้สมาร์ทโฟนสามารถทำการติดต่อสื่อสารระหว่างกันได้ แต่ทั้งนี้การที่สมาร์ทโฟนเป็นอุปกรณ์สื่อสารที่มีการเคลื่อนที่ตลอดเวลา และมีพลังงานที่จำกัด เป็นปัญหาสำคัญต่อประสิทธิภาพการทำงานของเครือข่ายสื่อสาร

เนื่องจากการสื่อสารเฉพาะกิจของสมาร์ทโฟน เป็นรูปแบบหนึ่งของเครือข่ายไร้สายเคลื่อนที่ จึงมีปัจจัยของปัญหาในการสื่อสาร[6]ดังต่อไปนี้

1. การเชื่อมต่อที่ไม่สม่ำเสมอ เป็นการขาดช่วงของเส้นทางการสื่อสารระหว่างผู้ส่งสารกับผู้รับสาร(Network Partitioning) เป็นผลมาจากการเคลื่อนที่อย่างไม่แน่นอนของโหนดในเครือข่าย

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
ห้ามใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. ความหน่วงมีค่าสูง เนื่องจากเป็นการสื่อสารในเครือข่ายไร้สายเคลื่อนที่ จึงทำให้เกิดปัญหาเกี่ยวกับ ดีเลย์ในการส่งข้อมูลระหว่างโหนดมีค่ามาก และมีความแปรปรวนของดีเลย์ที่เกิดจากการรอคิว

3. ความไม่สมดุลของอัตราการส่งข้อมูล ในสถานการณ์จริง ความแตกต่างของพื้นที่ในการสื่อสารและความสามารถในการสื่อสารของโหนด ส่งผลให้เกิดความไม่สมดุลของอัตราการส่งข้อมูลมากเกินรองรับได้

4. อัตราความผิดพลาดสูง เมื่อพิจารณาลักษณะของการสื่อสารในเหตุการณ์ภัยพิบัติ เช่น โหนดมีการเคลื่อนที่ สภาพพื้นที่กีดขวางการสื่อสาร เป็นต้น ทำให้อัตราความผิดพลาดสูงกว่าเครือข่ายทั่วไป

เมื่อพิจารณาเครือข่ายมาเน็ตพบว่า การที่โหนดต้นทางต้องค้นหาเส้นทางเพื่อเชื่อมต่อไปยังโหนดปลายทาง จากนั้นจึงเริ่มทำการส่งข้อมูล ซึ่งการสื่อสารอาจเกิดความขัดข้องหรือล้มเหลวได้ จากปัญหาที่โหนดต้นทางไม่สามารถหาเส้นทางได้ ในกรณีที่เครือข่ายมีความหนาแน่นของโหนดน้อย หรือปัญหาการเชื่อมโยงขาดอันเนื่องมาจากการเคลื่อนที่ของโหนด รวมไปถึงปัญหาการพลาดโอกาสเลือกโหนดรับช่วงต่อ(ที่ดีกว่า)ที่พึ่งเข้ามาในรัศมีการสื่อสารด้วย โดยปัญหาเหล่านี้มักพบบ่อยในเครือข่ายมาเน็ต

แต่ในเครือข่ายดีทีเอ็น โหนดไม่จำเป็นต้องมีการสร้างเส้นทางเชื่อมระหว่างโหนดต้นทางกับโหนดปลายทาง การส่งต่อข้อมูลจะเกิดขึ้นผ่านโหนดรับช่วงต่อสามารถถูกเลือกจากโหนดจร(Mobile Node) ใดๆก็ได้ ที่เป็นไปตามเงื่อนไขที่ถูกกำหนดขึ้นเพื่อโอกาสสำเร็จในการส่งข้อมูลไปปลายทาง จากความยืดหยุ่นในการเลือกโหนดรับช่วงต่อที่เหมาะสมของเครือข่ายดีทีเอ็นนี้ จึงสามารถแก้ไขปัญหาที่เกิดในเครือข่ายมาเน็ตได้

เพราะฉะนั้นแนวทางการพัฒนาต่อเนื่องในอนาคตคือ นำกลไกการส่งข้อความแบบ 1 Hop ของสมาร์ทโฟนผ่าน WiFi-Direct มาสร้างการส่งข้อความแบบ Multipath routing บนเครือข่ายดีทีเอ็น ซึ่งหมายถึงการฝากและส่งต่อข้อความไปกับโหรดจรใด ๆ อย่างต่อเนื่อง จนกระทั่งข้อความถูกส่งไปให้โหนดปลายทางนั่นเอง

เอกสารอ้างอิง

[1] Wi-Fi CERTIFIED Wi-Fi Direct™ Consumer. Reading: Wi-Fi Alliance®, October 2010.

[2] Wi-Fi CERTIFIED Wi-Fi Direct™ Industry. Reading: Wi-Fi Alliance®, October 2010.

[3] M. K. Jeya Kumar, R. S. Rajesh. "A Survey of MANET Routing Protocols in Mobility Models." Medwell Journals, 2009. [Available Online]: http://www.medwelljournals.com /fulltext/?doi=ijscomp.2009.136.141

[4] Sunil Taneja, Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks." Reading: International Association of Computer Science and Information Technology, August 2010.

[5] Forrest Warthman, Delay- and Disruption- Tolerant Network(DTNs): A Tutorial. Reading: Interplanetary Internet Special Interest Group, July 2012.

[6] Forrest Warthman, Delay- and Disruption- Tolerant Network(DTNs): A Tutorial. Reading: Interplanetary Internet Special Interest Group, July 2012.

[7] Laurent Franck, Performance comparison of mobile ad-hoc and delay tolerant network. [Available Online]: http://www-public.int-evry.fr/~kohlenb/sites_web_projets/i_pluton/Livrables/i%20Pluton%2011%20_%20Manets%20_%20DTN.pdf

[8] Samo Grasic, Anders Lindgren, An Analysis of Evaluation Practices for DTN Routing Protocols. [Available Online]: http://soda.swedish-ict.se/5290/1/practices-cameraready.pdf

[9] Evan P.C. Jones, Paul A.S. Ward, Routing Strategies for Delay-Tolerant Networks. [Available Online]: http://ccng.uwaterloo.ca/~pasward/Publications/dtn-routing-survey.pdf

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การศึกษาความเป็นไปได้ในการลดโอเวอร์เฮดบนระบบเครือข่ายไร้สายเฉพาะกิจ โดยการสร้างเงื่อนไขในการจำกัดการกระจายของข้อมูล ในขั้นตอนการค้นหาเส้นทาง

ธนานพ ทองถาวร วรวัชร ณรงคะชวนะ และ สุเมธ ประภาวัต

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: St_freedom2@hotmail.com, worravat@gamil.com, sumet@it.kmitl.ac.th

บทคัดย่อ

ในปัจจุบันระบบเครือข่ายไร้สายเฉพาะกิจ(Mobile Ad-hoc network) ได้มีการศึกษาอย่างแพร่หลาย โดยมีจุดประสงค์ที่จะผลักดันแนวคิดการทำงานของระบบเน็ตเวิร์คเฉพาะกิจให้สามารถนำมาใช้งานได้ในเชิงปฏิบัติ เพื่อที่จะให้บรรลุวัตถุประสงค์ดังกล่าว นักวิจัยจำเป็นต้องแก้ไขปัญหาหลักสองข้อซึ่งมีผลต่อประสิทธิภาพในการทำงานของระบบอย่างมาก ได้แก่ โอเวอร์เฮด หรือแพ็คเกตที่ไม่มีประโยชน์ต่อการสื่อสารระหว่างโหนดบนระบบเน็ตเวิร์ค และ ปัญหาเรื่องข้อจำกัดของพลังงานในระบบ ในบทความฉบับนี้ได้นำเสนอวิธีการจำกัดการกระจายของข้อมูลในระบบเน็ตเวิร์คเฉพาะกิจเพื่อลดจำนวนโอเวอร์เฮดในระบบ จากการศึกษาพบว่าแนวคิดที่นำเสนอขึ้นใหม่นั้น สามารถลดจำนวนโอเวอร์เฮดลง ในขณะที่ยังคงรักษาอัตราความสำเร็จในการสร้างช่องทางการติดต่อสื่อสารกันระหว่างโหนดได้

คำสำคัญ— เครือข่ายไร้สายเฉพาะกิจ; โอเวอร์เฮด; จำกัดการกระจายข้อมูล

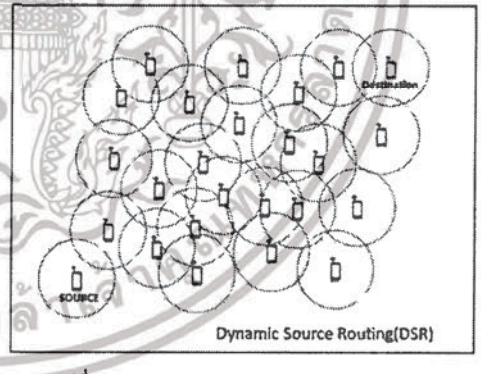
1. บทนำ

ระบบเครือข่ายไร้สายเฉพาะกิจ(Mobile Ad-hoc network) เป็นระบบเครือข่ายแบบไม่มีโครงสร้างโดยอาศัยสมาชิกในระบบเครือข่ายหรือโหนดเป็นสื่อกลางในการติดต่อสื่อสาร ซึ่งการใช้เครือข่ายไร้สายเฉพาะกิจนั้นจะมีประโยชน์มากเมื่อระบบเครือข่ายปกติไม่สามารถใช้งานได้ ยกตัวอย่างเช่น เมื่อเกิดเหตุภัยพิบัติทางธรรมชาติเป็นต้น โดยกระบวนการติดต่อสื่อสารภายในระบบเครือข่ายไร้สายเฉพาะกิจจำเป็นต้องมีโปรโตคอล[1] ที่ใช้ในการควบคุมการทำงานของระบบโดยเฉพาะ โดยใช้แนวคิดพื้นฐานจากสถาปัตยกรรมแบบเพียร์ทูเพียร์ [2] ในการกระจายแพ็คเกตออกไปรอบตัวเพื่อค้นหาและสร้างเส้นทางการติดต่อสื่อสารระหว่างโหนดปลายทาง ในขั้นตอนดังกล่าวจะมีแพ็คเกตอีกจำนวนหนึ่งที่ส่งไปไม่ถึงปลายทางหรือเรียกว่าโอเวอร์เฮด แพ็คเกตเหล่านี้จะส่งผลให้เกิดความแออัดให้แก่ระบบเน็ตเวิร์คเป็นอย่างมาก ซึ่งทำให้ระบบเน็ตเวิร์คประสบกับปัญหา NETWORK COLLISION[3] ที่ส่งผลเสียโดยตรงต่ออัตราความสำเร็จในการสร้างเส้นทางการติดต่อสื่อสารในระบบ

ในบทที่สองจะกล่าวถึงโปรโตคอลต่างๆที่ใช้ในการควบคุมการกระจายแพ็คเกตในระบบเครือข่ายไร้สายเฉพาะกิจ บทที่สามจะกล่าวถึงแนวคิดในการออกแบบโปรโตคอลใหม่ที่มีวัตถุประสงค์ในการลดโอเวอร์เฮดโดยที่ไม่ส่งผลกระทบต่อค่าความสำเร็จในการสร้างเส้นทางการติดต่อสื่อสาร และทำการทดสอบโปรโตคอลด้วยระบบซิมูเลชั่นในบทที่ 4 และสรุปผลการทดลองในบทที่ 5

2. ทฤษฎีและงานที่เกี่ยวข้อง

2.1. Dynamic Source Routing (DSR)



รูปที่ 1. Dynamic source routing protocol scheme

Dynamic Source Routing หรือ DSR [4] เป็นโปรโตคอลพื้นฐานที่ใช้ในการสื่อสารกันระหว่างโหนดในระบบเครือข่ายไร้สายเฉพาะกิจ โดยกระบวนการติดต่อสื่อสารนั้นจะเกิดขึ้นเมื่อโหนดต้นทางต้องการส่งข้อมูลไปยังโหนดปลายทาง โหนดต้นทางจะเริ่มขบวนการค้นหาเส้นทาง(Route discovery) โดยการกระจายแพ็คเกต Route request (RREQ) ออกไป ในกรณีที่โหนดที่ได้รับแพ็คเกต RREQ ไม่ใช่โหนดปลายทางก็จะทำการกระจายแพ็คเกตนั้นต่อไปและเพิ่มตำแหน่งของตัวเองลงไปบนเฮดเดอร์ของแพ็คเกตนั้น เมื่อแพ็คเกตถูกส่งไปจนถึงปลายทาง โหนดปลายทางจะใช้ตำแหน่งของโหนดที่ถูกบันทึกเอาไว้บนเฮดเดอร์มาใช้ในการสร้างเส้นทางการเชื่อมต่อสื่อสารกับโหนดต้นทาง

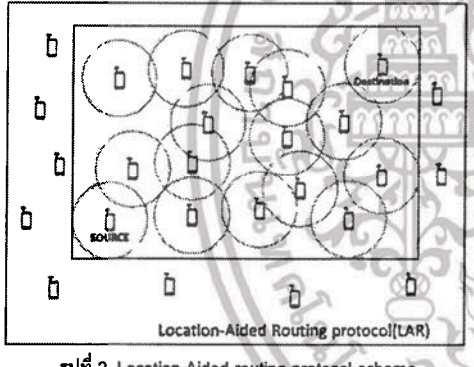
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยการส่งแพ็คเกต Route reply ที่บันทึกข้อมูลเส้นทางที่สามารถส่งข้อมูลมายังโหนดปลายทางได้กลับไปที่โหนดต้นทาง

เนื่องจากโหนดในระบบเครือข่ายไร้สายเฉพาะกิจมีการเคลื่อนที่ตลอดเวลา จึงมีความเป็นไปได้มากที่เส้นทางที่ถูกสร้างไว้ในขั้นตอน Route Discovery จะไม่สามารถใช้งานได้เมื่อระยะเวลาผ่านไป เมื่อโหนดใดๆไม่สามารถส่งข้อมูลตามเส้นทางที่กำหนดไว้โดยโหนดต้นทาง โหนดนั้นๆจะส่ง Route error message กลับมาที่โหนดต้นทาง จากนั้นโหนดต้นทางจะเริ่มกระบวนการ Route maintenance โดยการเลือกใช้เส้นทางอื่นที่ถูกเก็บอยู่ใน catch ของโหนดต้นทาง หรือเริ่มกระบวนการ Route discovery ใหม่อีกครั้ง

การจำกัดการกระจายแพ็คเกตบนโปรโตคอล DSR จะใช้ Route cache เข้ามาช่วยลดโอเวอร์เฮดในระบบ เมื่อโหนดปลายทางส่ง Route reply message กลับมายังโหนดต้นทาง โหนดที่อยู่ระหว่างทางจะทำการสำรองเส้นทางเอาไว้ใน Route cache เมื่อโหนดได้รับ RREQ แพ็คเกต ก็จะทำการตรวจสอบใน route cache ว่ามีเส้นทางที่จะสามารถส่งข้อมูลไปยังปลายทางที่ระบุไว้บน RREQ หรือไม่ ถ้ามีก็จะทำการส่ง Route reply กลับไปยังโหนดต้นทางทันที

2.2. Location-Aided Routing Protocol (LAR)



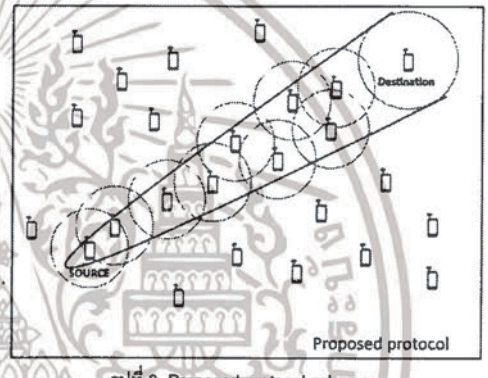
รูปที่ 2. Location-Aided routing protocol scheme

Location-Aided Routing protocol หรือ LAR [5] เป็นโปรโตคอลที่มีการพัฒนาต่อยอดมาจาก DSR โดยการใช้ระบบพิกัด GPS [6] เข้ามาช่วยในการคาดเดาตำแหน่งของปลายทาง ทำให้สามารถสร้างเงื่อนไขในการจำกัดการกระจายของข้อมูลได้ ในกระบวนการทำงานของโปรโตคอล LAR จำเป็นต้องรู้พิกัด GPS ของโหนดปลายทาง และความเร็วเฉลี่ยของโหนดปลายทางเพื่อที่จะคำนวณความเป็นไปได้ที่โหนดปลายทางจะเคลื่อนที่จากจุดเดิมเป็นระยะเท่าไหร่ หรือเรียกว่า expected zone จากนั้นจึงสร้างเงื่อนไขในการกระจายของข้อมูลให้อยู่ในพื้นที่ที่กำหนด ซึ่งจะถูกเรียกว่า forwarding zone จากรูปที่ 2 จะสังเกตได้ว่า expected zone คือพื้นที่วงกลมที่ล้อมรอบโหนดปลายทาง และ forwarding zone คือกรอบสี่เหลี่ยมที่มีโหนดต้นทางอยู่ที่ปลายของเส้นทแยงมุมที่ทำกับโหนดปลายทาง จากนั้นโปรโตคอล LAR จะเริ่มขั้นตอนการทำ Route Discovery เช่นเดียวกับโปรโตคอล DSR เพื่อค้นหาเส้นทางในการติดต่อสื่อสารต่อไป โดยที่โปรโตคอล LAR ยังคงมีการใช้ Route Cache เช่นเดียวกัน

3. แนวคิดการออกแบบโปรโตคอล

จากการศึกษาลักษณะการทำงานบนโปรโตคอล DSR และ LAR แล้ว ผู้วิจัยเล็งเห็นถึงประโยชน์ของการจำกัดการกระจายข้อมูลในขั้นตอน Route discovery ว่าสามารถช่วยลดปัญหาการเกิดโอเวอร์เฮดได้ แต่เนื่องจากเงื่อนไขการจำกัดการกระจายข้อมูลยังไม่รัดกุมมากพอ จึงทำให้มีแนวคิดในการเพิ่มประสิทธิภาพในการทำงานของโปรโตคอลให้สามารถช่วยลดโอเวอร์เฮดได้มากยิ่งขึ้น

การนำพิกัด GPS เข้ามาช่วยในการติดต่อสื่อสารในระบบเครือข่ายเฉพาะกิจ ทำให้โหนดต้นทางสามารถกำหนดทิศทางการกระจายข้อมูลไปยังโหนดปลายทางในขั้นตอน Route discovery ได้ ดังนั้นผู้วิจัยจึงได้มีแนวคิดในการปรับเปลี่ยนเงื่อนไขในขั้นตอน Route discovery รูปภาพที่ 3 แสดงถึงรูปแบบการจำกัดพื้นที่ของโปรโตคอลใหม่



รูปที่ 3. Proposed protocol scheme

ขั้นตอนการทำงานของโปรโตคอลใหม่นั้นโหนดต้นทางจะต้องทราบถึงพิกัด GPS และความเร็วเฉลี่ยของโหนดปลายทางก่อน โดยจะนำข้อมูลดังกล่าวบรรจุลงไปใน RREQ message เพื่อใช้ในการกำหนดบทบาทให้กับโหนดทุกโหนดในระบบเน็ตเวิร์ค ซึ่งในขั้นแรกจะต้องคำนวณพื้นที่ของ expected zone ก่อน ซึ่งสามารถหาได้จากสมการที่ 1

$$expected\ zone = V_{avg}(t_1 - t_0) \qquad (1)$$

โดยกำหนดให้ V_{avg} คือความเร็วเฉลี่ยของโหนดในระบบเครือข่าย และ $t_1 - t_0$ คือระยะเวลาที่โหนดปลายทางใช้ในการเปลี่ยนตำแหน่ง หลังจากคำนวณ expected zone แล้ว จะนำรัศมีของ *expected zone* มาใช้ในการกำหนดบทบาทให้กับโหนดที่จะทำหน้าที่เป็นตัวกลางในการกระจายข้อมูลหรือเรียกว่า forwarding node ร่วมกับสมการที่ 2 และตรวจสอบว่า forwarding node ใดที่อยู่ในรัศมีของ expected zone จากสมการที่ 3

$$f(x,y) = \left(\frac{y_d}{(x_d+r)^2}\right)x^2 - y$$

เมื่อ (2)

$$f(x,y) \neq 0$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$g(x,y) = (x - x_d^2) + (y - y_d^2) - r^2$$

เมื่อ (3)

$$g(x,y) \neq 0$$

โดยกำหนดให้ x_d, y_d เป็นพิกัดของโหนดปลายทาง x, y เป็นพิกัดของโหนดใดๆบนเน็ตเวิร์ค และ r เป็นรัศมีของ expected zone โดยก่อนการคำนวณ ต้องทำการหมุนและย้ายแกน X และ แกน Y ของโหนดต้นทางให้ตั้งฉากกับโหนดปลายทางก่อน จากนั้นโหนดต้นทางจะเริ่มกระบวนการ Route discovery ซึ่งโหนดทุกตัวในระบบเครือข่ายจะทำการตรวจสอบว่าตัวเองนั้นเป็น Forwarding node หรือไม่ ถ้าใช่จะทำการกระจายข้อมูลต่อ แต่ถ้าไม่ใช่ก็จะทำการดร็อปแพ็คเกตทิ้งไป จนกว่าแพ็คเกตจะไปถึงโหนดปลายทาง จากนั้นโหนดปลายทางจะส่งแพ็คเกต *Route reply* ที่บันทึกข้อมูลของ *forwarding node* ทั้งหมดที่จำเป็นต้องใช้ในการติดต่อตามลำดับกลับมาที่โหนดต้นทางเพื่อสร้างช่องทางการติดต่อสื่อสารกันต่อไป

4. การทดสอบและวิเคราะห์ผล

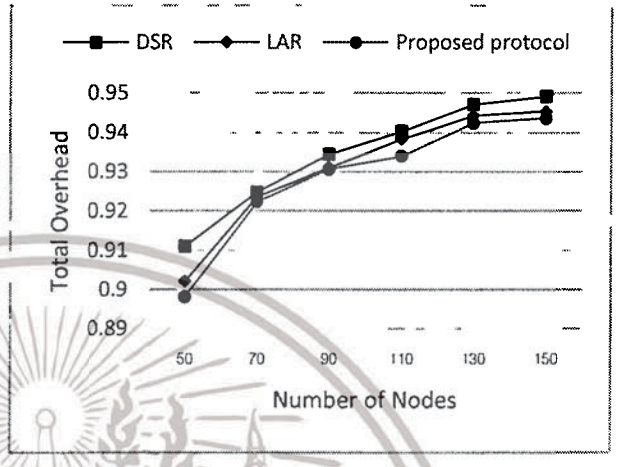
จากที่ได้กล่าวไว้ในบทที่ 3 ผู้วิจัยได้ทำการทดสอบโปรโตคอลที่นำเสนอด้วยโปรแกรมซิมูเลชั่นระบบเครือข่าย OMNET++ โดยเปรียบเทียบผลลัพธ์การทำงานร่วมกับโปรโตคอล DSR และ LAR โดยมีการใช้พารามิเตอร์ในการทดสอบดังตารางที่ 1

ตารางที่ 1 พารามิเตอร์ที่ใช้ในการจำลองเหตุการณ์

พารามิเตอร์	ค่าพารามิเตอร์
ระยะเวลาในการจำลองเหตุการณ์	1000 วินาที
ขอบเขตการกระจายข้อมูลของโหนด	250 เมตร
ความกว้างของพื้นที่ทดสอบ	1000 ตารางเมตร
ระยะเวลาที่ใช้ในการเปลี่ยนองศาการเคลื่อนที่ของโหนด	ใช้การสุ่มแบบ uniform ในช่วง 0-5 วินาที
ขนาดของมุมเมื่อมีการเปลี่ยนองศาการเคลื่อนที่	ใช้การสุ่มแบบ uniform ในช่วง 0-360 องศา
ความเร็วของโหนด	ใช้การสุ่มแบบ uniform ในช่วง 0-20 เมตรต่อวินาที
จำนวนโหนดต้นทาง	10 โหนด
อัตราการส่งข้อมูล	ใช้การสุ่มแบบ uniform ในช่วง 1-5 แพ็คเกตต่อวินาที
ขนาดของแพ็คเกต	64 byte

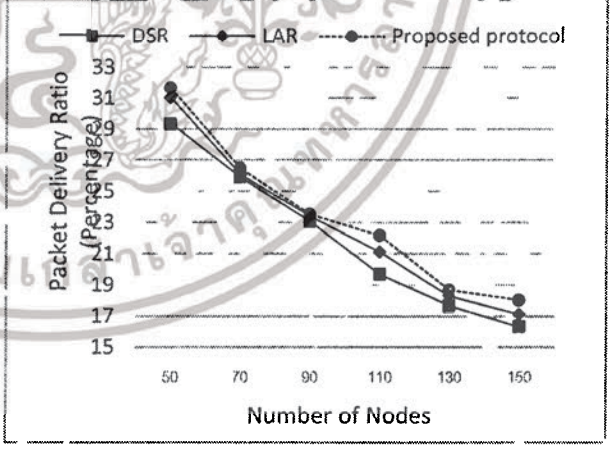
โดยสาเหตุที่ใช้จำนวนโหนดต้นทางมากกว่า 1 โหนดนั้นเนื่องจากผู้วิจัยต้องการให้เกิดการเรียกใช้งานฟังก์ชั่น route cache บนโปรโตคอลที่ใช้ในการทดสอบทั้งสามตัว เนื่องจากโปรโตคอล DSR ไม่มีกลไกอื่นที่สามารถช่วยลดโอเวอร์เฮดได้นอกจากการใช้งานแคชเพียงอย่างเดียว

ในการสรุปผลการทดลองจะใช้ตัวชี้วัดทั้งหมด 4 ประเภทคือ ปริมาณโอเวอร์เฮดในระบบเครือข่าย อัตราความสำเร็จในการส่งข้อมูล ระยะเวลาที่ใช้ในการสร้างเส้นทาง และความล่าช้าในการส่งข้อมูลระหว่างโหนด โดยแสดงผลด้วยกราฟดังต่อไปนี้



รูปที่ 4. กราฟแสงปริมาณโอเวอร์เฮดในระบบเครือข่าย

จากกราฟจะเห็นได้ว่าโปรโตคอลที่นำเสนอสามารถลดจำนวนโอเวอร์เฮดได้เมื่อเปรียบเทียบกับโปรโตคอล DSR และ LAR เนื่องจากการเปลี่ยนเงื่อนไขในการกระจายข้อมูลให้มีความรัดกุมมากยิ่งขึ้นโดยค่าโอเวเวอร์เฮดนั้นเป็นสัดส่วนระหว่างจำนวนแพ็คเกตที่ใช้ในการค้นหาเส้นทางต่อจำนวนแพ็คเกตทั้งหมดที่เกิดขึ้นในระบบเครือข่าย

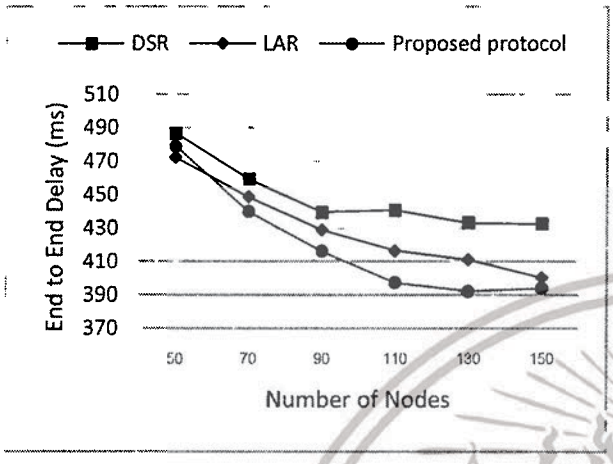


รูปที่ 5. กราฟแสดงอัตราความสำเร็จในการส่งข้อมูล

วิธีการจำกัดพื้นที่ในการกระจายข้อมูลเพื่อลดโอเวอร์เฮดที่นำเสนอนั้นมีจุดประสงค์เพื่อลดจำนวน forwarding node ลง การกำหนดเงื่อนไขเพื่อควบคุมจำนวน forwarding node ให้เหมาะสม จะส่งผลกระทบต่ออัตราความสำเร็จในการส่งข้อมูล จากรูปที่ 5 แสดงให้เห็นว่าโปรโตคอลที่นำเสนอนั้นสามารถช่วยลดโอเวอร์ได้ ในขณะเดียวกันยังช่วยเพิ่มอัตราความสำเร็จในการส่งข้อมูลอีกด้วย ในกรณีของโปรโตคอล LAR และ DSR ที่ทีอัตราความสำเร็จในการส่งข้อมูลน้อยกว่าเนื่องจากโอ

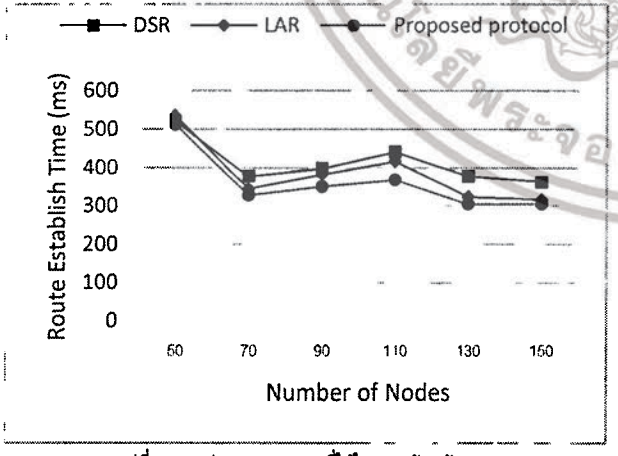
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เวอร์เฮดที่เกิดจากขั้นตอน route discovery ส่งผลกระทบต่อระบบเครือข่ายทำให้เกิดความแออัดในระบบเน็ตเวิร์คจนกระทั่งเกิดการชนกันของข้อมูล ซึ่งเป็นการขัดขวางการส่งข้อมูลจากต้นทางไปยังปลายทาง



รูปที่ 6. กราฟแสดงความล่าช้าในการส่งข้อมูลระหว่างโหนด

ค่าความล่าช้าในการส่งข้อมูลระหว่างโหนดนั้นแปรผันตรงกับความคับคั่งในระบบเน็ตเวิร์ค ในกรณีของโปรโตคอลที่นำเสนอนั้นสามารถลดปริมาณ forwarding node ในระบบเครือข่ายลง ซึ่งช่วยลดปริมาณการจราจรในระบบเน็ตเวิร์คได้ ค่าความล่าช้าที่ลดลงเมื่อจำนวนโหนดเพิ่มมากขึ้นเป็นผลมาจากความหนาแน่นของ forwarding node ที่เพิ่มขึ้น ทำให้ในการส่งต่อข้อมูลไปยังโหนดใกล้เคียงเป็นไปได้รวดเร็วยิ่งขึ้น ผลลัพธ์ในการช่วยลดค่าความล่าช้าในระบบเน็ตเวิร์คของโปรโตคอลสามารถตรวจสอบได้จากรูปที่ 6



รูปที่ 7. กราฟแสดงระยะเวลาที่ใช้ในการสร้างเส้นทาง

จากรูปที่ 7 จะสังเกตได้ว่าในกรณีที่จำนวน forwarding node มีจำนวนน้อย จะต้องใช้ระยะเวลาในการสร้างเส้นทางเป็นจำนวนมาก เนื่องจากการค้นหาโหนดที่จำเป็นต้องใช้ในการติดต่อไปยังปลายทางนั้นเป็นไปได้ยาก เมื่อจำนวน forwarding node เพิ่มขึ้นก็จะส่งผลให้ระยะเวลาในการสร้างเส้นทางลดลง แต่เมื่อโอเวอร์เฮดมีค่าสูงขึ้น ณ จุดหนึ่ง จะทำให้ระยะเวลาในการสร้างเส้นทางเพิ่มขึ้นเนื่องจากความหนาแน่นของระบบเน็ตเวิร์คที่เพิ่มขึ้น และในกรณีที่มีจำนวนโหนดเพิ่มขึ้นถึง 130 โหนดจากการทดสอบ จะสังเกตได้ว่าระยะเวลาในการสร้างเส้นทางค่อยๆลดลง เป็นผลมาจากโอกาสที่ฟังก์ชั่น route cache จะทำงานมีมากขึ้น ซึ่ง route cache นั้น สามารถช่วยลดระยะเวลาในขั้นตอนการทำ route discovery ให้สั้นลงได้

5. บทสรุป

การจำกัดการกระจายข้อมูลในขั้นตอน route discovery โดยการลดจำนวนโหนดที่ทำหน้าที่เป็น forwarding node อย่างเหมาะสม สามารถช่วยลดอัตราการเกิดโอเวอร์เฮดในระบบเครือข่ายไร้สายเฉพาะกิจ และยังคงรักษาประสิทธิภาพของระบบเครือข่ายเอาไว้ได้ แต่อย่างไรก็ตามผลการทดลองยังคงแสดงให้เห็นว่าประสิทธิภาพในการลดโอเวอร์เฮดของโปรโตคอลที่นำเสนอนั้นยังไม่ส่งผลต่อระบบเครือข่ายไร้สายเฉพาะกิจอย่างมีนัยสำคัญ และเนื่องจากเงื่อนไขที่ใช้ในการจำกัดการกระจายข้อมูลในรายงานฉบับนี้ จะลดปริมาณ forwarding node ในบริเวณรอบข้างโหนดต้นทางเป็นจำนวนมาก ซึ่งอาจก่อให้เกิดปัญหาเมื่อไม่มีโหนดใดๆ มารับข้อมูลจากโหนดต้นทางเลย เป็นสาเหตุให้การสร้างช่องทางในการติดต่อสื่อสารในระบบเครือข่ายนั้นล้มเหลว

ในส่วนของปัญหาดังกล่าว ผู้วิจัยมีแนวคิดที่จะปรับเปลี่ยนเงื่อนไขในการจำกัดการกระจายตัวข้อข้อมูลให้มีความยืดหยุ่นมากยิ่งขึ้น และเพื่อให้โปรโตคอลใหม่นั้น สามารถลดปริมาณโอเวอร์เฮดในระบบเครือข่ายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

เอกสารอ้างอิง

[1] Sunil taneja and Ashwani kush." A survey of routing protocols in mobile ad hoc networks". international journal of innovation, management and technology, vol. 1, no. 3, august, 2010.

[2] S. Sen and J. Wang. "Analyzing Peer-to-Peer Traffic Across Large Networks", *Proc. Internet Measurement Workshop, Proc. Internet Measurement Workshop, 2002.*

[3] Young-Bae Ko and Nitin H. Vaidya. "Location-Aided Routing (LAR) in mobile Ad Hoc Networks". September, 2000.

[4] Johnson, D., Maltz, D., Broch, J., DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, 2001.

[5] Ghaith Bader Al-Suwaidi, Mohamed Jamal Zemerly. "Locating Friend and Family Using Mobile Phones with Global Positioning System (GPS)". 2009 IEEE, 2009.

[6] R. Bajaj, S. L. Ranaweera and D. P. Agrawal, "GPS: Location-Tracking Technology", IEEE Computer, Vol. 35, No. 4, 2002, pp. 92-94.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การปรับปรุงกลไกการแพร่กระจายข้อความ เพื่อลดการแลกเปลี่ยนข้อมูล บนเครือข่ายดีทีเอ็น

ธีรพงษ์ โชคสถิตย์, เบญจพร ปาวะรีย์, วรวัชร ณรงคะชวนะ และ สุเมธ ประภาวัต

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: TeerapongC@outlook.com, benjabhon@gmail.com, worravat@gmail.com, sumet@it.kmitl.ac.th

บทคัดย่อ

เราจะทำอย่างไร หากคุณต้องการใช้โทรศัพท์มือถือเพื่อแจ้งข่าวไปยังเพื่อนที่อยู่ไกลออกไป แต่เสากระจายสัญญาณกลับใช้การไม่ได้ ทางออกของจุดวิกฤตนี้คือ สร้างเครือข่ายสื่อสารเฉพาะกิจ เก็บและส่งต่อข้อความจากโทรศัพท์มือถือเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ซึ่งในทางปฏิบัติ กระบวนการดังกล่าวทำให้เครือข่ายต้องรองรับข้อความจำนวนมาก ส่งผลให้เกิดความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสาร และการที่โทรศัพท์มือถือต้องสูญเสียพลังงานในการส่งข้อความ ทำให้จำนวนโทรศัพท์มือถือที่สามารถช่วยส่งต่อข้อความลดลงอย่างต่อเนื่อง เพราะฉะนั้นการพัฒนา n-Anti Entropy ซึ่งได้ดัดแปลงข้อดีของ Anti Entropy และ n-Epidemic โดยผลการทดสอบในโมเดลจำลองแสดงให้เห็นว่า n-Anti Entropy มีแนวโน้มในการแก้ไขปัญหาข้างต้นได้ดีกว่ากลยุทธ์การส่งข้อความรูปแบบอื่นๆซึ่งสะท้อนให้เห็นถึงประสิทธิภาพของการสื่อสารในสถานการณ์จริงได้เป็นอย่างดี

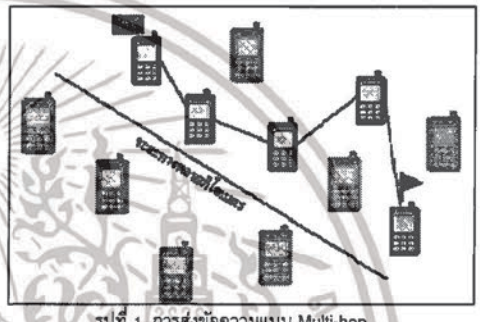
คำสำคัญ– เครือข่ายเฉพาะกิจ; เครือข่ายดีทีเอ็น; Anti Entropy; การแพร่กระจายข้อมูล; ลดการแลกเปลี่ยนข้อมูล

1. บทนำ

ระบบสื่อสารเป็นสิ่งจำเป็น เพราะในทุกๆกิจกรรมที่เกิดขึ้นในการดำรงชีวิตล้วนมีความเกี่ยวข้องกับการสื่อสารไม่มากก็น้อย ในขณะที่โลกกำลังก้าวข้ามผ่านการสื่อสารแบบเก่า ไปสู่โลกแห่งการสื่อสารไร้สาย นักพัฒนาก็กำลังสร้างเครือข่ายสื่อสารเฉพาะกิจ ที่อนุญาตให้อุปกรณ์สื่อสารต่างๆสามารถติดต่อระหว่างกันได้โดยตรง

ในบทความนี้ ผู้เขียนให้ความสนใจกับเครือข่ายที่มีความคงทนต่อความหน่วง (DTN : Delay Tolerant Network) ซึ่งเป็นเครือข่ายสื่อสารเฉพาะกิจ (Ad Hoc Network) ถูกออกแบบสำหรับแก้ไขปัญหาต้นทางไม่สามารถคาดการณ์ได้ว่าจะพบปลายทางได้เมื่อใด โดยอาศัยกระบวนการเก็บและส่งต่อข้อความ (Store-and-Forward Message Switching) เป็นการส่งข้อความไปกับอุปกรณ์อื่นๆหลายต่อ (Multi-hop) จนกระทั่งถึงปลายทาง[1] ดังรูปที่ 1 แสดงให้เห็นว่า ยิ่งสามารถแพร่กระจายข้อความไปได้มากเท่าไร โอกาสที่ข้อความถูกส่งไปยังโหนดปลายทางก็เพิ่มมากขึ้นเท่านั้น

ถึงแม้การสื่อสารบนเครือข่ายดีทีเอ็นมีความยืดหยุ่นมาก แต่ก็แลกมาด้วยโจทย์หลายข้อที่เป็นอุปสรรคต่อประสิทธิภาพในการแพร่กระจายข้อความ ในบทความนี้ผู้เขียนให้ความสนใจกับโจทย์สองข้อได้แก่ ความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสาร และแหล่งพลังงานที่จำกัดของอุปกรณ์สื่อสาร ซึ่งโจทย์ทั้งสองมักพบบนเครือข่ายสื่อสารเฉพาะกิจที่มีการส่งข้อมูลแบบบรอดแคสต์ (Broadcast) ด้วยเหตุนี้จึงนำไปสู่แนวคิดในการพัฒนากลยุทธ์การส่งข้อความ (Routing Strategies) เพื่อแก้ไขโจทย์ทั้งสองข้อ โดยไม่ส่งผลกระทบต่อประสิทธิภาพในการแพร่กระจายข้อความจนทำให้การสื่อสารของเครือข่ายล้มเหลว



รูปที่ 1. การส่งข้อความแบบ Multi-hop

หัวข้อต่อไปที่จะกล่าวถึงงานวิจัยต่างๆที่เกี่ยวข้อง ตามด้วยหัวข้อแนวทางการพัฒนา ซึ่งนำเสนอกลยุทธ์การส่งข้อความที่ได้พัฒนาขึ้น โดยกลยุทธ์ดังกล่าวถูกนำมาเปรียบเทียบกับกลยุทธ์ชนิดอื่นๆในหัวข้อการวิเคราะห์และประเมินผล และหัวข้อสุดท้ายเป็นการอภิปรายถึงบทสรุปการพัฒนา

2. งานวิจัยที่เกี่ยวข้อง

ความท้าทายของเทคโนโลยีเครือข่ายดีทีเอ็นคือ การสร้างกลยุทธ์การส่งข้อความ บนเครือข่ายที่ไม่สามารถทราบได้ถึงการเชื่อมต่อระหว่างโหนดใดๆ เพื่อสร้างเส้นทางการสื่อสารจากต้นทางไปยังปลายทางได้เลย ซึ่ง Jones E., Li L., Schmidtke J. และ Ward P. ได้เสนอกลยุทธ์การส่งข้อความเพื่อแก้ไขจุดบกพร่องดังกล่าว โดยใช้ข้อมูลจากเครือข่ายประมาณเวลาที่ข้อความบนโหนดจะถูกส่งต่ออีกครั้ง[2] นอกจากนั้น Jones E. และ Ward P. ได้ศึกษารวบรวมกลยุทธ์ในการส่งข้อความหลากหลายรูปแบบ ที่ได้ถูกสร้างขึ้นมาเพื่อแก้ไขโจทย์หัวข้อต่างๆ ซึ่ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เป็นอุปสรรคต่อการสื่อสารบนเครือข่ายดีทีเอ็น [3] เช่น Tree-Based Flooding, Epidemic Routing, Link Metrics เป็นต้น

ในสถานการณ์การสื่อสารปกติของเครือข่ายดีทีเอ็น นิยมใช้กลยุทธ์การส่งข้อความแบบฟลัด ที่อาศัยการคัดลอกข้อความส่งไปยังโหนดเพื่อนบ้านโดยรอบ เพื่อเพิ่มประสิทธิภาพในการแพร่กระจายข้อความ ซึ่งหมายถึงโอกาสที่ข้อความจะถูกส่งต่อไปยังโหนดปลายทางมีโอกาสมากขึ้น เมื่อเปรียบเทียบกับกลยุทธ์รูปแบบอื่น แต่ทั้งนี้กลยุทธ์ดังกล่าวก็เป็นต้นเหตุให้เกิดความคับคั่งของปริมาณข้อความบนเส้นทางการสื่อสาร นอกจากนี้การส่งข้อมูลแบบบรอดแคสต์ของอุปกรณ์ไร้สาย ยังทำให้พลังงานในแหล่งพลังงานสำรองสูญเสียไปกับการเคลื่อนที่ของโหนด และการส่งข้อความจำนวนมากเกินความจำเป็น

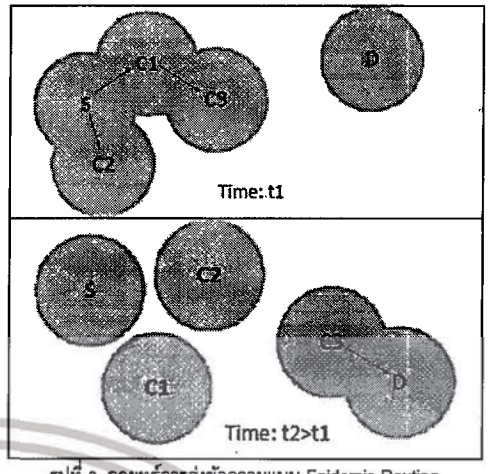
Epidemic Routing มีวิธีการส่งข้อความชนิดหนึ่งเรียกว่า Anti Entropy ซึ่งมีจุดประสงค์เพื่อลดความคับคั่งของปริมาณข้อความบนเส้นทางการสื่อสาร โดย Alan D. และคณะ ได้เสนอแนวคิดให้โหนดมีการแลกเปลี่ยนรายชื่อของข้อความ เพื่อตรวจสอบสถานะ ก่อนการส่งข้อความจริง[4] หลังจากนั้น Anti Entropy ก็มีการพัฒนาอย่างต่อเนื่องจนกระทั่ง Vahdat A., Becker D. และ คณะ ได้พัฒนากระบวนการดังกล่าว ให้เหมาะสมกับการใช้งานมากขึ้น โดยให้โหนดร้องขอเฉพาะข้อความที่ตนเองต้องการได้ [5]

แต่อย่างไรก็ตามการลดปริมาณการสูญเสียพลังงานของโหนด ก็เป็นอีกหนทางหนึ่งในการแก้ไขปัญหา จากการศึกษา n-Epidemic Routing ของ Lu X. และ Pan H. ซึ่งมีแนวคิดที่จะลดจำนวนครั้งการส่งข้อความ โดยการกำหนดให้มีการส่งข้อมูลแบบบรอดแคสต์ เมื่อมีโหนดเพื่อนบ้านครบตามจำนวนที่กำหนด เงื่อนไขดังกล่าวส่งผลให้การสูญเสียพลังงานจากการส่งข้อมูลลดลง อีกทั้งยังทำให้การส่งแต่ละครั้งมีโหนดที่ได้รับข้อความเพิ่มมากขึ้น[6] นอกจากนี้ De R. และ Amelio S. ยังได้พัฒนาต่อยอดให้ n-Epidemic Routing มีกลไกในการเลือกส่งต่อข้อความ (Dynamic Forwarding) โดยพิจารณาจากความหนาแน่นของโหนดในแต่ละกลุ่มเป็นสำคัญ[7]

และเพื่อเป็นการพิสูจน์ว่า ประสิทธิภาพการกระจายข้อความของกลยุทธ์การส่งข้อความที่นำเสนอ ไม่ได้ลดลงไปจากกลยุทธ์ต้นแบบ ในหัวข้อการวิเคราะห์และประเมินผล จึงได้มีการนำสัดส่วนของจำนวนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา เมื่อเทียบกับจำนวนโหนดทั้งหมด ของแต่ละกลยุทธ์การส่งข้อความ มาแสดงผลเปรียบเทียบในรูปแบบของกราฟ ซึ่งการเปรียบเทียบลักษณะนี้ถูกใช้สำหรับการวิเคราะห์และประเมินผลในหลากหลายบทความ[5][6][7] โดยสัดส่วนโหนดที่ได้รับข้อความในช่วงเวลา t สามารถคำนวณได้จากสูตร

$$R(t) = \frac{m(t)}{Node} \quad (1)$$

โดย $R(t)$ = สัดส่วนโหนดที่ได้รับข้อความในช่วงเวลา t
$m(t)$ = จำนวนโหนดทั้งหมดที่ได้รับข้อความ ณ เวลา t
$Node$ = จำนวนโหนดทั้งหมด



รูปที่ 2. กลยุทธ์การส่งข้อความแบบ Epidemic Routing

3. แนวทางการพัฒนา

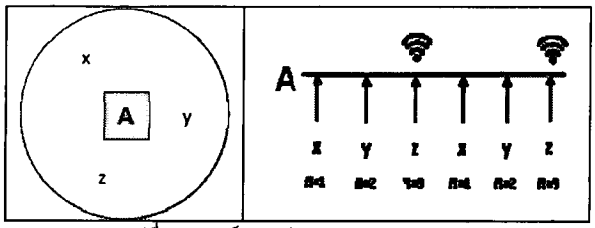
Epidemic Routing เป็นรูปแบบหนึ่งของกลยุทธ์การส่งข้อความแบบฟลัด ซึ่งอนุญาตให้โหนดคู่หนึ่งเชื่อมต่อกันเพื่อแลกเปลี่ยนข้อความของทั้งสองฝ่ายให้เหมือนกัน(Synchronize) โดยแต่ละข้อความจะถูกแลกเปลี่ยนไปเรื่อยๆ จนกระทั่งถึงโหนดปลายทาง อธิบายรูปแบบการทำงานตามรูปที่ 2 จากภาพแสดงให้เห็นว่ามีการแบ่งกลุ่มของโหนด ทำให้โหนด S ไม่สามารถส่งข้อความไปให้โหนด D ซึ่งอยู่คนละกลุ่มได้ ทำให้ที่เวลา t1 โหนด S จึงเพิ่มสัดส่วนโหนดที่ได้รับข้อความ โดยฝากข้อความดังกล่าวไปกับโหนด C1 C2 จากนั้นโหนด C1 จึงฝากข้อความไปให้โหนด C3 ตามลำดับ และที่เวลา t2>t1 โหนดต่างๆในเครือข่ายมีการเคลื่อนที่ ทำให้โหนด C3 อยู่ในระยะการสื่อสารของโหนด D ข้อความจึงถูกส่งไปถึงโหนด D ซึ่งเป็นโหนดปลายทางสำเร็จ

ดังที่กล่าวไปในหัวข้องานวิจัยที่เกี่ยวข้อง ผู้เขียนให้ความสนใจกับ Anti Entropy ซึ่งลดความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสารด้วยการส่งเฉพาะข้อความที่ได้รับการร้องขอ (Partial Message) และ n-Epidemic ที่สร้างเงื่อนไขให้การส่งข้อมูล เพื่อลดปริมาณการใช้พลังงาน (อายุของโหนดเพิ่มขึ้น) อีกทั้งผลลัพธ์ของทั้งสองกลยุทธ์ต่างทำให้ปริมาณข้อความที่ถูกส่งต่อทั้งหมดในเครือข่ายลดลง ดังนั้นผู้เขียนจึงนำเสนอกลยุทธ์การส่งข้อความใหม่ที่พัฒนาต่อเนื่องจาก n-Epidemic โดยอาศัยเทคนิคการส่งเฉพาะข้อความที่ถูกร้องขอของ Anti Entropy (n-Epidemic with Anti Entropy) โดยเรียกแบบย่อว่า n-Anti Entropy ซึ่งประกอบไปด้วยส่วนการทำงานหลัก ดังนี้

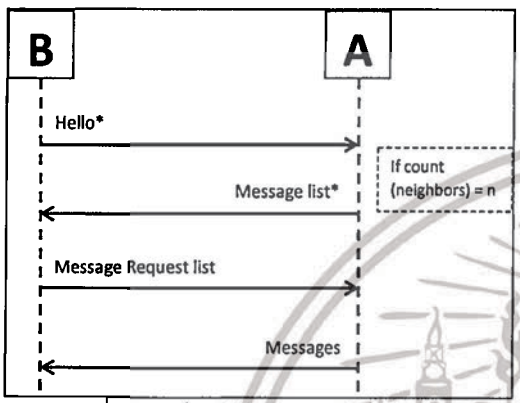
3.1 ส่วนกระบวนการก่อนส่งข้อความ

การทำงานในส่วนนี้ ใช้ประโยชน์จาก n-Epidemic ซึ่งจะเริ่มการส่งข้อมูลเมื่อโหนดมีจำนวนโหนดเพื่อนบ้านครบตามที่กำหนด ทำให้ไม่จำเป็นต้องส่งข้อมูลทุกครั้งที่พบโหนดอื่นๆในเครือข่าย โดยn-Epidemic อาศัยการส่งข้อมูลแบบบรอดแคสต์ ทำให้ในการส่งเพียงหนึ่งครั้ง โหนดเพื่อนบ้านจะได้รับข้อมูลทั้งหมด ส่งผลให้พลังงานที่โหนดสูญเสียไปกับการส่งข้อมูลแต่ละครั้งลดลง ตามรูปที่ 3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3. กลยุทธ์การส่งข้อความแบบ n-Epidemic



รูปที่ 4. กลยุทธ์การส่งข้อความแบบ n-Anti Entropy

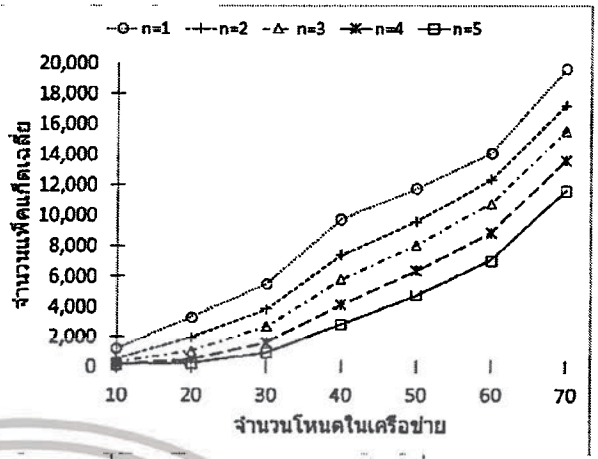
รูปที่ 4 อธิบายการทำงานที่ได้รับการพัฒนาขึ้น โดยกำหนดให้ ณ ช่วงเวลาหนึ่ง โหนด A มีโหนด x y และz เป็นโหนดเพื่อนบ้าน เมื่อโหนด A พบว่ามีโหนดเพื่อนบ้านครบ 3 โหนดตามที่ได้กำหนดไว้ หลังจากนั้นโหนด A ก็จะบรอดแคสต์ข้อมูลออกมาและเริ่มรอคอยโหนดเพื่อนบ้านใหม่อีกครั้ง

3.2 ส่วนคัดเลือกและส่งต่อข้อความ

โดยปกติในกระบวนการส่งข้อความ โหนดจำเป็นต้องส่งข้อความทั้งหมด เพราะไม่ทราบว่าโหนดที่กำลังติดต่อด้วยต้องการข้อความอะไรบ้าง ซึ่งเมื่อปริมาณข้อความภายในโหนดต่างๆบนเครือข่ายเพิ่มมากขึ้น ความคับคั่งของปริมาณข้อมูลบนเส้นทางการสื่อสารก็เกิดขึ้นอย่างหลีกเลี่ยงไม่ได้ แต่ทว่ากระบวนการส่งข้อมูลด้วย Anti Entropy ทำให้โหนดส่งเฉพาะข้อความที่โหนดเพื่อนบ้านต้องการเท่านั้น ปริมาณข้อมูลที่ต้องถูกส่งในแต่ละครั้งจึงลดลงอย่างมาก โดยหลักการทำงานที่ได้รับการพัฒนาเพื่อรองรับการทำงานต่อจากส่วนรอคอยการติดต่อจากโหนดเพื่อนบ้าน สามารถอธิบายการทำงานได้ตามรูปที่ 4 โดยแรกเริ่มโหนดแต่ละโหนดจะบรอดแคสต์ Hello แพ็คเก็ตออกไป เพื่อเป็นสัญญาณให้โหนดอื่นๆรู้ถึงการมีอยู่ของตน จากนั้นเมื่อโหนด A ได้รับสัญญาณจากโหนดต่าง ๆ ครบตามจำนวนที่กำหนด โหนด A จะบรอดแคสต์รายชื่อข้อความ (Message List) ที่มีออกไป และส่งข้อความ (Messages) ไปให้แต่ละโหนดตามที่ระบุไว้ในรายชื่อข้อความที่แต่ละโหนดต้องการ (Message Request List)

3.3 จำนวนข้อความทั้งหมดของ n-Anti Entropy

ดังที่กล่าวไปก่อนหน้านี้ การที่ผลรวมของจำนวนข้อความที่ถูกส่งออกของโหนดทั้งหมดในเครือข่ายลดลง ย่อมหมายถึงการที่โหนดทั้งหมดมีจำนวนข้อมูลที่ส่งในแต่ละครั้ง หรือจำนวนครั้งการส่งข้อมูลลดลงตามไปด้วย เพราะฉะนั้นจากการที่ n-Anti Entropy ซึ่งได้นำส่วนที่ดีของ n-Epidemic และ Anti Entropy มาทำงานร่วมกัน แสดงให้เห็นว่าการลดลงของจำนวนดังกล่าว ส่งผลให้ความคับคั่งของข้อมูลบนเส้นทางการสื่อสารได้รับการแก้ไขหรือบรรเทาลง ในขณะเดียวกันการสูญเสียพลังงานอันเนื่องมาจากการส่งข้อมูลของโหนดก็ลดลงเช่นกัน



รูปที่ 5. กราฟแสดงผลรวมของจำนวนแพ็คเก็ตที่ถูกส่งออก

ผลรวมของจำนวนข้อความที่ถูกส่งออกของโหนดทั้งหมดในเครือข่าย สามารถคำนวณได้จากสูตร

$$\text{sumPacket} = \sum_{i=1}^{m} f(i) \quad (2)$$

โดย sumPacket = ผลรวมของจำนวนแพ็คเก็ตที่ถูกส่งออก

m = จำนวนครั้งการส่งข้อความทั้งหมด

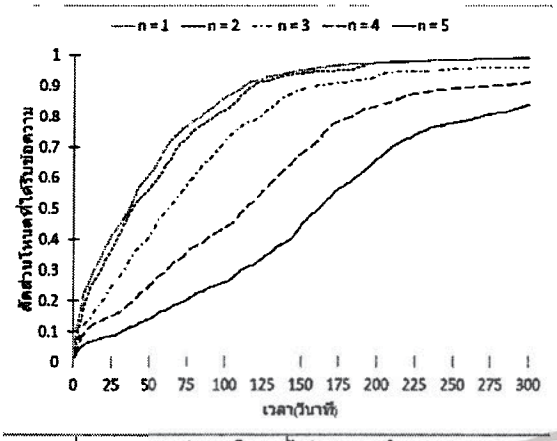
$f(i)$ = ขนาดข้อความที่ถูกส่ง ในการส่งครั้งที่ i ในหน่วยแพ็คเก็ต

รูปที่ 5 กราฟแสดงผลรวมของจำนวนแพ็คเก็ตเฉลี่ย ที่ถูกส่งออกไปในเครือข่าย เพื่อให้ทุกโหนดได้รับข้อความทั้งหมด ในช่วงเวลาที่น้อยที่สุดเปรียบเทียบกับจำนวนโหนดในเครือข่าย โดยกราฟแต่ละเส้นมีความแตกต่างกันตามจำนวนการรอคอยสัญญา (Hello) จากโหนดเพื่อนบ้าน โดยปกติการเพิ่มจำนวนของโหนดในกราฟแต่ละเส้นย่อมทำให้จำนวนแพ็คแก็ตที่ถูกส่งออกเพิ่มสูงขึ้น แต่จากการที่ n-Anti Entropy มีการสร้างเงื่อนไขให้โหนดต้องรอคอยสัญญาณจากโหนดเพื่อนบ้านส่งผลให้จำนวนแพ็คแก็ตที่ถูกส่งออกลดลงตามจำนวนการรอคอยสัญญาณที่เพิ่มขึ้น

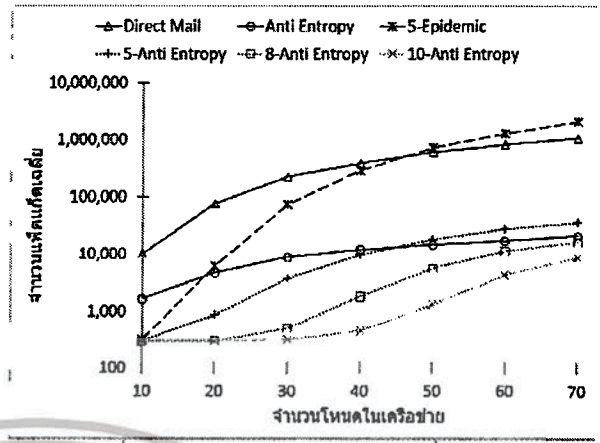
3.4 อัตราการกระจายข้อความของ n-Anti Entropy

เมื่อพิจารณา n-Anti Entropy การลดลงของผลรวมของจำนวนแพ็คแก็ตที่ถูกส่งออก สามารถพิสูจน์ได้จากรูปที่ 5 แต่ทั้งนี้เพื่อเป็นการตรวจสอบเพิ่มเติมถึงความถูกต้องของแบบจำลองที่สร้างขึ้น จึงได้มีการสร้างกราฟแสดงถึงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา ที่มีการกำหนดสภาพแวดล้อมของเครือข่ายตามบทความ[6] โดยกราฟในรูปที่ 6 แสดง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 6. กราฟแสดงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา



รูปที่ 7. กราฟแสดงผลรวมของจำนวนแพ็คเก็ตที่ถูกส่งออก

ตารางที่ 1. ตารางแสดงสภาพแวดล้อมของเครือข่าย

จำนวนโหนด	30-70 โหนด
ขนาดของพื้นที่	1500 x 300 m^2
รัศมีการสื่อสารของโหนด	100 m
อัตราเร็วในการเคลื่อนที่ของโหนด	0-20 m/s
ความยาวของข้อความ	1 KB
อัตราการส่งสัญญาณของโหนด	ทุก 1 วินาที
เวลาที่ใช้ในการทดสอบ	300 วินาที

ให้เห็นว่า กราฟดังกล่าวมีลักษณะคล้ายคลึงกับกราฟสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลาในบทความที่อ้างอิง นอกจากนี้จากการศึกษาลักษณะของกราฟทั้งสองพบว่า ความชันเส้นกราฟแต่ละเส้นที่ลดลง มีความสัมพันธ์โดยตรงกับการเพิ่มขึ้นของจำนวนสัญญาณที่ต้องรอคอยก่อนการส่งข้อความ หรือกล่าวได้อีกนัยหนึ่งคือ การที่โหนดต้องรอคอยสัญญาณจากโหนดเพื่อนบ้านมากขึ้น ส่งผลอัตราการแพร่กระจายข้อความให้ทั่วทั้งเครือข่ายใช้เวลานานขึ้น

4. วิเคราะห์และประเมินผล

เพื่อพิสูจน์ว่า n-Anti Entropy มีผลรวมของจำนวนข้อความที่ส่งออกไปยังเครือข่ายน้อยกว่ากลยุทธ์ต้นแบบ ซึ่งประกอบไปด้วย Epidemic (Direct Mail) , Anti Entropy และn-Epidemic จึงได้มีการสร้างแบบจำลองของกลยุทธ์การส่งข้อความทั้ง 4 รูปแบบ ควบคู่ไปกับการศึกษาบทความของ Grasic S. และ Anders L. ที่ได้ศึกษาและพัฒนาโมเดล สำรับใช้ในการทดสอบกลยุทธ์การส่งข้อความของเครือข่ายดีทีเอ็น โดยมุ่งหวังให้การทดสอบมีความคล้ายคลึงกับการนำกลยุทธ์ดังกล่าวไปใช้สำหรับการสื่อสารในสถานการณ์จริงมากที่สุด[8]

4.1 สภาพแวดล้อมของเครือข่ายที่ใช้ในการทดสอบ

ในการทดสอบครั้งนี้ได้มีการกำหนดตามสถานการณ์การสื่อสารจากบทความ[5] ที่มีการทดสอบอัตราการแพร่กระจายข้อความของ Anti Entropy ในหลากหลายสถานการณ์ อีกทั้งสถานการณ์การสื่อสารจากบทความนี้ยังถูกใช้ในบทความอื่นๆ[9] ซึ่งการกำหนดสภาพแวดล้อมของเครือข่ายของสถานการณ์การสื่อสาร ที่ใช้ในการทดสอบถูกระบุไว้ในตารางที่ 1 ดังนี้

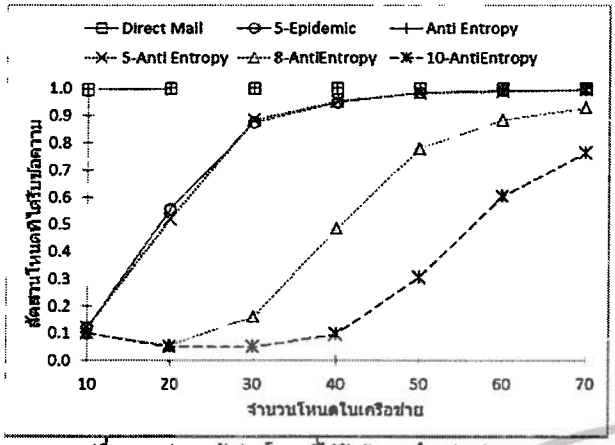
เพื่อให้การทดสอบแบบจำลอง มีความสอดคล้องกับการสื่อสารในสถานการณ์จริงมากที่สุด จึงได้มีการกำหนดให้ 90% ของโหนดทั้งหมดมีการสร้างข้อความเพื่อส่งถึงกันและกัน ส่วนโหนดอีก 10% ที่เหลือจะไม่มีการสร้างข้อความแต่ยังคงสามารถทำหน้าที่เป็นโหนดถ่ายทอดได้ ยกตัวอย่างเช่น มีโหนดทั้งหมดในเครือข่าย 50 โหนด เพราะฉะนั้นมีโหนดที่สามารถสร้างข้อความได้จำนวน 45 โหนด โดยโหนดที่ 1 จะสร้างข้อความจำนวน 44 ข้อความ เพื่อส่งไปหาโหนด 2-45 ส่วนโหนด 46-50 จะไม่มีการสร้างข้อความใดๆทั้งสิ้น ดังนั้นในการทดสอบในเครือข่าย 50 โหนด จะมีข้อความถูกสร้างทั้งหมด 1980 ข้อความ นอกจากนั้นเพื่อเป็นการหลีกเลี่ยงโอกาสที่โหนดจะส่งข้อความชนกัน จึงมีการกำหนดค่าความหน่วงในการส่งข้อความเท่ากับ 0.01 วินาที

4.2 กราฟแสดงผลรวมของจำนวนแพ็คเก็ต กับจำนวนโหนดในเครือข่าย

จากรูปที่ 7 แสดงให้เห็นว่า Direct Mail มีระดับจำนวนแพ็คเก็ตสูงที่สุด เนื่องจากการที่โหนดส่งข้อความทั้งหมดที่ตนมี เมื่อมีการแลกเปลี่ยนข้อมูลเกิดขึ้น ซึ่งระดับดังกล่าวถูกทำให้ลดลงด้วย Anti Entropy ที่อนุญาตให้โหนดส่งเฉพาะข้อความที่ถูกร้องขอเท่านั้น และเมื่อไม่นานมานี้ n-Epidemic ได้มีการเสนอแนวคิดที่น่าสนใจ เพื่อลดจำนวนครั้งการส่งข้อความ ซึ่งจากกราฟแสดงให้เห็นว่า สามารถลดจำนวนแพ็คเก็ตได้อย่างมาก เมื่อมีการกำหนดจำนวนโหนดที่ต้องรอคอยให้เหมาะสมกับจำนวนโหนดในเครือข่าย

เนื่องจาก n-Anti Entropy เป็นกลยุทธ์การส่งข้อความที่ได้รวมเอาข้อดีของ Anti Entropy และ n-Epidemic ทำให้จำนวนแพ็คเก็ตที่ถูกส่งออกไปในเครือข่ายน้อยกว่ากลยุทธ์อื่นๆที่เปรียบเทียบ และเมื่อมีการเพิ่มจำนวนโหนดเพื่อนบ้านของ n-Anti Entropy ก็ยิ่งทำให้ระดับของจำนวนแพ็คเก็ตลดลงมากยิ่งขึ้น แต่เมื่อพิจารณาจุดที่เครือข่ายมีโหนดมากกว่า 50 โหนด เส้นกราฟ 5-Anti Entropy จะมีจำนวนแพ็คเก็ตมากกว่า Anti Entropy ซึ่งแสดงให้เห็นว่า การนำ n-Anti Entropy มาใช้ในการสื่อสารเพื่อลดจำนวนแพ็คเก็ตที่ถูกส่งออกไปยังเครือข่าย จำเป็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 8. กราฟแสดงสัดส่วนโหนดที่ได้รับข้อความในแต่ละช่วงเวลา

ต้องรักษาสมดุลระหว่างจำนวนโหนดที่รอคอยกับจำนวนโหนดในเครือข่ายให้สอดคล้องกันมากที่สุด

4.3 กราฟแสดงสัดส่วนของจำนวนโหนดที่ได้รับข้อความ กับจำนวนโหนดในเครือข่าย

ในรูปที่ 8 กราฟแสดงให้เห็นถึงสัดส่วนของโหนดที่ได้รับข้อความครบต่อโหนดทั้งหมดในเครือข่าย ในช่วงเวลาหนึ่งๆซึ่งจากการพิจารณากราฟแต่ละเส้นสามารถสรุปได้ว่า เมื่อหยุดการจำลองวินาทีที่ 300 วินาที โหนดทั้งหมดในเครือข่ายที่ใช้กลยุทธ์การส่งข้อความแบบDirect Mail และAnti Entropy ได้รับข้อความครบทั้งหมด หรืออีกนัยหนึ่งหมายความว่าข้อความถูกส่งไปยังปลายทางครบทั้งหมดแล้ว แต่สำหรับ n-Epidemic และn-Anti Entropy สัดส่วนของโหนดที่ได้รับข้อความจะเพิ่มขึ้นตามความหนาแน่นของโหนด อีกทั้งการเพิ่มจำนวนโหนดเพื่อนบ้านที่ต้องรอคอย ส่งผลให้ความชันของสัดส่วนโหนดที่ได้รับข้อความเมื่อเทียบกับความหนาแน่นของโหนดลดลง

ปรากฏการณ์การเปลี่ยนแปลงสัดส่วนโหนดที่ได้รับข้อความของn-Epidemic และn-Anti Entropy สามารถอธิบายได้จากทฤษฎีการเชื่อมต่อของกราฟ (Connectivity Graph Theory) ซึ่งมีความคล้ายคลึงกับการทำงานของกลยุทธ์ทั้งสอง ถ้าเปรียบโหนดในเครือข่ายเป็นจุดบนกราฟ การเชื่อมต่อกันของโหนดคู่หนึ่งก็เปรียบเสมือนเส้นที่เชื่อมจุดหนึ่งไปยังอีกจุดหนึ่ง การที่กลยุทธ์มีการกำหนดจำนวนโหนดเพื่อนบ้าน(เชื่อมต่อ)ที่ต้องรอคอย ก็เปรียบเสมือนกราฟต้องมีเชื่อมต่อของจุดจำนวนหนึ่งด้วยเช่นกัน เพราะฉะนั้นจากกราฟจะสังเกตได้ว่า การที่จะทำให้กลยุทธ์ที่กำหนดจำนวนโหนดเพื่อนบ้านไว้สูง มีสัดส่วนของโหนดที่ได้รับข้อความเยอะ จำเป็นต้องอาศัยเครือข่ายที่มีความหนาแน่นของโหนดมากพอในระดับหนึ่งเช่นกัน นอกจากนั้นปัญหาดังกล่าวยังเป็นปัญหาเบื้องต้นในการออกแบบเครือข่ายเซ็นเซอร์ไร้สาย (Wireless Sensor Network) Gu X. และ Hailin F. ได้อธิบายไว้ว่า การทำให้โหนดใดๆเชื่อมต่ออยู่กับเครือข่ายนานที่สุดเท่าที่จะทำได้ คือรากฐานสำคัญในการออกแบบเครือข่ายเซ็นเซอร์ไร้สาย ซึ่งเป็นไปไม่ได้สำหรับโหนดในพื้นที่การสื่อสารขนาดใหญ่ และมีการการกระจายตัวที่ไม่สามารถคาดเดาได้ แต่อย่างไรก็ตามในสถานการณ์จริง ความเป็นไปไม่ได้มักเป็นไปได้ เพราะเราเพียงแค่ต้องการโหนดจำนวนหนึ่ง ซึ่งมากเพียงพอสำหรับสร้างเส้นทางการสื่อสาร เพื่อส่งข้อความจากโหนดหนึ่งไปยังอีกโหนดหนึ่งที่อยู่ใกลออกไปเท่านั้น[10]

จากกราฟในรูปที่ 7 เมื่อสังเกต 8-Anti Entropy ก่อนจำนวนโหนดในเครือข่ายจะมากกว่า 70 โหนด จำนวนแพ็คแก็ตยังคงน้อยกว่ากลยุทธ์รูปแบบอื่นๆ(จำนวนแพ็คแก็ตเข้าใกล้ Anti Entropy) ซึ่งเมื่อพิจารณาสัดส่วนของโหนดที่ได้รับข้อความ ในกราฟรูปที่ 8 เมื่อมีโหนดในเครือข่าย 60 โหนด จะพบว่า 8-Anti Entropy มีสัดส่วนมากกว่า 80% ทั้งที่ในขณะเดียวกัน 10-Anti Entropy ยังมีสัดส่วนที่ต่ำมาก และถึงแม้ว่า 5-Anti Entropy จะมีค่าเข้าใกล้ 100% แต่จำนวนแพ็คแก็ต(รูปที่7) ก็มีค่ามากกว่า Anti Entropy อย่างมาก ซึ่งกรณีดังกล่าวเป็นตัวอย่างการกำหนดโหนดเพื่อนบ้านให้มีความสอดคล้องกับโหนดในเครือข่ายของ n-Anti Entropy

5. สรุปการพัฒนา

ถ้าในเครือข่ายมีโหนดเพียงจำนวนหนึ่ง ซึ่งมีความต้องการการส่งข้อความเพื่อสื่อสารไปยังโหนดปลายทางที่น้อย เราควรให้ความสำคัญกับการเลือกใช้กลยุทธ์การส่งข้อความที่มีอัตราการแพร่กระจายสูง แต่ทว่าในสถานการณ์การสื่อสารจริง ที่โหนดแต่ละโหนดสร้างข้อความเพื่อสื่อสารไปยังโหนดต่างๆในเครือข่ายอย่างต่อเนื่อง สิ่งที่สำคัญมากกว่าอัตราการแพร่กระจายคือ ทำอย่างไรให้ทุกโหนดมีอายุการใช้งานเพิ่มขึ้นเพื่อช่วย(เพิ่มความเป็นไปได้) ในการส่งต่อข้อความไปยังปลายทาง และทำอย่างไรให้เส้นทางการสื่อสารสามารถรองรับข้อมูลได้อย่างต่อเนื่องโดยไม่เกิดปัญหาความคับคั่งของปริมาณข้อมูลเสียก่อน บทความนี้แสดงให้เห็นว่า n-Anti Entropy ซึ่งเป็นกลยุทธ์การส่งข้อความที่ได้รับการพัฒนามาจาก n-Epidemic และ Anti Entropy สามารถตอบโจทย์การสื่อสารในสถานการณ์จริงได้เป็นอย่างดี จากผลการทดลองแสดงให้เห็นว่า n-Anti Entropy มีผลรวมจำนวนข้อความที่ส่งออกน้อยกว่ากลยุทธ์ต้นแบบ ซึ่งสะท้อนให้เห็นว่าโหนดสูญเสียพลังงานในการส่งข้อมูลน้อยกว่า อีกทั้งยังสามารถลดปัญหาความคับคั่งของเส้นทางการสื่อสารได้ดีกว่าอีกด้วย และจากกราฟสัดส่วนของโหนดที่ได้รับข้อความ ยังแสดงให้เห็นถึงความสัมพันธ์ระหว่างความหนาแน่นของโหนดในเครือข่าย กับการกำหนดจำนวนโหนดเพื่อนบ้านที่ต้องรอคอย เพื่อให้ n-Anti Entropy มีประสิทธิภาพในการสื่อสารสูงสุด

เอกสารอ้างอิง

[1] Forrest Warthman. "Delay- and Disruption- Tolerant Networks (DTNs): A Tutorial" Interplanetary Internet Special Interest Group, July 2012.

[2] Jones, Evan PC, et al. "Practical routing in delay-tolerant networks." *Mobile Computing, IEEE Transactions on* 6.8 (2007): 943-959.

[3] Jones, Evan PC, and Paul AS Ward. "Routing strategies for delay-tolerant networks." *Submitted to ACM Computer Communication Review (CCR)* (2006).

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[4] Demers, Alan, et al. "Epidemic algorithms for replicated database maintenance." Proceedings of the sixth annual ACM Symposium on Principles of distributed computing. ACM, 1987.

[5] Vahdat, Amin, and David Becker. Epidemic routing for partially connected ad hoc networks. Technical Report CS-200006, Duke University, 2000.

[6] Lu, Xiaofeng, and Pan Hui. "An energy-efficient n-epidemic routing protocol for delay tolerant networks." *Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on*. IEEE, 2010.

[7] De Rango, and Amelio S. "Performance evaluation of scalable and energy efficient dynamic n-epidemic routing in Delay Tolerant Networks" Performance Evaluation of Computer and Telecommunication Systems (SPECTS), 2013 International Symposium on. IEEE, 2013.

[8] Grasic, Samo, and Anders Lindgren. "An analysis of evaluation practices for DTN routing protocols." Proceedings of the seventh ACM international workshop on Challenged networks. ACM, 2012.

[9] Mundur, Padma, Matthew Seligman, and Ginnah Lee. "Epidemic routing with immunity in delay tolerant networks." Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE, 2008.

[10] Gu, Xin, and Hailin Feng. "Connectivity analysis for a wireless sensor network based on percolation theory." Computer Application and System Modeling (ICCASM), 2010 International Conference on. Vol. 5. IEEE, 2010.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การปรับปรุงกลไกค้นหาเกตเวย์เพื่อลดโอเวอร์เฮด จากการแลกเปลี่ยนข้อมูลในเครือข่ายเฉพาะกิจ

สุเมธ ประภาวัต ทะนง ชูวณิชชานนท์ สารัช ศรีสวัสดิ์พงษ์ และ วรวัชร ณรงคะชวนะ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: sumet@it.kmitl.ac.th, tanong3200@hotmail.com, acecharmil@gmail.com, worravat@gmail.com

บทคัดย่อ

สำหรับระบบเครือข่ายสื่อสารที่สามารถใช้งานในสถานการณ์ภัยพิบัติ หรือโครงสร้างพื้นฐาน (Infrastructure) ถูกทำลายโดยส่วนใหญ่จะใช้ระบบเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด (Mobile Ad hoc Network: MANET) เพื่อสร้างเครือข่ายที่ไม่พึ่งพาโครงสร้างพื้นฐาน อีกทั้งมีการขยายขีดการเชื่อมต่อให้เครือข่ายสื่อสารเฉพาะกิจสามารถเชื่อมต่อระหว่างเครือข่ายได้โดยการค้นหาเกตเวย์ (Gateway Discovery) ทำให้ผู้ใช้สามารถติดต่อขอความช่วยเหลือกับคนที่อยู่นอกเครือข่ายหรือเขตภัยพิบัติได้ แต่การค้นหาเกตเวย์ที่มีอยู่นั้นมีโอเวอร์เฮดในการแลกเปลี่ยนข้อมูลสำหรับการค้นหาเกตเวย์จำนวนมาก ดังนั้นในงานวิจัยนี้จึงทำการลดโอเวอร์เฮดดังกล่าวเพื่อปรับปรุงกลไกค้นหาเกตเวย์ ซึ่งอาจส่งผลให้การใช้แบนด์วิดธ์ (Bandwidth) และพลังงานของโมบายล์โหนดในการค้นหาเกตเวย์ลดลง

คำสำคัญ-- เครือข่ายสื่อสารเฉพาะกิจ; การเชื่อมต่อระหว่างเครือข่าย; การค้นหาเกตเวย์

1. บทนำ

การติดต่อสื่อสารเป็นสิ่งที่จำเป็นอย่างมาก และด้วยความก้าวหน้าทางด้านเทคโนโลยีที่มีการพัฒนาไปอย่างรวดเร็วจึงทำให้เกิดนวัตกรรมใหม่ ๆ ทางด้านการสื่อสารแบบไร้สายขึ้นและมีการใช้งานกันอย่างแพร่หลาย อาทิ การเชื่อมต่ออินเทอร์เน็ตความเร็วสูงผ่านทางเครือข่ายไร้สาย และ เครือข่ายอินเทอร์เน็ตโทรศัพท์ไร้สาย จนทำให้การสื่อสารแบบไร้สายกลายเป็นส่วนหนึ่งในการดำเนินชีวิตของมนุษย์ ทั้งนี้เองหากมีภัยพิบัติหรือเหตุการณ์ไม่คาดฝัน เช่น แผ่นดินไหว สึนามิ ซึ่งทำให้โครงสร้างพื้นฐาน (Infrastructure) ถูกทำลาย หรือขาดแคลนแหล่งพลังงาน (แหล่งจ่ายไฟฟ้ากระแสสลับ) ส่งผลให้การติดต่อสื่อสารระหว่างโมบายล์โหนดกับโครงสร้างพื้นฐานถูกตัดขาด จึงไม่สามารถติดต่อสื่อสารหรือขอความช่วยเหลือจากบุคคลภายนอกได้ โดยมีนักวิจัยหลายกลุ่มพยายามพัฒนาเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด (MANET : Mobile Ad-hoc Network) [1] ทำให้โมบายล์โหนดที่ติดต่อสื่อสารกันได้โดยไม่ต้องใช้โครงสร้างพื้นฐาน

ในเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนด แต่ละโหนดจะส่งต่อแพ็กเก็ตให้กับโหนดข้างเคียง โดยอาศัยการเชื่อมต่อแบบโหนดต่อโหนด (Peer-to-Peer) ผ่านคลื่นความถี่วิทยุ (Radio Frequency) เช่น เครือข่ายระหว่างยานพาหนะ (VANET : Vehicular ad hoc network)

แต่การเชื่อมต่อกันเพียงในเครือข่ายดังกล่าวทำให้เกิดปัญหาการจำกัดทางด้านขอบเขตของเครือข่าย และในการที่โมบายล์โหนดต้องทำหน้าที่เป็นผู้ส่งต่อข้อมูลให้โหนดอื่น ๆ ทำให้มีการใช้พลังงานเพื่อทำหน้าที่ดังกล่าวนอกเหนือจากเพื่อการส่งข้อมูลของตนเอง ซึ่งส่งผลให้เกิดปัญหาในการใช้พลังงานที่มีอยู่อย่างจำกัด (จากแบตเตอรี่) ของโมบายล์โหนด

จากปัญหาดังกล่าว ผู้จัดทำจึงศึกษารูปแบบการหาเส้นทางบนเครือข่ายเฉพาะกิจของโมบายล์โหนด ให้สามารถหาเส้นทางเชื่อมต่อที่ผ่านเกตเวย์ออกไปยังโครงสร้างพื้นฐานได้ (อย่างเช่น เครือข่ายอินเทอร์เน็ต) เพื่อขยายขอบเขตเครือข่ายในการติดต่อสื่อสารให้กว้างขึ้น ทำให้ติดต่อสื่อสารออกไปนอกพื้นที่ได้ และเพื่อลดการใช้พลังงานที่มีอยู่อย่างจำกัดของโมบายล์โหนดให้ทำงานได้นานขึ้น ทำให้ลดโอกาสเกิดความไม่ต่อเนื่องในเครือข่าย ซึ่งเป็นการพัฒนาเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนดให้มีประสิทธิภาพมากยิ่งขึ้น

ในส่วนที่ 2 นั้นจะอธิบายถึงเทคโนโลยีที่นำมาใช้และทฤษฎีต่าง ๆ ที่เกี่ยวข้องในการพัฒนา ส่วนที่ 3 จะกล่าวถึงรายละเอียดของอัลกอริทึมในการค้นหาเกตเวย์ที่ได้ทำการพัฒนาขึ้น สำหรับส่วนที่ 4 จะเป็นการประเมินและวัดประสิทธิภาพของอัลกอริทึมดังกล่าว และสุดท้ายส่วนที่ 5 จะเป็นส่วนที่กล่าวถึงการสรุปผลของงานวิจัยนี้

2. ทฤษฎีและงานที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวกับเครือข่ายสื่อสารเฉพาะกิจของโมบายล์โหนดทำให้ทราบได้ว่าโพรโทคอลค้นหาเส้นทาง (Routing Protocols) ในเครือข่ายดังกล่าวสามารถแบ่งได้เป็น 3 กลุ่มตามรูปแบบพฤติกรรมในการค้นหาเส้นทาง [2] คือ 1) โพรโทคอลค้นหาเส้นทางแบบรีแอกทีฟ (Reactive Routing Protocols) ซึ่งทำการค้นหาเส้นทางเมื่อต้องการส่งข้อมูล ตัวอย่างของโพรโทคอลค้นหาเส้นทางที่มีลักษณะแบบนี้ ได้แก่ โพรโทคอลเอโอดีวี (AODV : Ad hoc On-Demand Distance Vector) [6] และโพรโทคอลดีเอสอาร์ (DSR : Dynamic Sort Routing) [5] เป็นต้น 2) โพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ (Proactive Routing Protocols) ซึ่งจะทำการค้นหาเส้นทางไปยังทุกปลายทางที่น่าจะเป็นไปได้ก่อนที่จะมีการส่งข้อมูล ตัวอย่างของโพรโทคอลค้นหาเส้นทางที่มี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ลักษณะแบบนี้ เช่น โพรโทคอลโอแอลเอสอาร์ (OLSR : Optimized Link State Routing) [7] และสุดท้าย 3) โพรโทคอลค้นหาเส้นทางแบบไฮบริดจ์ (Hybrid Routing Protocols) ซึ่งจะมีการทำงานผสมผสานระหว่างโพรโทคอลค้นหาเส้นทางทั้ง 2 แบบที่ได้กล่าวไว้ก่อนหน้า ตัวอย่างของโพรโทคอลค้นหาเส้นทางที่มีลักษณะแบบนี้ เช่น โพรโทคอลแซดอาร์พี (ZRP : Zone Routing Protocol)

โดยทั้งหมดนี้มีงานวิจัยบางส่วนได้พูดถึงการเชื่อมต่อระหว่างเครือข่ายเฉพาะกิจของโมบายล์โหนดกับเครือข่ายอื่นๆ เช่น เครือข่ายโทรศัพท์ (Cellular Network) [11] เครือข่ายอินเทอร์เน็ต [8],[9],[10] โดยในการเชื่อมต่อนักวิจัยได้เลือกใช้การค้นหาโหนดเกตเวย์ซึ่งมีหน้าที่เป็นตัวกลางในการเชื่อมต่อ โดยโหนดที่เป็นเกตเวย์นั้นเปรียบเสมือนประตูในการเชื่อมต่อระหว่างเครือข่ายสื่อสารเฉพาะกิจและเครือข่ายอินเทอร์เน็ตหรือเครือข่ายอื่นๆ ซึ่งเกตเวย์นั้นมีหน้าที่ทำความเข้าใจโพรโทคอลในการค้นหาเส้นทางทั้งแบบลำดับชั้น (Hierarchical) ของเครือข่ายอินเทอร์เน็ต และแบบแบน (Flat) ในเครือข่ายสื่อสารเฉพาะกิจ

จากการศึกษางานวิจัยที่เกี่ยวข้องกับการค้นหาเกตเวย์ นักวิจัยได้นำโพรโทคอลค้นหาเส้นทาง AODV [8],[10] มาทำการปรับแก้รูปแบบและการส่งของข้อความ (Message) จากที่กำหนดใน RFC [6] โดยแก้ไข HELLO messages ซึ่งในโพรโทคอล AODV นั้นใช้ HELLO messages เพื่อบอกถึงการมีตัวตนของตนเองกับโหนดรอบข้างโดยการบรอดแคสต์ซึ่งถูกส่งก็ต่อเมื่อโหนดนั้นๆยังไม่มีการส่ง คำร้องขอเส้นทาง (Route Request) การตอบกลับเส้นทาง (Route Reply) หรือข้อความในชั้นสื่อสารเชื่อมต่อข้อมูล (Data Link layer) โดยในการปรับแก้รูปแบบข้อความนั้นได้ทำการเพิ่มแฟล็ก (Flag) พิเศษ ที่เรียกว่า แฟล็ก I (I-flag) เพื่อระบุว่าเป็น HELLO message ที่ส่งมาจากเกตเวย์ และยังทำการบันทึกแอดเดรสของเกตเวย์ (Gateway Address) ใน HELLO message ด้วยเพื่อระบุว่าถูกสร้างมาจากเกตเวย์โหนดใด ซึ่งทั้งค่าแฟล็ก I และ แอดเดรสของเกตเวย์ (Gateway Address) จะถูกเก็บในฟิลล์ที่ไม่ได้ใช้ (Unused Field) ของ HELLO messages ทั้งนี้จึงขอเรียก HELLO messages ที่มีการปรับแต่งว่า HELLO_I ซึ่งในการส่ง HELLO I นั้นจะเริ่มส่งจากโหนดเกตเวย์เพื่อบอกถึงการมีอยู่ของโหนดเกตเวย์ให้ทุกโหนดที่อยู่ภายในช่วงคลื่นสัญญาณของเกตเวย์รับรู้ผ่านการรับ HELLO_I (จากการบรอดแคสต์ HELLO_I ของเกตเวย์) และจากนั้นโหนดที่ได้รับ HELLO_I จะทำการบรอดแคสต์ (Rebroadcast) HELLO_I ซ้ำออกไป โดยก่อนหน้านั้นจะทำการบันทึกเส้นทางที่สามารถไปยังเกตเวย์ได้ให้เป็น Default Route และมีเป้าหมายที่จะส่งต่อไป (Next Hop) เป็นโหนดที่ส่ง HELLO_I มาหาโหนดตัวนั้น (สำหรับโหนดที่ได้รับจากเกตเวย์คือ แอดเดรสของเกตเวย์) แต่ถ้าโหนดใดไม่ได้รับ HELLO_I ในช่วงระยะเวลาของการส่ง HELLO messages (HELLO interval) โหนดนั้นก็จะทำการส่ง HELLO messages แบบดั้งเดิมแทน (แบบปกติที่ไม่มีการปรับแก้)

เพื่อง่ายต่อความเข้าใจจึงขอเรียกการค้นหาเส้นทางไปยังเกตเวย์นี้ว่า อัลกอริทึม HELLO ซึ่งภายในงานวิจัยดังกล่าวนักวิจัยได้ทำการเปรียบเทียบอัลกอริทึม HELLO เข้ากับอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ และแบบรีแอกทีฟ โดยผลสรุปของงานวิจัยที่ได้ศึกษานี้คือ อัลกอริทึม HELLO มีเวลาที่ใช้ในการค้นหาเกตเวย์ที่น้อยกว่าเมื่อเปรียบเทียบกับอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ และแบบรีแอกทีฟ โดยอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟนั้นจะใช้เวลาในการค้นหาเกตเวย์ที่มากและคงที่ ทั้งนี้เราจึงให้ความสนใจเพียงอัลกอริทึม HELLO และอัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ

โดยสำหรับโพรโทคอลค้นหาเส้นทางแบบโพรแอกทีฟ [10] เมื่อโหนดได้รับข้อมูลเกี่ยวกับเกตเวย์จะตัดสินใจว่าจะรับหรือทิ้งข้อมูลนั้น โดยจะรับข้อมูลนั้นก็ต่อเมื่อโหนดไม่รู้เส้นทางไปยังเกตเวย์หรือข้อมูลนั้นมีเส้นทางที่สั้นกว่าหรือข้อมูลนั้นมาจากแหล่งกำเนิดเดียวกันแต่มีความใหม่กว่า (มี sequence number ที่มากกว่า) และถ้าหากโหนดได้รับข้อมูลเส้นทางก็จะหยุดการร้องขอเส้นทาง จากนั้นจึงทำการตั้งค่าหรือปรับปรุงเส้นทางไปยังเกตเวย์ตามข้อมูลที่ได้รับมา และส่งต่อไปยังโหนดอื่นๆ

3. แนวคิดและการดำเนินงาน

จากตัวอย่างงานวิจัยที่เกี่ยวกับการค้นหาเกตเวย์ที่ได้ทำการศึกษาและแสดงอยู่ในส่วนที่ 2 ของงานวิจัยนี้ อัลกอริทึม HELLO ที่ใช้การปรับแก้ HELLO message นั้นมีความน่าสนใจเป็นอย่างมากเนื่องจากมีเวลาในการทำให้แต่ละโหนดรับรู้ถึงการมีอยู่ของเกตเวย์น้อยกว่าอัลกอริทึมอื่นๆ แต่ก็ยังมีข้อเสียอยู่เช่นกัน คือภายในกลไกของอัลกอริทึม HELLO นั้นมักจะเกี่ยวข้องกับการบรอดแคสต์ข้อมูลเป็นส่วนใหญ่ซึ่งมีส่วนทำให้เกิดการสูญเสียพลังงานของโมบายล์โหนดโดยไม่จำเป็น ซึ่งในงานวิจัยของเราได้เล็งเห็นถึงปัญหาในส่วนนี้ จึงนำอัลกอริทึม HELLO มาเพิ่มกลไกบางอย่าง เพื่อลดการบรอดแคสต์ข้อมูลเส้นทางที่เกี่ยวข้องกับเกตเวย์โดยลดการบรอดแคสต์ที่มีปลายทางซ้ำ ๆ กันโดยไม่จำเป็นในเครือข่ายด้วยวิธีการลดจำนวนโหนดที่ทำการบรอดแคสต์ ซึ่งกลไกนี้แต่เดิมจะถูกใช้ในโพรโทคอลค้นหาเส้นทาง OLSR และมีชื่อเรียกว่าการเลือกโหนดเอ็มพีอาร์ (MPR: Multipoint Relays Selection) โดยโหนด MPR นั้นเป็นกลุ่มของโหนดข้างเคียง (Neighbor nodes) ที่มีหน้าที่ในการส่งต่อข้อมูล (Retransmission) ซึ่งทุกโหนดที่เป็นโหนดข้างเคียงไม่จำเป็นต้องเป็นโหนด MPR โดยโหนดที่ทำหน้าที่ในการเลือกโหนด MPR จะถูกเรียกว่าผู้คัดเลือกโหนด MPR (MPR Selectors) และกลุ่มของโหนด MPR ก็สามารถเปลี่ยนแปลงได้ตลอดตามความเหมาะสมด้วย โดยในการคัดเลือกโหนด MPR นั้นจะเลือกจากโหนดที่เป็นโหนดข้างเคียงในระยะ 1 hop (One Hop Neighbors) ที่สามารถเชื่อมต่อกับโหนดข้างเคียงในระยะ 2 hop (Two Hop Neighbors) ที่มากที่สุด ซึ่งโหนดข้างเคียงในระยะ 1 hop คือ โหนดที่ตนเองสามารถเชื่อมต่อได้ (โหนดที่อยู่ภายในช่วงคลื่นสัญญาณของตนเอง) แต่โหนดข้างเคียงในระยะ 2 hop คือ โหนดที่ตนเองไม่สามารถเชื่อมต่อได้แต่สามารถเชื่อมต่อโดยผ่านโหนดข้างเคียงในระยะ 1 hop ได้ ซึ่งในกลไกนี้โหนดข้างเคียงในระยะ 2 hop จะต้องมีการเชื่อมต่อแบบสองทิศทาง (Bi-Directional Link) กับโหนดข้างเคียงในระยะ 1 hop เพื่อยืนยันว่าทั้งคู่สามารถสื่อสารโต้ตอบกันได้มิใช่เพียงแต่โหนดข้างเคียงในระยะ 1 hop ส่งข้อมูลไปยังโหนดข้างเคียงในระยะ 2 hop ได้เท่านั้น โดยในงานวิจัยของเราจะนำกลไกการเลือกโหนด MPR มาปรับแก้และนำไปใช้เพื่อให้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เข้ากับอัลกอริทึม HELLO เพื่อจะได้มีเวลาที่ใช้ในการค้นหาเกตเวย์ที่ต่ำตามอัลกอริทึม HELLO และมีจำนวนข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งเครือข่ายจำนวนน้อยตามอัลกอริทึมแบบโพรแอกทีฟ โดยข้อมูลที่จะนำมาใช้ในการคำนวณหาโหนด MPR สำหรับอัลกอริทึมที่ได้พัฒนานั้นคือ ข้อมูลโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงของตน โดยข้อมูลดังกล่าวถูกบรรจุอยู่ใน HELLO message แบบดั้งเดิมซึ่งหลักการในการคัดเลือกโหนด MPR ที่ได้พัฒนาขึ้นนั้นได้นำทฤษฎีเซ็ต (Set Theory) เข้ามาช่วย ซึ่งมีการทำงานตามโค้ดเทียมในรูปที่ 1

```
1:   for x in V
2:   assume N = Nx - Nx'
3:        for i in N
4:             for j in N - i
5:                  if Nj ⊆ Ni
6:                       N = N - j
7:                  end
8:             end
9:        end
10:       for i in N
11:            for j in N - i
12:                 Ni,j = Ni,j ∪ (Ni ∩ Nj)
13:            end
14:       end
15:       for i in N
16:            if Ni ⊆ Ni,j
17:                 N = N - i
18:                 Ni,j = Ni,j - Ni
19:            end
20:       end
21:       V = V - (Nx - N)
22:  end
```

รูปที่ 1. แสดงโค้ดเทียมของอัลกอริทึมในการหาโหนด MPR

โดย G = กราฟเชื่อมโยง (Connected Graph) โดยที่ G = (V,E)

V = เซ็ตของโมบายล์โหนด

E = เส้นทางการเชื่อมโยงของแต่ละโมบายล์โหนด

x' = โหนด MPR ก่อนหน้า (Predecessor node)

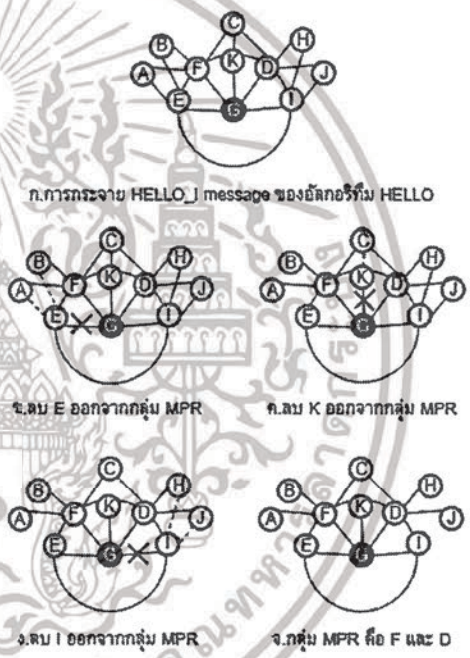
$N_{x \in V}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ของ x ใดๆใน V

$N'_{x \in V}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop ของ x ใดๆที่ไม่มีโหนดที่ก่อให้เกิดเส้นทางที่ซ้ำซ้อน (Redundancy Paths) โดยที่ $N'_{x \in V}$ เป็นเซ็ตย่อยของ $N_{x \in V}$ และทำให้ G' = (V',E') โดยที่ V' = $U_{(x \in V)} N'_x$ หรือกล่าวได้ว่า $N'_{x \in V}$ คือกลุ่มของโหนด MPR

$N_{i,j}$ = เซ็ตของโหนดข้างเคียงในระยะ 1 hop (1-hop neighbors) ร่วมของโหนด i และ j โดย $i,j \in N$ และ $i \neq j$

จากโค้ดเทียมในรูปที่ 1 นั้นจะแสดงให้เห็นถึงอัลกอริทึมที่ใช้ในการคำนวณหาโหนด MPR หรือ $N'_{x \in V}$ และรูปที่ 2 แสดงตัวอย่างการหาโหนด MPR โดยการทำงานของอัลกอริทึมสามารถแบ่งออกได้เป็น 2 ขั้นตอนคือ 1) หาความเป็นเซ็ตย่อย (Subset) ของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียง แสดงอยู่ในรูปที่ 1 บรรทัดที่ 3 ถึง 9 และรูปที่ 2 (ข และ ค) และขั้นตอนที่ 2) หาเซ็ตของโหนดข้างเคียงในระยะ 1 hop ของโหนดข้างเคียงที่เหลือที่ครอบคลุมโหนดข้างเคียงในระดับ 2 hop ของตนมากที่สุด แสดงอยู่ในรูปที่ 1 บรรทัดที่ 10 ถึง 20 และรูปที่ 2(ง) โดยทำการคำนวณในขั้นตอนที่ 2 ซ้ำไปเรื่อยๆจนกว่าจะไม่สามารถคัดเซ็ตใดออกจากการพิจารณาได้อีกซึ่งจะได้ออกมาเป็นเซ็ตของโหนด MPR ซึ่งแสดงให้รูปที่ 2 (จ)

โดยในการคำนวณหาโหนด MPR นั้นจะเริ่มทำการคำนวณจากโหนดเกตเวย์ โดยเมื่อคำนวณเสร็จเรียบร้อยแล้วเกตเวย์จะทำการส่ง HELLO_I message ที่บรรจุข้อมูลเกี่ยวกับโหนด MPR ที่เกตเวย์คำนวณได้ เพื่อระบุว่าโหนดใดเป็นโหนด MPR ไปยังโหนดข้างเคียงในระยะ 1 hop จากนั้นเมื่อโหนดข้องเคียงที่เป็น MPR ได้รับ HELLO_I message ดังกล่าวก็จะทำการคำนวณหาโหนด MPR ของตนต่อไป และส่ง HELLO_I message ไปยังโหนด MPR ที่คำนวณได้ต่อไปเรื่อยๆ พร้อมทั้งบันทึกเส้นทางไปยังเกตเวย์ตามอัลกอริทึม HELLO ที่ได้กล่าวไว้ในส่วนที่ 2 แต่สำหรับโหนดข้างเคียงที่ได้รับ HELLO_I message ไม่ใช่โหนด MPR ก็จะไม่ส่งต่อ HELLO_I message แต่บันทึกเส้นทางไป ยังเกตเวย์เพียงเท่านั้น



รูปที่ 2. แสดงตัวอย่างการหากลุ่มโหนด MPR

ดังนั้นสรุปว่าอัลกอริทึมที่เราได้พัฒนาได้มีการลดโอเวอร์เฮดจากการแลกเปลี่ยน HELLO_I message ของอัลกอริทึม HELLO คือ การลดจำนวนโหนดที่ทำหน้าที่กระจาย HELLO_I message ซึ่งอาจให้เกิดความซ้ำซ้อน ดังรูปที่ 2 (ก) ที่ทุกโหนดต้องทำหน้าที่บรอดแคสต์ข้อความ แต่สำหรับอัลกอริทึมที่เราได้พัฒนาขึ้นโดยขอเรียกว่า HELLOMPR จำมีเพียงบางโหนดที่ทำหน้าที่ในการบรอดแคสต์ ตัวอย่างเช่น ในรูปที่ 2 (ก) ที่ใช้อัลกอริทึม HELLO ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด E และ F เมื่อเปรียบเทียบกับรูปที่ 2 (จ) ที่ใช้อัลกอริทึม HELLOMPR ที่โหนด A และ B จะได้รับ HELLO_I message จากโหนด F เท่านั้น

ในส่วนถัดไปจะแสดงการเปรียบเทียบอัลกอริทึมในการค้นหาเกตเวย์ทั้ง 3 รูปแบบ คือ 1)อัลกอริทึมค้นหาเกตเวย์แบบโพรแอกทีฟ 2) อัลกอริทึม HELLO และ 3)อัลกอริทึมที่เราได้พัฒนาขึ้นโดยขอเรียกว่า อัลกอริทึม HELLOMPR ผ่านทางโปรแกรมจำลอง OMNET++ ซึ่งใน 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

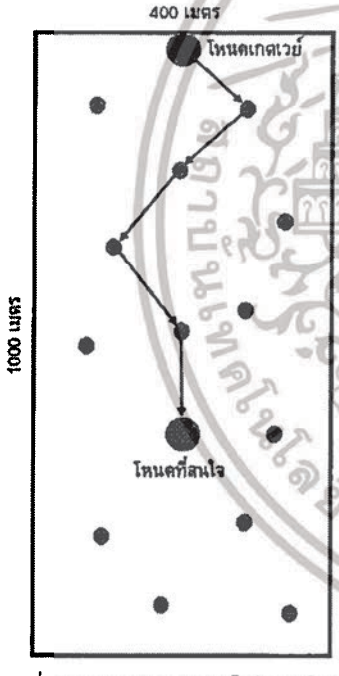
อัลกอริทึมแรกอ้างอิงการทำงานทำงานตามงานวิจัยที่ [8] เพื่อตรวจสอบความถูกต้องของอัลกอริทึมตามสมมติฐาน

4. การทดลองและการประเมินผล

ในการทดลองนั้นนักวิจัยได้ทำการจำลองการทำงานของอัลกอริทึมผ่านโปรแกรมจำลอง OMNET++ ซึ่งเป็นการเปรียบเทียบระหว่างอัลกอริทึมในการค้นหาเกตเวย์ทั้ง 3 รูปแบบ (อัลกอริทึมโพรแอกทีฟ อัลกอริทึม HELLO และอัลกอริทึม HELLOMPR) โดยมีข้อกำหนดเกี่ยวกับเหตุการณ์จำลอง และผลการทดลองเปรียบเทียบดังนี้

4.1 เหตุการณ์จำลองและตัวแปรต่าง ๆ ที่ใช้ในการจำลอง

ในการตรวจสอบและวัดประสิทธิภาพการทำงานของอัลกอริทึมในการค้นหาเกตเวย์ที่ได้กล่าวไปนั้นกำหนดให้การกระจายตัวของโหนดจะกระจายแบบสุ่มอยู่ในเครือข่ายมีพื้นที่ 2 รูปแบบคือ 1) ขนาดกว้าง 400 เมตร และยาว 1,000 เมตร ดังแสดงในรูปที่ 3 และ 2) ขนาดกว้าง 1,000 เมตร และยาว 400 เมตร



รูปที่ 3. แสดงภาพจำลองทอพอโลยีของเครือข่าย

ซึ่งแต่ละโหนดจะไม่มีการเคลื่อนที่ โดยในการทดลองแต่ละครั้งใช้การกระจายแบบสม่ำเสมอ (Uniform Distribution) เพื่อให้โหนดมีการกระจายตัวที่แตกต่างกัน และใช้เพียง ทราฟฟิค (Traffic) สำหรับการสร้างการเชื่อมต่อของโหนดภายในเครือข่ายสื่อสารเฉพาะกิจเท่านั้น โดยจากรูปที่ 3 กำหนดให้โหนดที่เป็นเกตเวย์ (Gateway node) อยู่ทางเหนือสุดของเครือข่าย และกำหนดให้โหนดที่สนใจซึ่งคือ โหนดที่จะต้องได้รับข้อมูลเส้นทางไปยังเกตเวย์ อยู่ห่างจากเกตเวย์ระยะ 600 เมตร โดยที่ทุกโหนดมีระยะในการส่งข้อมูล 250 เมตรรอบตัวโหนด

นอกเหนือจากข้อมูลที่ได้กล่าวไปยังมีตัวแปรต่าง ๆ ที่ได้กำหนดและใช้ในการจำลองเพิ่มเติมดังแสดงในตารางที่ 1

ตารางที่ 1. ตัวแปรต่าง ๆที่กำหนดในการทดลอง

จำนวนโหนดในเครือข่ายสื่อสารเฉพาะกิจ	15, 60
พื้นที่ของเครือข่าย	400 เมตร × 1,000 เมตร 1000 เมตร × 400 เมตร
ระยะส่งข้อมูลของโหนด	250 เมตร
เวลาทั้งหมดในการทดลอง	300 วินาที
ช่วงเวลาในการส่ง HELLO message	1, 5, 10, 15, 20, 25, 30
ระยะทางระหว่างโหนดเกตเวย์และโหนดที่สนใจ	600 เมตร
จำนวนรอบที่ใช้ในการทดลอง	100 รอบ (15 โหนด) 100 รอบ (60 โหนด)

4.2 ตัวชี้วัดและผลการทดลอง

ในการวัดผลการทดลองนั้นจะทำการเปรียบเทียบระหว่างอัลกอริทึมในการค้นหาเส้นทางไปยังเกตเวย์ดังนี้ คือ อัลกอริทึมโพรแอกทีฟ อัลกอริทึม HELLO และอัลกอริทึม HELLOMPR ซึ่งมีตัวชี้วัดที่ใช้ในการทดลองคือ 1) จำนวนของข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบ และ 2) เวลาที่ใช้ในการค้นหาเกตเวย์ เนื่องจากในการพัฒนาอัลกอริทึมนี้เป็นการพัฒนาเพื่อลดจำนวนข้อความที่ถูกส่งภายในเครือข่ายและยังสามารถคงสภาพเวลาที่ใช้ในการค้นหาเกตเวย์เพื่อให้เหมาะสำหรับการใช้งานในสถานการณ์ภัยพิบัติ

ในรูปที่ 4 รูปที่ 5 และตารางที่ 2 แสดงให้เห็นถึงผลลัพธ์ของการทดลองในตัวชี้วัดด้านจำนวนข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบ สำหรับเครือข่ายที่มีความหนาแน่นของโหนดจำนวน 15 โหนดและ จำนวน 60 โหนดตามลำดับ ซึ่งจะเห็นได้ว่าอัลกอริทึมแบบโพรแอกทีฟมีการส่งข้อความเกี่ยวกับ เกตเวย์ภายในเครือข่ายเป็นจำนวนน้อยที่สุด เนื่องจากโพรโทคอลที่นำมาพัฒนาให้ใช้อัลกอริทึมนี้คือโพรโทคอล OLSR ซึ่งมีกลไกในการลดจำนวนโหนดที่ใช้ในการส่งข้อมูลเส้นทาง แต่ในทางกลับกันอัลกอริทึม HELLO นั้นมีจำนวนข้อความที่ส่งในเครือข่ายมากที่สุด เนื่องจากกลไกในการส่งข้อความเส้นทางนั้นทุกโหนดในเครือข่ายจะมีส่วนร่วมในการบรอดแคสต์ทุกโหนด

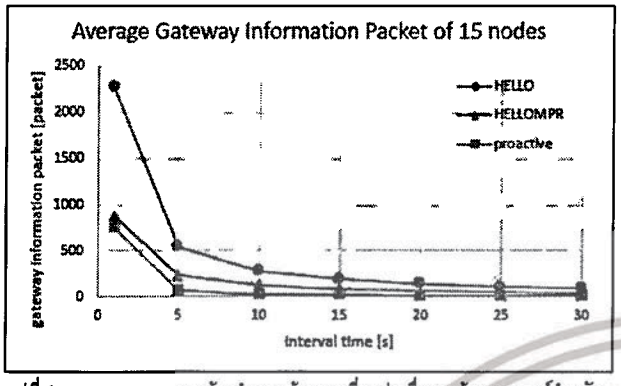
และจากผลลัพธ์สำหรับอัลกอริทึม HELLOMPR นั้นแสดงให้เห็นว่ามีจำนวนข้อความในระบบน้อยกว่าอัลกอริทึม HELLO แบบดั้งเดิมก่อนพัฒนา ซึ่งจากในตารางที่ 2 จะเห็นได้ว่าต่ำประมาณ 2 เท่า เนื่องจากได้มีการนำกลไกในการลดจำนวนโหนดที่ใช้ในการ ส่งข้อมูลเส้นทางของโพรโทคอล OLSR เข้ามาเป็นกลไกเพิ่มเติม แต่ทั้งนี้เองอัลกอริทึม HELLOMPR ก็ยังมีจำนวนข้อความที่มากกว่าอัลกอริทึมแบบโพรแอกทีฟอยู่ดี เนื่องจากอัลกอริทึม HELLOMPR นั้นแต่เดิมถูกพัฒนามาจากโพรโทคอล AODV ที่เป็นโพรโทคอลแบบรีแอกทีฟ

ในรูปที่ 6 รูปที่ 7 และตารางที่ 3 นั้นแสดงให้เห็นถึงผลลัพธ์ของการทดลองในตัวชี้วัดด้านเวลาที่ใช้ในการค้นหาเกตเวย์ (Gateway Discovery Time) สำหรับเครือข่ายที่มีโหนดจำนวน 15 โหนดและจำนวน 60 โหนดตามลำดับ โดยจะเริ่มจับเวลาตั้งแต่เกตเวย์เริ่มประกาศข้อมูลเกี่ยวกับเส้นทางจนกระทั่งถึงเวลาที่โหนดที่สนใจรู้เส้นทางในการติดต่อไปยังเกตเวย์

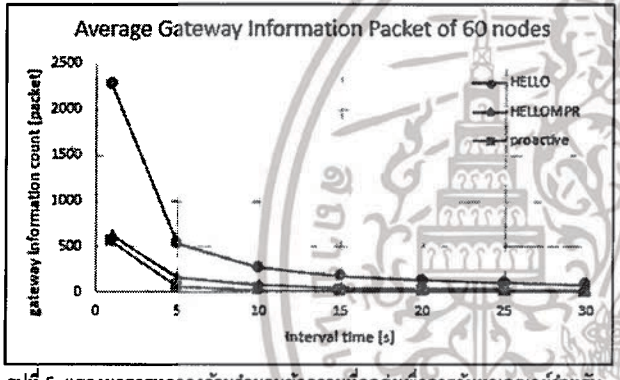
ซึ่งเห็นได้ชัดเจนว่าอัลกอริทึมแบบโพรแอกทีฟนั้นมีเวลาที่ใช้ในการค้นหาเกตเวย์เป็นครึ่งหนึ่งของช่วงเวลาในการส่งข้อความ ซึ่งถ้า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ช่วงเวลาดังกล่าวเพิ่มขึ้นเวลาที่ใช้ในการค้นหาเกตเวย์ก็จะเพิ่มขึ้นจนกระทั่งสูงมาก ๆ ไม่ว่าจะเป็นเครือข่ายที่มีจำนวนโหนด 15 โหนด หรือ 60 โหนดก็ตาม



รูปที่ 4. แสดงผลการทดลองด้านจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์สำหรับโหนดจำนวน 15 โหนด



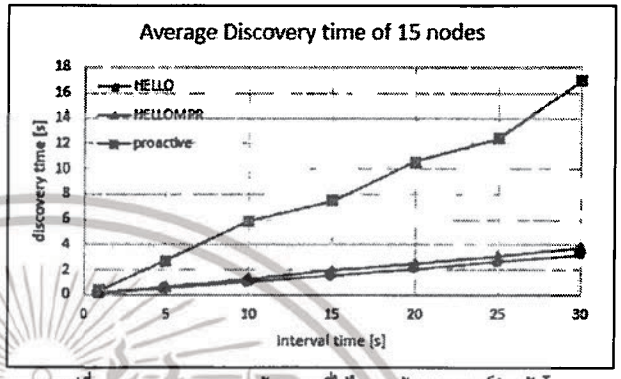
รูปที่ 5. แสดงผลการทดลองด้านจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด

ตารางที่ 2. ผลการทดลองสำหรับจำนวนข้อความที่ถูกส่งเพื่อการค้นหาเกตเวย์

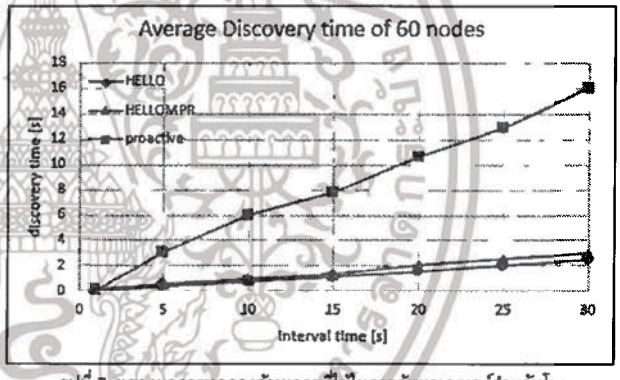
	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	764.679 packet	31.432 packet	12 packet
HELLO	2270.706 packet	277.093 packet	88.7103 packet
HELLOMPR	883.861 packet	124.876 packet	37.284 packet
60 nodes			
proactive	558.348 packet	31.384 packet	10 packet
HELLO	2269.694 packet	275.809 packet	87.39 packet
HELLOMPR	628.5188 packet	87.445 packet	27.771 packet

ส่วนอัลกอริทึม HELLO ถึงแม้ช่วงเวลาของการส่งข้อความมากขึ้น แต่เวลาที่ใช้ในการค้นหาเกตเวย์เพิ่มขึ้นเพียงเล็กน้อย ในตารางที่ 3 จะเห็นได้ว่าเครือข่ายที่มีความหนาแน่นสูงหรือมีโหนดจำนวน 60 โหนดมีเวลาเฉลี่ยที่ใช้ในการค้นหาที่ต่ำกว่าเครือข่าย ที่มีความหนาแน่นน้อยๆ

และอัลกอริทึม HELLOMPR เมื่อช่วงเวลาในการส่งข้อความเพิ่มขึ้นก็มีเวลาที่ใช้ในการค้นหาเกตเวย์เพิ่มเพียงเล็กน้อยเช่นเดียวกับอัลกอริทึม HELLO แต่เมื่อเทียบกับอัลกอริทึม HELLO แล้วยังมีเวลาที่ใช้ในการค้นหาเกตเวย์มากกว่าเล็กน้อยดังตารางที่ 3 เพราะผลของกลไกการเลือกโหนดบรอดแคสต์ทำให้บางครั้งโหนดที่สนใจจะได้รับ HELLO_I message ช้ากว่าในกรณีที่โหนดที่สนใจนั้นอยู่ใกล้กับโหนดที่ไม่ได้ถูกเลือกให้บรอดแคสต์มากกว่าโหนดที่ถูกเลือกให้บรอดแคสต์ ดังนั้นโหนดที่สนใจจึงได้รับ HELLO_I message ช้ากว่าอัลกอริทึม HELLO อีกทั้งยังมีเรื่องของระยะห่างระหว่างโหนดที่บรอดแคสต์และโหนดที่สนใจที่แตกต่างกันอีกด้วย



รูปที่ 6. แสดงผลการทดลองด้านเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับโหนดจำนวน 15 โหนด



รูปที่ 7. แสดงผลการทดลองด้านเวลาที่ใช้ในการค้นหาเกตเวย์สำหรับโหนดจำนวน 60 โหนด

ตารางที่ 3. ผลการทดลองสำหรับเวลาเฉลี่ยที่ใช้ในการค้นหาเกตเวย์

	Interval [s]		
15 nodes	**1**	**10**	**30**
proactive	0.4s	5.862s	16.96s
HELLO	0.126s	1.027s	3.222s
HELLOMPR	0.197s	1.277s	3.832s
60 nodes			
proactive	0.094s	5.976s	16.1s
HELLO	0.108s	0.787s	2.509s
HELLOMPR	0.167s	0.967s	2.978s

โดยสรุปแล้วจากผลลัพธ์ของการทดลอง 100 ครั้งของเครือข่ายทั้ง 2 ขนาด โดยที่แต่ละการทดลองมีรูปแบบการกระจายของโหนดที่แตกต่างกัน ซึ่งโหนดมีการกระจายสุ่มแบบยูนิฟอร์ม ซึ่งผลที่ได้จากทั้ง 2 เครือข่ายมีใกล้เคียงกัน (แตกต่างกันเฉลี่ยเพียง 7% - 8%) และได้ค่าเฉลี่ยของผลลัพธ์ดังกราฟในรูปที่ 4 ถึง 7 โดยมีความแปรปรวน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เท่ากับ 0.0271, 0.0294และ 0.0172 สำหรับผลของอัลกอริทึม HELLO HELLOMPR และโพรแอกทีฟตามลำดับ ในการค้นหาเกตเวย์ของอัลกอริทึมโพรแอกทีฟมีการส่งข้อความเกี่ยวกับเกตเวย์ในเครือข่ายจำนวนน้อยที่สุด ในเครือข่ายที่มีความหนาแน่นทั้ง 15 โหนด และ 60 โหนด แต่สำหรับเวลาในการค้นหาเกตเวย์นั้นมีอัตราที่สูงกว่าเมื่อเทียบกับอัลกอริทึม HELLO แม้ช่วงเวลาในการส่งข้อความจะเพิ่มขึ้นก็ตาม

แต่อย่างไรก็ตามจำนวนการส่งข้อความของอัลกอริทึม HELLO เกี่ยวกับเกตเวย์กลับมีจำนวนมากเมื่อเทียบกับอัลกอริทึมแบบโพรแอกทีฟ ซึ่งอัลกอริทึม HELLOMPR นั้นมีการส่งข้อความเกี่ยวกับเกตเวย์เป็นจำนวนน้อยใกล้เคียงกับอัลกอริทึมโพรแอกทีฟและใช้เวลาในการค้นหาเกตเวย์น้อยใกล้เคียงกับอัลกอริทึม HELLO ทั้งเครือข่ายที่มีความหนาแน่นจำนวนของโหนด 15 โหนด และ 60 โหนด หรืออาจบอกได้ว่าอัลกอริทึม HELLOMPR นั้นได้รวมเอาข้อดีในด้านการส่งข้อมูลเส้นทางเกี่ยวกับเกตเวย์ที่มีจำนวนน้อยของอัลกอริทึมแบบโพรแอกทีฟ และนำเอาข้อดีในด้านเวลาในการค้นหาเกตเวย์ที่ต่ำของอัลกอริทึม HELLO เข้าด้วยกัน

5. สรุปผล

ในงานวิจัยนี้เราได้พัฒนาอัลกอริทึมในการค้นหาเกตเวย์สำหรับเครือข่ายสื่อสารเฉพาะกิจโดยมีพื้นฐานมาจากโพรโทคอล AODV ซึ่งได้นำหลักการในการคัดเลือกโหนด MPR จากโพรโทคอล OLSR และทฤษฎีเซ็ตมาใช้เพื่อเพิ่มประสิทธิภาพโดยการลดจำนวนข้อมูลที่ส่งต่อภายในเครือข่าย

จากผลการทดลองและการประเมินผลในส่วนที่ 4 ของงานวิจัยนี้สามารถสรุปผลได้ว่าเครือข่ายที่ใช้อัลกอริทึม HELLOMPR ที่ได้พัฒนาขึ้นนั้นมีจำนวนของข้อความที่บรรจุข้อมูลเส้นทางไปยังเกตเวย์ที่ถูกส่งภายในระบบน้อยกว่าเครือข่ายที่ใช้อัลกอริทึม HELLO จนเข้าใกล้อัลกอริทึมแบบโพรแอกทีฟในการค้นหาเกตเวย์ เป็นผลจากการลดจำนวนโหนดที่ต้องบรอดแคสต์ข้อมูลที่ใช้ในการค้นหาเกตเวย์ และยังส่งผลให้โหนดในเครือข่ายมีพลังงานและอยู่ในระบบได้นานขึ้น เพราะทุกโหนดไม่จำเป็นต้องบรอดแคสต์ข้อมูลเส้นทางที่เกี่ยวข้องกับเกตเวย์ จึงทำให้ไม่เสียพลังงานไปโดยเปล่าประโยชน์ และจากผลการทดลองเกี่ยวกับเวลาที่ใช้ในการทำให้โหนดที่สนใจรับจักเส้นทางไปยังเกตเวย์จะเห็นได้ว่าอัลกอริทึมที่พัฒนามิได้ลดประสิทธิภาพของอัลกอริทึม HELLO ก่อนพัฒนาลงอีกด้วย

ซึ่งในสถานการณ์ภัยพิบัตินั้นมีความจำกัดทางด้านแหล่งพลังงานของโมบายล์โหนด (จากแบตเตอรี่) ดังนั้นอัลกอริทึมที่มีความเหมาะสมคือ อัลกอริทึมแบบโพรแอกทีฟ และอัลกอริทึม HELLOMPR เพราะมีการส่งข้อความเป็นจำนวนน้อยเมื่อเทียบกับอัลกอริทึมแบบ HELLO และเนื่องด้วยการสื่อสารควรสามารถสื่อสารได้อย่างเร่งด่วนดังนั้นอัลกอริทึมที่มีความเหมาะสมมากที่สุดที่สำหรับสภานการณ์ภัยพิบัตินี้คือ อัลกอริทึม HELLOMPR เพราะเมื่อเปรียบเทียบเวลาในการค้นหาเกตเวย์ระหว่างอัลกอริทึมแบบโพรแอกทีฟ และโพรโทคอล HELLOMPR จะเห็นได้ว่าอัลกอริทึม HELLOMPR นั้นมีเวลาที่น้อยกว่าตามผลการทดลอง

เอกสารอ้างอิง

[1] T. S. Rappaport. "Wireless Communications Principles & Practice." Upper Saddle River, New Jersey: Prentice-Hall, Inc.1996

[2] T. Lin. "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications." Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the Ph.D. in Computer Engineering. 2004

[3] Wireless Embedded Systems, Computer Science Department, University of California at Berkeley, "Self-organized wireless sensor network." August, 2001.
Available :http://webs.cs.berkeley.edu/800demo

[4] K.Gorantala. "Routing Protocols in Mobile Ad-hoc Networks" Master's Thesis in Computing Science at Ume°a University. June 15, 2006

[5] D. B. Johnson, D. A. Maltz, Y. C. Hu, and J. G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)." Internet Engineering Task Force (IETF) draft, February 2007. [Online]
Available :http://datatracker.ietf.org/doc/rfc4728/

[6] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing." Internet Engineering Task Force (IETF) draft, July 2003.[Online]
Available :http://datatracker.ietf.org/doc/rfc3561/

[7] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol (OLSR)." Internet Engineering Task Force(IETF) draft, October 2003.[Online]
Available :https://datatracker.ietf.org/doc/rfc3626/

[8] M. Rosenschon, "Internet Gateway Discovery for Mobile Ad Hoc Networks" Submitted for the Degree of Doctor of Philosophy School of Engineering and Mathematical Sciences CITY University London. 2 October 2007

[9] J. Broch, et al. "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks" International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN99), Workshop on Mobile Computing, Perth, Western Australia. June 1999

[10] M. Rosenschon, T. Manz, J. Habermann, V. Rakocevic. "Gateway Discovery Algorithm for Ad-Hoc networks using HELLO Messages" International Workshop on Wireless Ad Hoc Networks IWWAN 2005, London. May 2005.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

[11] H. Luo, R. Ramjeey, P. Sinhaz, L. Liy, S. Lu "UCAN: A Unified Cellular and AdHoc Network Architecture" MobiCom'03, San Diego, California, USA, September 2003.



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การประยุกต์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉินและตำแหน่งที่อยู่ เพื่อขอรับบริการรถนำส่งและบริการทางการแพทย์

สุเมธ ประภาวัต ธนานพ ทองถาวร และ ณัชชา วัฒนอรุณกิจ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: sumet@it.kmitl.ac.th, St_freedom2@hotmail.com, ZinreF@gmail.com

บทคัดย่อ

ในปัจจุบันผู้ป่วยฉุกเฉินวิกฤตที่มีสาเหตุมาจากอาการเจ็บป่วยหรืออุบัติเหตุมีมากกว่า 200,000 รายต่อปี โดยระบบที่ใช้ในการรองรับผู้ป่วยดังกล่าวคือระบบสายด่วนฉุกเฉิน 1669 ซึ่งเป็นระบบการแจ้งเหตุผ่านทางโทรศัพท์เพื่อแจ้งที่อยู่ และอาการของผู้ป่วยแก่เจ้าหน้าที่ ก่อนที่เจ้าหน้าที่จะทำการช่วยเหลือต่อไป ซึ่งในบทความฉบับนี้จะกล่าวถึงการประยุกต์ใช้งานระบบระบุตำแหน่งบนพื้นโลกและสมาร์ทโฟนเพื่อใช้ในการระบุตำแหน่งของผู้ป่วยหรือพื้นที่ที่เกิดอุบัติเหตุ ก่อนที่จะส่งความช่วยเหลือทางการแพทย์ที่เหมาะสมไปยังผู้ป่วย โดยมีระบบช่วยตัดสินใจในการคัดกรองเส้นทางและเลือกทรัพยากรที่จำเป็นต่อการช่วยเหลือผู้ป่วยเพื่อลดระยะเวลาปฏิบัติการที่ใช้ในการตัดสินใจของเจ้าหน้าที่ ซึ่งจะส่งผลให้ผู้ป่วยมีอัตราการรอดชีวิตหรือรอดพ้นจากสภาวะพิการที่อาจเกิดขึ้นในขณะที่ทำการช่วยเหลือผู้ป่วยมากขึ้น และหลังจากศึกษาบทความนี้ ผู้อ่านจะได้ทราบถึงแนวคิดและวิธีการดำเนินงานของระบบ บทสรุป และแนวทางการพัฒนาต่อยอดของงานชิ้นนี้ต่อไป

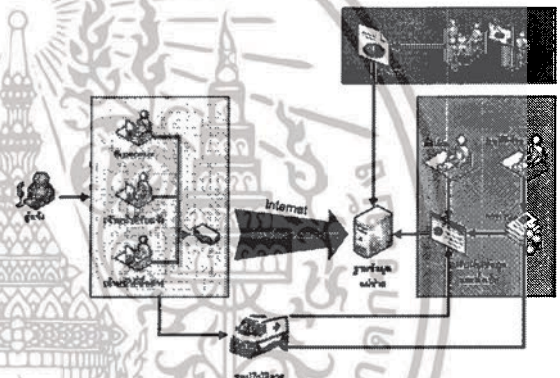
คำสำคัญ— แจ้งเหตุผ่านสมาร์ทโฟน; ระบบช่วยตัดสินใจ; การช่วยชีวิต

1. บทนำ

ในปัจจุบันสมาร์ทโฟนเป็นอุปกรณ์สื่อสารที่ได้รับความนิยมและสามารถพบเห็นได้ทั่วไป เนื่องจากสามารถเชื่อมต่ออินเตอร์เน็ตและระบุตำแหน่งบนพื้นโลกได้ ประกอบกับระบบที่ใช้ในการแจ้งเหตุฉุกเฉินในปัจจุบันยังคงใช้วิธีการติดต่อสื่อสารกับผู้ป่วยผ่านทางโทรศัพท์โดยตรง[1] ในการสอบถามอาการและที่อยู่ของผู้ป่วย ซึ่งต้องใช้เวลาและปัจจัยอีกหลายอย่างมาเกี่ยวข้องเพื่อทำให้การสื่อสารในลักษณะนี้ประสบความสำเร็จในสภาวะฉุกเฉิน จึงมีแนวคิดในการประยุกต์ใช้สมาร์ทโฟนในการแจ้งเหตุฉุกเฉินเพื่อช่วยเพิ่มช่องทางในการแจ้งเหตุฉุกเฉินและลดระยะเวลาการติดต่อสื่อสารกับเจ้าหน้าที่ในการแจ้งเหตุฉุกเฉิน ประกอบกับระบบช่วยตัดสินใจในส่วนของเจ้าหน้าที่ซึ่งสามารถช่วยลดระยะเวลา และปริมาณข้อมูลที่ใช้ในการตัดสินใจ ส่งผลให้การช่วยเหลือผู้ป่วยมีประสิทธิภาพมากยิ่งขึ้น

2.ทฤษฎีและงานที่เกี่ยวข้อง

2.1 ระบบสนับสนุนการช่วยเหลือผู้ประสบเหตุ



รูปที่ 1. ภาพรวมของระบบ สพฉ.

ปัจจุบันมีหลายหน่วยงานที่ให้บริการนำส่งผู้ป่วยเหตุฉุกเฉินไม่ว่าจะเป็นภาครัฐหรือเอกชน สถาบันการแพทย์ฉุกเฉินแห่งชาติเป็นหน่วยงานหลักหน่วยหนึ่งที่ได้รับมอบหมายในการให้บริการดังกล่าว ซึ่งเป็นที่รู้จักกันในนาม "บริการสายด่วนฉุกเฉิน 1669[2]" ในการรับแจ้งเหตุฉุกเฉิน โดยมีเจ้าหน้าที่เป็นผู้ประสานงาน ทำหน้าที่ในการรับการแจ้งเหตุจากผู้ป่วย ตัดสินใจเลือกรถนำส่งและสถานพยาบาล ในส่วนของระบบสารสนเทศจะมีบทบาทเพียงแค่การรวบรวมผลรายงาน และการอนุมัติการเงินในการรักษาเท่านั้น ซึ่งหน่วยงานอื่นที่มาร่วมให้บริการ อย่างเช่น หน่วยรับแจ้งเหตุของโรงพยาบาลหรือมูลนิธิอาสาสมัครต่างๆ ก็มีรูปแบบการทำงานที่ไม่แตกต่างกันมากนัก

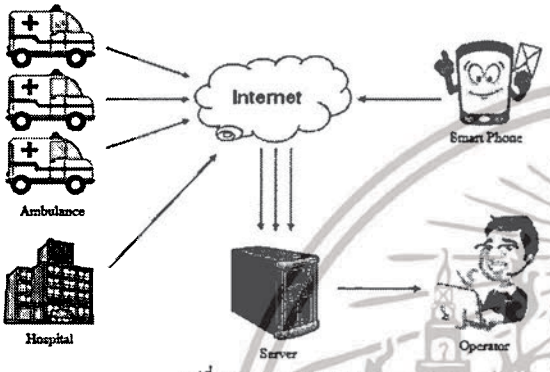
2.2 ระบบดาวเทียมนำร่อง

ระบบดาวเทียมนำร่องถูกพัฒนาขึ้นเพื่อระบุพิกัดสำหรับอ้างอิงตำแหน่งบนพื้นโลก อย่างเช่น ระบบจีพีเอส[3] ซึ่งเป็นหนึ่งในระบบนำร่องสำหรับการระบุตำแหน่งที่ถูกใช้กันอย่างแพร่หลาย โดยใช้ดาวเทียมเข้ามาช่วยในการคำนวณตำแหน่งต่างๆ ซึ่งในการระบุตำแหน่งต่างๆ นั้น ภายในอุปกรณ์ที่จะถูกระบุตำแหน่งจำเป็นต้องมีอุปกรณ์รับสัญญาณจากดาวเทียมติดตั้งอยู่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากนั้นในการคำนวณตำแหน่งของอุปกรณ์รับสัญญาณจะประมวลผลจากการรับสัญญาณดาวเทียมมากกว่าสามตัวขึ้นไป เพื่อหาพื้นที่คาบเกี่ยวระหว่างดาวเทียมทั้งหมดโดยใช้ Triangulation Method ซึ่งจะทำให้ทราบว่า อุปกรณ์รับสัญญาณนั้นอยู่ในพิกัดละติจูดและลองจิจูดที่เท่าไร นอกจากระบบจีพีเอสแล้วยังมีอีกหลายระบบอาทิเช่น โกลนาสของรัสเซีย กาลิเลโอของยุโรป คอมพาสของจีน เป็นต้น แต่ระบบเหล่านี้ส่วนใหญ่ยังไม่ถูกรองรับในอุปกรณ์สมาร์ทโฟนในไทย

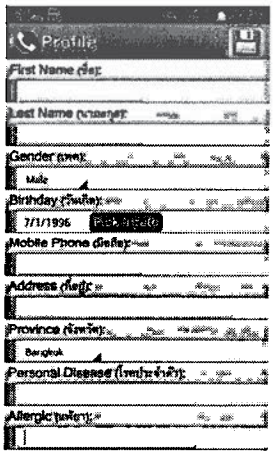
3. แนวคิดและการดำเนินงาน



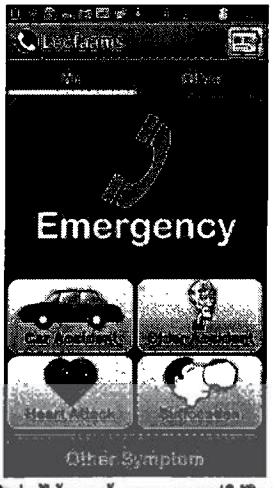
รูปที่ 2. ภาพรวมของระบบ

จากรูปที่ 2 หลังจากมีการส่งข้อมูลของผู้ป่วยเข้ามาที่เซิฟเวอร์แล้วระบบจะทำการตรวจสอบพิกัดจีพีเอสที่จุดเกิดเหตุและทำการค้นหาโรงพยาบาลและรถนำส่งที่อยู่ใกล้กับจุดเกิดเหตุ เพื่อสร้างตารางเส้นทางระหว่างโรงพยาบาลและรถนำส่งที่เหมาะสม โดยคำนึงถึงอาการของผู้ป่วยเป็นสำคัญ เพื่อให้สามารถเลือกรถนำส่งที่เหมาะสมไปทำการช่วยเหลือผู้ป่วยได้ ในกรณีที่ไม่สามารถระบุอาการได้ระบบจะนำประวัติส่วนตัวของผู้ป่วยมาประมวลผลแทน จากนั้นเจ้าหน้าที่จะทำการตัดสินใจครั้งสุดท้ายในการเลือกเส้นทางจากตารางที่ระบบสร้างขึ้น และประสานงานไปยังเจ้าหน้าที่ประจำรถนำส่งเพื่อทำการช่วยเหลือผู้ป่วยต่อไป

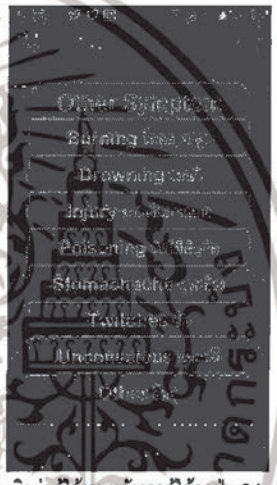
3.1. แอพพลิเคชั่นบนสมาร์ทโฟน



รูปที่ 3. ส่วนติดต่อผู้ใช้งานหลังจากผู้ใช้กดปุ่ม Profile (มุมขวา)



รูปที่ 4. ส่วนติดต่อผู้ใช้งานหน้าแรกบนระบบปฏิบัติการแอนดรอยด์



รูปที่ 5. ส่วนติดต่อผู้ใช้งานหลังจากผู้ใช้กดปุ่ม Other Symptom

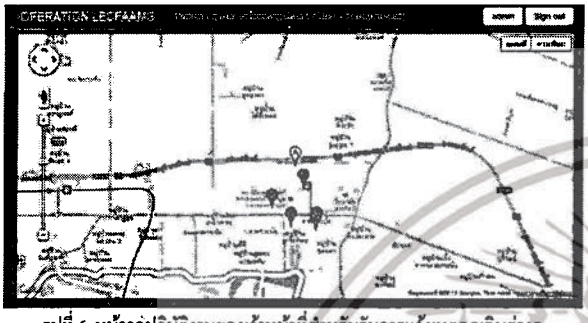
ระบบนี้ถูกพัฒนามาจากงานวิจัยการศึกษาการใช้งานระบบจีพีเอส[4][5] ซึ่งในการแจ้งเหตุฉุกเฉินผู้ป่วยจะต้องเรียกใช้งานแอพพลิเคชั่นบนสมาร์ทโฟนในการแจ้งเหตุฉุกเฉิน โดยจะมีการเก็บบันทึกประวัติส่วนตัวของผู้ป่วยเอาไว้ดังรูปที่ 3 ในกรณีที่เกิดเหตุฉุกเฉินและผู้ป่วยไม่มีสติมากพอที่จะตัดสินใจ ผู้ป่วยสามารถกดปุ่ม "Emergency" ดังรูปที่ 4 เพื่อแจ้งเหตุฉุกเฉิน หรือในกรณีที่ผู้ป่วยอยู่ในสภาวะพอมีสติในการตัดสินใจ ผู้ป่วยสามารถกดปุ่มเลือกอาการของผู้ป่วยในขณะนั้นได้ดังรูปที่ 4-5 โดยหลังจากผู้ใช้ทำการกดปุ่มอาการใดๆ บนสมาร์ทโฟนแล้ว จะมีการหน่วงเวลา 5 วินาที เพื่อให้โอกาสผู้ใช้ยกเลิกการแจ้งเหตุในกรณีที่เกิดการแจ้งเหตุโดยไม่ตั้งใจ แต่ในกรณีที่ต้องการยืนยันการแจ้งเหตุฉุกเฉิน ผู้ใช้สามารถกดปุ่ม "Send" เพื่อยกเลิกการหน่วงเวลา และทำการส่งข้อมูลในทันทีได้ จากนั้นระบบจะส่งข้อมูลของผู้ป่วยเช่น ประวัติส่วนตัว อาการและพิกัดจีพีเอสไปยังเซิฟเวอร์เพื่อทำการประมวลผลต่อไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.2. ระบบช่วยตัดสินใจ

ในส่วนของระบบช่วยตัดสินใจนั้นแบ่งการทำงานออกเป็น 3 ส่วน คือ

1. ส่วนที่ทำการรับข้อมูล โดยจะรับข้อมูลจากการแจ้งเหตุของผู้ป่วย ข้อมูลเกี่ยวกับรถพยาบาล และข้อมูลของโรงพยาบาล
2. ส่วนประมวลผลข้อมูลและเปรียบเทียบข้อมูลเพื่อค้นหาเส้นทางที่เหมาะสม
3. ส่วนติดต่อกับเจ้าหน้าที่ในการแสดงผลข้อมูล



รูปที่ 6. หน้าจอปฏิบัติงานของเจ้าหน้าที่สำหรับรับการแจ้งเหตุฉุกเฉินต่างๆ

Path No.	Ambulance	Hospital	Path info	Estimate distance
1	ID:001(B)	LADKRABANG		3.9 KM
2	ID:001(B)	CHULARUT 7		4.1 KM
3	ID:002(A)	CHULARUT7		4.7 KM
4	ID:003(B)	LADKRABANG		5 KM

รูปที่ 7. ตารางเปรียบเทียบเส้นทางการนำส่งผู้ป่วย



รูปที่ 8. ข้อมูลเส้นทางที่ใช้ในการนำส่งผู้ป่วย

หลังจากระบบรับข้อมูลการแจ้งเหตุจากผู้ป่วยแล้ว ข้อมูลดังกล่าวจะถูกแสดงผลออกมาดังตัวอย่างในรูปที่ 6 ซึ่งจะแสดงหน้าจอระบบช่วยตัดสินใจของเจ้าหน้าที่ โดยจะแสดงผลตำแหน่งของจุดเกิดเหตุ รถพยาบาล และโรงพยาบาลที่อยู่ใกล้กับจุดเกิดเหตุลงบนแผนที่ จากนั้นจึงทำการประมวล และแสดงผลออกมาในรูปแบบตารางแนะนำเส้นทางดังรูปที่ 7 ซึ่งเรียงลำดับตามระยะทางจากรถพยาบาล ไปยังจุดเกิดเหตุรวมกับระยะทางจากจุดเกิดเหตุไปยังโรงพยาบาลที่ใกล้ที่สุด และจะแสดงผลข้อมูลระดับของรถพยาบาลซึ่งมีอยู่ทั้งหมด 4 ระดับ[1] แบ่งตามความพร้อมของอุปกรณ์ช่วยเหลือที่มีอยู่บนรถพยาบาลนั้นๆ (ในรูปที่ 7 สมมุติว่ามีรถพยาบาลระดับ A และ B อยู่ในบริเวณที่มีการแจ้งเหตุ) โดยเจ้าหน้าที่จะทำการเลือกเส้นทางและรถพยาบาลที่เหมาะสมกับผู้ป่วย และส่งข้อมูลเส้นทางดังรูปที่ 8 ไปยังเจ้าหน้าที่ประจำรถพยาบาลผ่านทางเว็บไซต์ โดยจะนำเส้นทางที่ได้ไปแสดงผลบนอุปกรณ์ระบุพิกัดจีพีเอสที่ติดตั้งอยู่บนรถพยาบาล เพื่อให้เจ้าหน้าที่ประจำรถพยาบาลสามารถทำการช่วยเหลือผู้ป่วยได้อย่างรวดเร็ว

4. การประเมินและวิเคราะห์การทำงาน

เมื่อเปรียบเทียบกับระบบเก่าแล้ว[6] งานชิ้นนี้จะมีความแตกต่างจากระบบเก่าตามตารางต่อไปนี้

ตารางที่ 1. ตารางการเปรียบเทียบระบบ

รูปแบบการทำงาน	ระบบเดิม	ระบบใหม่
วิธีการแจ้งเหตุ	โทรศัพท์	แอพพลิเคชั่นบนสมาร์ทโฟน
ประวัติส่วนตัวของผู้ป่วย	ไม่ทราบ	ทราบ
การระบุตำแหน่ง	แจ้งผ่านโทรศัพท์	พิกัดจีพีเอส
การจัดการทรัพยากร	ไม่มี	มี
ระบบช่วยตัดสินใจ	ไม่มี	มี
การระบุอาการ	แจ้งผ่านโทรศัพท์	แอพพลิเคชั่นบนสมาร์ทโฟน
การป้องกันการแจ้งข้อมูลเท็จ	ไม่มี	ไม่มี

จากตารางที่ 1. ระบบที่นำเสนอจะสามารถแจ้งเหตุฉุกเฉินได้รวดเร็วกว่าเมื่อเปรียบเทียบการแจ้งเหตุผ่านโทรศัพท์ซึ่งต้องระบุทั้งที่อยู่ และอาการของผู้ป่วย ในขณะที่การใช้พิกัดจีพีเอสสามารถระบุตำแหน่งได้แม่นยำและใช้เวลาน้อยกว่าเพียงกดปุ่มบนสมาร์ทโฟนซึ่งใช้เวลาเพียงไม่กี่วินาที รวมทั้งสามารถระบุอาการของผู้ป่วยได้พร้อมกัน แต่อาจมีข้อเสียในเรื่องความละเอียดของอาการที่สามารถระบุได้ แต่ถ้าคำนึงถึงสภาวะของผู้ป่วยที่แตกต่างกันในกรณีที่ผู้ป่วยมีสติไม่มากพอที่จะสื่อสารได้ ระบบเก่าจะไม่สามารถทำงานได้เลย ในขณะที่ระบบใหม่ใช้ปริมาณการตัดสินใจน้อยกว่าการโทรศัพท์มาก ในส่วนปัญหาด้านความคลาดเคลื่อนของการระบุตำแหน่งจีพีเอส อาจส่งผลต่อความแม่นยำในการคำนวณเส้นทางในการนำส่งผู้ป่วยได้ แต่ปัญหานี้สามารถถูกแก้ไขได้ด้วยการอัพเดทพิกัดจีพีเอสใหม่ โดยระบบจะมีการอัพเดทพิกัดจีพีเอสของผู้ป่วยอยู่เป็นระยะ ดังนั้นปัญหานี้จึงได้รับการแก้ไขอย่างอัตโนมัติ ในด้านการจัดการทรัพยากร ระบบเก่าไม่มีการแสดงข้อมูลรถนำส่งทั้งหมดที่สามารถปฏิบัติการได้ในขณะนั้น จึงทำให้การตัดสินใจของเจ้าหน้าที่อาจผิดพลาดได้ ในส่วนของระบบช่วยตัดสินใจที่เพิ่มเข้ามาจะทำให้เจ้าหน้าที่สามารถทำงานได้ง่ายและรวดเร็วขึ้น แต่อย่างไรก็ตามระบบใหม่ก็ยังไม่สามารถป้องกันปัญหาการแจ้งข้อมูลเท็จได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. บทสรุป

โดยสรุปการใช้สมาร์ทโฟนเข้ามาช่วยในการแจ้งเหตุฉุกเฉินสามารถทำให้การแจ้งเหตุฉุกเฉินเป็นไปได้อย่างรวดเร็วและง่ายขึ้น โดยลดการสื่อสารระหว่างผู้ป่วยกับเจ้าหน้าที่เป็นการแจ้งเหตุผ่านแอพพลิเคชั่นและแจ้งตำแหน่งผ่านพิกัดจีพีเอส รวมทั้งระบบใหม่ยังมีระบบช่วยตัดสินใจเพื่อให้การช่วยเหลือมีโอกาสประสบความสำเร็จสูงขึ้นจากระยะเวลาที่ลดลง คุณภาพและปริมาณของข้อมูลที่ใช้ในการช่วยเหลือผู้ป่วยมีมากขึ้น แต่ระบบที่นำเสนอก็ยังไม่สามารถแก้ปัญหาการแจ้งข้อมูลเท็จได้ รวมทั้งมีข้อจำกัดด้านการใช้งานระบบ โดยสมาร์ทโฟนที่จะสามารถใช้งานแอพพลิเคชั่นนี้ได้ต้องสามารถเชื่อมต่ออินเตอร์เน็ตได้ในขณะที่ทำการแจ้งเหตุฉุกเฉินและต้องสนับสนุนการใช้งานระบบระบุพิกัดบนพื้นโลกได้

6. แนวทางการพัฒนาต่อยอด

6.1. แอพพลิเคชั่นบนสมาร์ทโฟน

ในส่วนของแอพพลิเคชั่นบนสมาร์ทโฟนมีส่วนที่พัฒนาต่อยอด ได้แก่ การเพิ่มเติมระบบการแจ้งเหตุอัตโนมัติโดยใช้ประโยชน์จากระบบเซนเซอร์บนสมาร์ทโฟน ซึ่งจะทำการตรวจสอบรูปแบบการเขย่าที่ผิดปกติที่สามารถสันนิษฐานได้ว่า ผู้ใช้เกิดการล้มหรือเกิดอุบัติเหตุหรือไม่ อีกทั้งการส่งข้อมูลรูปถ่ายที่เกิดเหตุหรือบริเวณจุดเกิดเหตุเพื่อเพิ่มข้อมูลในการตัดสินใจให้แก่เจ้าหน้าที่ได้ และเพิ่มฟังก์ชั่นการแจ้งเหตุผ่านทางโทรศัพท์ไปยังเจ้าหน้าที่เพื่อแจ้งข้อมูลเพิ่มเติมทันทีหลักจากมีการแจ้งเหตุฉุกเฉินผ่านทางแอพพลิเคชั่นบนสมาร์ทโฟน

6.2. ระบบช่วยตัดสินใจ

ในส่วนของระบบช่วยตัดสินใจสามารถพัฒนาในส่วนของความแม่นยำในการระบุตำแหน่งของผู้ป่วย เช่น การใช้ Altitude ในการคำนวณความสูงของจุดเกิดเหตุในกรณีที่ผู้ป่วยประสบอุบัติเหตุในอาคารที่มีความสูงหลายชั้น และเพิ่มความฉลาดของระบบช่วยตัดสินใจให้สามารถระบุจุดเกิดเหตุที่ละเอียดยิ่งขึ้นจากการคาดเดาพฤติกรรม และสถานที่ที่ผู้ใช้นำสมาร์ทโฟนไปบ่อยครั้ง ซึ่งมีโอกาสจะเกิดเหตุได้ เช่น บ้าน ที่ทำงาน หรือสถานที่ที่ไปเป็นกิจวัตรประจำวัน

เอกสารอ้างอิง

[1] สถาบันการแพทย์ฉุกเฉินแห่งชาติ. "รายงานประจำปี 2554 สถาบันการแพทย์ฉุกเฉินแห่งชาติ". พิมพ์ครั้งที่ 1, มีนาคม, 2555.

[2] คำรณ ไชยศิริ, วิทยา ชาติบัญชาชัย. "การประเมินผลโครงการพัฒนาระบบบริการการแพทย์ฉุกเฉินโดยความร่วมมือระหว่างภาครัฐ ภาคเอกชนและองค์กรปกครองส่วนท้องถิ่นจังหวัดขอนแก่น". วารสารวิชาการสาธารณสุข, ปีที่ 17, ฉบับเพิ่มเติม 4 (มีนาคม-เมษายน), 2551.

[3] Sheng-Cheng Yeh, Wu-Hsiao Hsu, Ming-Yang Su, Ching-Hui Chen and Ko-Hung Liu. "A Study on Outdoor Positioning Technology Using GPS and WiFi Networks". Proceedings of the 2009 IEEE International Conference on Networking, Sensing and Control, Okayama, Japan, March 26-29, 2009.

[4] Ankur Chandra, Shashank Jain, Mohammed Abdul Qadeer. "GPS Locator: An Application for Location Tracking and Sharing using GPS for Java Enabled Handhelds". 2011 IEEE International Conference on Computational Intelligence and Communication Systems, 2011.

[5] Ghaith Bader Al-Suwaidi, Mohamed Jamal Zemerly. "Locating Friend and Family Using Mobile Phones with Global Positioning System (GPS)". 2009 IEEE, 2009.

[6] สถาบันการแพทย์ฉุกเฉินแห่งชาติ. "ระบบสารสนเทศการแพทย์ฉุกเฉิน". http://ws.emit.go.th/items_front/CallCenter.aspx.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การประยุกต์ใช้สมาร์ทโฟนเพื่อการพิสูจน์ตัวตนด้วยข้อมูลพิกัดจีพีเอส

สุเมธ ประภาวัต นิติ ชัยกะเสวี ภรภัทร นนทะบรรหาญ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพฯ

Emails: sumet@it.kmitl.ac.th, numnoiiniti@hotmail.com, alllives@live.com

บทคัดย่อ

การทำธุรกรรมผ่านบัตรเครดิตนั้นจะทำอย่างไรให้มีความปลอดภัยและยืนยันได้ว่าผู้ที่ทำธุรกรรมเป็นเจ้าของบัตรตัวจริง ซึ่งการซื้อสินค้าผ่านบัตรเครดิตนั้นมีความสะดวกสบายอย่างมาก แต่ก็แฝงไปด้วยภัยต่างๆ ที่ตามมา และปัจจุบันความสามารถของโทรศัพท์สมาร์ทโฟนที่เหนือกว่าโทรศัพท์มือถือพื้นฐานทั่วไป ทำให้โทรศัพท์สมาร์ทโฟนกลายเป็นอุปกรณ์สื่อสารที่มีผู้คนนิยมใช้อย่างมาก ภายในโทรศัพท์สมาร์ทโฟนจะมีเครื่องรับสัญญาณตำแหน่งดาวเทียมหรือจีพีเอส ซึ่งสามารถนำมาประยุกต์ใช้ประโยชน์ได้มากมาย หนึ่งในนั้นคือการระบุตำแหน่งเพื่อยืนยันตัวตนของผู้ใช้โดยจีพีเอส โดยจะใช้ประกอบกับการทำธุรกรรมทางการเงินผ่านบัตรเครดิต ทำให้ผู้ใช้มีความปลอดภัยจากผู้ไม่ประสงค์ดีที่จะทำการบิดเบือนข้อมูลที่มีความสำคัญไปหรือโจรกรรมบัตรเครดิตเพื่อนำไปใช้โดยผิดกฎหมาย

คำสำคัญ-- โทรศัพท์สมาร์ทโฟน; จีพีเอส; ธุรกรรมบัตรเครดิต

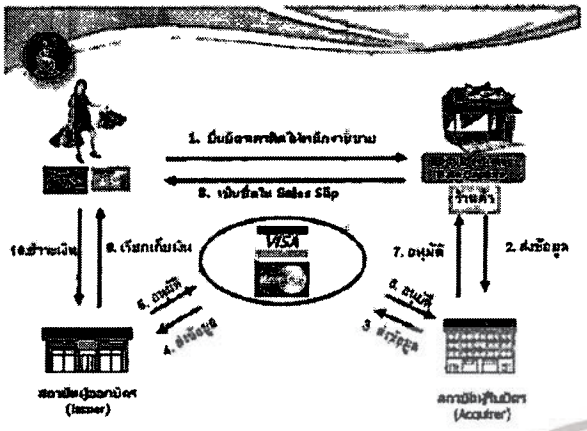
1. บทนำ

บัตรเครดิตได้เข้ามามีบทบาทในการทำธุรกรรมทางการเงินของผู้บริโภคมากขึ้น เพราะมีความสะดวกสบายในการซื้อสินค้าต่างๆ โดยไม่จำเป็นต้องพกเงินสดจำนวนมาก ทั้งนี้ยังได้รับสิทธิในรายการส่งเสริมการขายมากกว่าการซื้อด้วยเงินสด ซึ่งในปัจจุบันมีบัตรเครดิตและบัตรเดบิตรวมกันทั้งสิ้นกว่า 72 ล้านใบ [1] และมีเครื่องรูดบัตรมากกว่าสองแสนเครื่อง [2] นอกจากนั้นบัตรเครดิตยังสามารถซื้อสินค้าออนไลน์ซึ่งมีให้เลือกมากมายและสะดวกกว่าเดินไปซื้อตามร้านค้า ทำให้การทำธุรกรรมทางการเงินในปัจจุบัน บัตรเครดิตจะเป็นสื่อกลางหลักที่ผู้บริโภคนิยมใช้และได้รับการตอบรับอย่างดีจากร้านค้า ในส่วนของโทรศัพท์มือถือได้กลายมาเป็นปัจจัยสำคัญในการดำเนินชีวิตมนุษย์ในปัจจุบัน ต่อมาเมื่อโทรศัพท์มือถือได้รับการพัฒนาอย่างก้าวกระโดดจนกลายเป็นโทรศัพท์สมาร์ทโฟนที่มีความสามารถหลากหลาย เช่นการเชื่อมต่ออินเตอร์เน็ต ดาวน์โหลดแอพพลิเคชัน หรือการใช้งาน GPS ซึ่งสามารถรับพิกัดตำแหน่งของผู้ใช้ได้ว่าอยู่ส่วนใดบนแผนที่โลก จากการที่เทคโนโลยีของการซื้อขายแลกเปลี่ยนสินค้าและเทคโนโลยีของโทรศัพท์สมาร์ทโฟนมีการพัฒนาไปอย่างต่อเนื่อง แต่ความปลอดภัยในการซื้อขายนั้นยังไม่มีการเพิ่มประสิทธิภาพมากนัก โครงการนี้จึงจะทำการเพิ่มความปลอดภัยในการซื้อสินค้าผ่านบัตรเครดิต โดยมีการนำ GPS ของสมาร์ทโฟนมาประยุกต์ใช้ในการยืนยันและระบุตัวตนว่าบุคคลผู้เป็นเจ้าของบัตรเครดิตนั้นอยู่ในสถานที่นั้นจริงขณะทำธุรกรรม

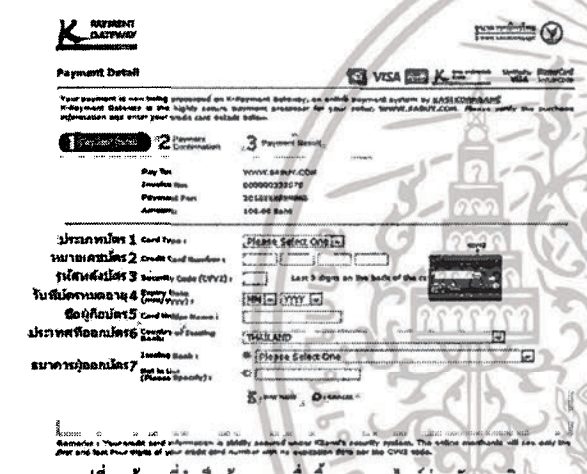
2. ทฤษฎีและงานที่เกี่ยวข้อง

กระบวนการซื้อสินค้าผ่านบัตรเครดิต[3][4] ผู้ซื้อต้องทำการยื่นบัตรเครดิตให้กับพนักงานขาย จากนั้นพนักงานขายจะนำบัตรเครดิตไปรูดที่เครื่องรูดบัตร (Electronic Data Capture: EDC) ซึ่งอาจเป็นของธนาคาร หรือ Non-bank แห่งอื่น ๆ ซึ่งเรียกว่า สถาบันผู้รับบัตร หรือ Acquirer จากนั้น เครื่อง EDC จะส่งข้อมูลกลับไปยังสถาบันผู้รับบัตร สถาบันผู้รับบัตรจะส่งข้อมูลต่อไปยังศูนย์เครือข่ายบัตรเครดิต (เช่น VISA หรือ MASTER CARD เป็นต้น) จากนั้นศูนย์เครือข่ายบัตรเครดิตจะส่งข้อมูลไปยังธนาคาร หรือ Non-bank ที่เป็นผู้ออกบัตรเครดิตนั้น ซึ่งเรียกว่า สถาบันผู้ออกบัตร หรือ Issuer เพื่อขออนุมัติการใช้บัตรเครดิต สถาบันผู้ออกบัตรจะตรวจสอบวงเงินว่ามีเพียงพอหรือไม่ และแจ้งการอนุมัติกลับไปยังศูนย์เครือข่ายบัตรเครดิต ศูนย์เครือข่ายบัตรเครดิตจะแจ้งการอนุมัติกลับไปยังสถาบันผู้รับบัตร สถาบันผู้รับบัตรจะแจ้งการอนุมัติกลับไปยังร้านค้าเพื่อพิมพ์ใบบันทึกการขาย (Sales Slip) จากนั้นผู้ซื้อต้องทำการตรวจสอบความถูกต้องของใบบันทึกรายการขาย (Sales Slip) ก่อนที่จะเซ็นชื่อ ซึ่งการเซ็นชื่อเป็นการยืนยันตัวตนเพียงอย่างเดียวเท่านั้น ซึ่งมีความเสี่ยงที่จะมีการปลอมแปลงลายเซ็นได้ เพราะบัตรเครดิตจะไม่ปรากฏภาพของเจ้าของบัตร เมื่อเซ็นเสร็จเรียบร้อยแล้วให้เก็บ Sales Slip ไว้เป็นหลักฐานการชำระเงินเพื่อตรวจสอบกับใบแจ้งหนี้การชำระเงิน สถาบันผู้ออกบัตรจะจัดส่งใบแจ้งหนี้ให้ผู้ซื้อก่อนครบกำหนดชำระเงิน โดยผู้ซื้อควรชำระค่าใช้จ่ายตามยอดหนี้ที่ระบุในใบแจ้งหนี้ให้แก่สถาบันผู้ออกบัตรภายในเวลาที่กำหนด ไม่เช่นนั้น ต้องเสียค่าดอกเบี้ยและค่าบริการต่าง ๆ โดยกระบวนการทำงานทั้งหมดสามารถสรุปเป็นแผนภาพได้ดังรูปที่ 1.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 1. ขั้นตอนการทำงานของบัตรเครดิต



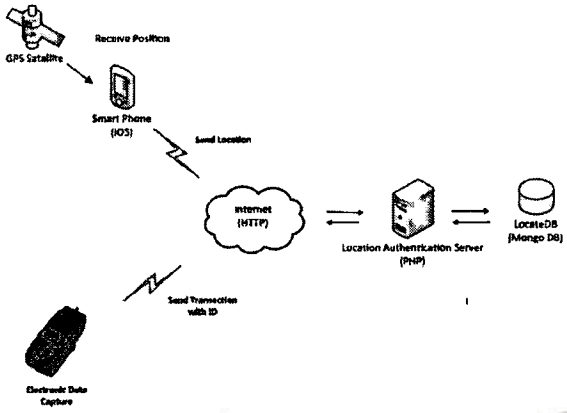
รูปที่ 2. ข้อมูลที่จำเป็นต้องกรอกเมื่อซื้อของออนไลน์ผ่านบัตรเครดิต

จากรูปที่ 2. จะเป็นรายละเอียดที่ต้องกรอกข้อมูลเมื่อมีการซื้อสินค้าออนไลน์ผ่านบัตรเครดิต[5] เว็บไซต์ส่วนมากจะใช้หมายเลขบัตรเครดิต 16 หลัก รหัสหลังบัตร (Security Code) 3 หลัก วันที่บัตรหมดอายุและชื่อผู้ถือบัตรประกอบกันเพื่อยืนยันตัวตนของผู้ซื้อ ซึ่งข้อมูลทั้งหมดที่กล่าวไว้ข้างต้นจะปรากฏอยู่บนบัตรเครดิตทั้งหมด ผู้ใดที่มีข้อมูลดังกล่าวสามารถซื้อสินค้าออนไลน์ได้

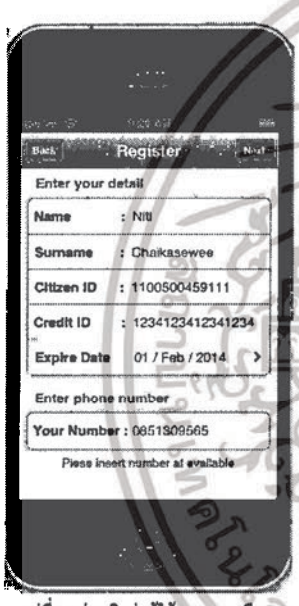
3. แนวคิดการดำเนินงาน

การทำงานโดยรวมนั้นสามารถสรุปเป็นใจความสาคัญได้คือ "ไม่มีสมาร์ทโฟน ไม่มีการซื้อขาย" โดยจะใช้โทรศัพท์สมาร์ทโฟนเป็นเครื่องมือหลักในการระบุตำแหน่งของผู้ใช้ ซึ่งจะไปซื้อสินค้า ณ ร้านค้าต่างๆ ที่มีเครื่องรูดบัตรเครดิต โดยในขั้นแรกผู้ใช้ต้องลงทะเบียนบัตรเครดิต โดยใช้ข้อมูลพื้นฐานที่ปรากฏบนบัตรเครดิต เพื่อให้บัตรเครดิตกับสมาร์ทโฟนมีความสัมพันธ์กันและเมื่อต้องการซื้อสินค้ากับบัตรเครดิตที่ทำการลงทะเบียนไว้แล้ว ให้ทำการเปิดแอพพลิเคชันในโทรศัพท์สมาร์ทโฟนขึ้นมา และกดปุ่ม "Send Location" เพื่อส่งตำแหน่งปัจจุบันของผู้ใช้ (สามารถใช้ได้ 30 นาที โดยไม่ต้องกดทุกครั้งที่มีการซื้อ) และเมื่อมีข้อมูลตำแหน่งปัจจุบันของผู้ซื้อจึงสามารถซื้อสินค้าตามปรกติ แต่หากไม่สะดวกที่จะต้องเข้ามาอัพเดทข้อมูลทุกๆ 30 นาที ผู้ใช้สามารถตั้งค่าให้แอพพลิเคชันส่งข้อมูลพิกัดโดยอัตโนมัติแทนได้ แต่การส่งข้อมูลอัตโนมัติจะสูญเสียพลังงานมากเมื่อเปรียบเทียบกับการกดอัพเดทข้อมูลทีละครั้งเมื่อต้องการซื้อสินค้า เมื่อมีการรูดบัตรเครื่องรูดบัตรจะทำการส่งพิกัดและข้อมูลเกี่ยวกับการซื้อไปยังเครื่องเซิร์ฟเวอร์ แต่เนื่องจากเครื่องรูดบัตรเครดิตไม่สามารถที่จะส่งข้อมูลพิกัดบนแผนที่ไปยังเครื่องเซิร์ฟเวอร์ได้โดยตรง เพราะไม่มีจีพีเอสติดตั้งอยู่ภายในเครื่อง ซึ่งระบบจะใช้วิธีการเก็บข้อมูลพิกัดเครื่องรูดบัตรตั้งแต่ที่ร้านค้าขอเครื่องรูดบัตรไปติดตั้งที่ร้าน โดยนำตำแหน่งร้านไปค้นหาพิกัดและเก็บข้อมูลพิกัดไว้ในฐานข้อมูล เมื่อข้อมูลจากเครื่องรูดบัตรส่งมาถึงเครื่องเซิร์ฟเวอร์ เครื่องเซิร์ฟเวอร์จะเปรียบเทียบกับพิกัดของผู้ใช้ที่ส่งมาก่อนว่าอยู่ในระยะใกล้เคียงหรือไม่ สำหรับการซื้อขายออนไลน์นั้นมีลักษณะเดียวกัน คือเมื่อต้องการซื้อสินค้าให้ทำการส่งข้อมูลพิกัดปัจจุบันไปก่อน และเมื่อกรอกข้อมูลที่หน้าเว็บไซต์ที่ทำการซื้อสินค้า จะต้องกรอกชื่อเมือง อำเภอ(เขต) และตำบล(แขวง) โดยใช้ AJAX เข้ามาช่วยในการหาชื่อเมืองให้ไวขึ้น หากพิมพ์ "S" ภายในช่องที่ให้กรอก จะขึ้นคำว่า "Samutprakarn" "Samutsakorn" "Samutsongkram" เพื่อให้ผู้ใช้ไม่พิมพ์ชื่อต่างๆ ผิด การตรวจสอบพิกัดในการซื้อสินค้าผ่านเครื่องรูดบัตรและซื้อสินค้าออนไลน์จะมีความเหมือนกันคือหากพิกัดของผู้ซื้อไม่ได้อยู่ในบริเวณที่ผู้ใช้ซื้อสินค้า เซิร์ฟเวอร์จะส่งการแจ้งเตือนไปยังโทรศัพท์สมาร์ทโฟนเพื่อให้ยืนยันคำสั่งซื้อหรือสามารถกดยกเลิกเพื่อไม่ให้เกิดการซื้อขายขึ้น การอิมพลิเมนท์ระบบจำเป็นต้องเพิ่มเครื่องเซิร์ฟเวอร์และระบบฐานข้อมูลลงไปเพื่อเก็บข้อมูลที่จำเป็น โดยเซิร์ฟเวอร์ที่เพิ่มเข้ามาจะเชื่อมต่อกับสถาบันผู้รับบัตร (Acquirer) โดยเป็นจุดแรกที่เครื่องรูดบัตรส่งข้อมูลมาถึง ทำให้ลดการส่งข้อมูลตั้งแต่ต้นทาง กระบวนการทำงานของระบบที่สร้างขึ้นมาใหม่แสดงดังรูปที่ 3. โครงสร้างของระบบ ในส่วนของระบบปฏิบัติที่ใช้ในโทรศัพท์สมาร์ทโฟนคือ iOS[6] โดยมีเครื่องเซิร์ฟเวอร์ที่ใช้ภาษา PHP และฐานข้อมูลจะใช้ NOSQL ในการอิมพลีเมนท์ ซึ่งสาเหตุที่ใช้ NOSQL นั้นเพราะว่ามีความรวดเร็วในการทำงานและสามารถขยายฐานข้อมูลต่อไปในอนาคตได้โดยมีข้อจำกัดไม่มากเมื่อเทียบการฐานข้อมูลแบบมี Relation ที่จำเป็นต้องมีแบบ ER Model และทำการ Normalize เพื่อให้ตารางมีความซ้ำซ้อนน้อยที่สุด และในส่วนของส่วนติดต่อผู้ใช้ในโทรศัพท์สมาร์ทโฟนจะออกแบบให้เรียบง่าย และสื่อความหมายชัด จากรูปที่ 4. คือการลงทะเบียนโทรศัพท์สมาร์ทโฟนให้เชื่อมโยงกับบัตรเครดิต และหลังจากลงทะเบียนเมื่อเปิดแอพพลิเคชันจะปรากฏปุ่ม "Send Location" ดังปรากฏในรูปที่ 5. ในส่วนของมีการแจ้งเตือนแบบพุชโนทิฟิเคชันจะแจ้งเตือนเมื่อตำแหน่งของโทรศัพท์สมาร์ทโฟนและบริเวณที่ทำการซื้อขายไม่ใกล้เคียงกัน ดังปรากฏในรูปที่ 6. ในส่วนของเซิร์ฟเวอร์จะสามารถ เพิ่ม ลบ และแสดงข้อมูลของผู้ใช้แต่ละคนได้ โดยการเข้าสู่ระบบจำเป็นต้องมีการ Log in ก่อน เพื่อความปลอดภัยของข้อมูลผู้ใช้ ซึ่งเป็นข้อมูลที่มีความสำคัญมาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



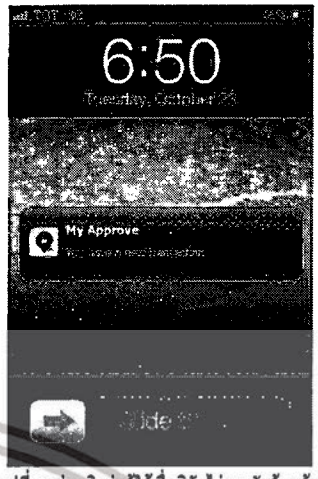
รูปที่ 3. โครงสร้างของระบบ



รูปที่ 4. ส่วนติดต่อผู้ใช้การลงทะเบียน



รูปที่ 5. ส่วนติดต่อผู้ใช้การส่งพิกัด



รูปที่ 6. ส่วนติดต่อผู้ใช้เมื่อพิกัดไม่ตรงกับร้านค้า



รูปที่ 7. ส่วนติดต่อผู้ใช้ของเซิร์ฟเวอร์

4. วิเคราะห์การทำงานและประเมินผล

การทำงานจะเริ่มขึ้นเมื่อผู้ใช้กดส่งข้อมูลพิกัดไปยังเครื่องเซิร์ฟเวอร์โดยข้อมูลพิกัดนี้มีระยะการใช้งานได้เพียง 30 นาทีเท่านั้น โดยภายในระยะเวลา 30 นาที ลูกค้าจะสามารถซื้อสินค้าร้านใดก็ได้ภายในบริเวณที่กดส่งข้อมูลพิกัดไป แต่หากหมดเวลา 30 นาทีจะมีการแจ้งเตือนว่าหมดเวลาและให้ส่งเข้าไปใหม่หากต้องการซื้อสินค้าเพิ่มเติม หากไม่ส่งข้อมูลพิกัดใหม่จะไม่สามารถซื้อสินค้าใดๆ ได้อีก หรือผู้ใช้อาจจะเลือกการส่งพิกัดอัตโนมัติ สามารถซื้อสินค้าได้ตลอดเวลาโดยไม่ต้องกดส่งใหม่ทุกครั้ง แต่อาจส่งผลกระทบต่อระดับพลังงานภายในโทรศัพท์สมาร์ทโฟนได้ ในส่วนของเครื่องเซิร์ฟเวอร์ซึ่งต้องคอยรับข้อมูลจากโทรศัพท์สมาร์ทโฟนและจากเครื่องรูดบัตรเพื่อนำมาประมวลผลข้อมูล โดยข้อมูลที่เข้ามาจะมีจำนวนมากเพราะการซื้อขายจะเกิดขึ้นตลอดเวลา จำนวนข้อมูลที่เข้าไปในเซิร์ฟเวอร์จะมีจำนวนมาก ซึ่งจำเป็นต้องใช้เซิร์ฟเวอร์จำนวนมาก เพื่อช่วยในการประมวลผลและจัดเก็บเซสชันที่เข้ามา ดังนั้นหากนำแอพพลิเคชันนี้ไปใช้ร่วมกับการซื้อขายจริงผ่านบัตรเครดิตจะลดปัญหาต่างๆ มากมายอาทิ เช่น การโจรกรรมบัตรเครดิตเพื่อนำบัตรเครดิตนั้นไปซื้อสินค้าต่างๆ โดยที่เจ้าของบัตรไม่รู้ เพราะผู้โจรกรรมจะไม่สามารถซื้อสินค้าได้เลย หากไม่มีโทรศัพท์สมาร์ทโฟน เสมือนนำบัตรเครดิตที่หมดอายุแล้วไปใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. บทสรุป

แอพพลิชันนี้สามารถเพิ่มความปลอดภัยให้กับการใช้บัตรเครดิตให้ไม่สามารถที่จะรูดซื้อสินค้าโดยที่เจ้าของบัตรนั้นไม่ยินยอม โดยการใช้ข้อมูลจีพีเอสผ่านโทรศัพท์สมาร์ทโฟนมายืนยันตัวตนร่วมกับการใช้บัตรเครดิตในการทำธุรกรรมทางการเงิน ในส่วนของแอพพลิเคชันจะมีลักษณะเรียบง่าย เพียงกดส่งข้อมูลเท่านั้น โดยอาจจะส่งผลต่อเวลาในการทำธุรกรรมทางการเงินที่อาจจะเพิ่มขึ้นเล็กน้อย แต่สามารถเพิ่มความปลอดภัยให้กับบัตรเครดิตอย่างมาก หรือผู้ใช้อาจจะเลือกการส่งพิกัดอัตโนมัติ โดยสามารถสรุปได้ในตาราง 1. และตาราง 2.

ตาราง 1. เปรียบเทียบการซื้อด้วยบัตรเครดิตผ่านเครื่องรูดบัตรกับการใช้แอพพลิเคชันใหม่

	ระบบเดิม	แอพพลิเคชันใหม่
การยืนยันตัวตนเจ้าของบัตรเครดิต	ตรวจดูลายเซ็นต์ที่ใบเสร็จเปรียบเทียบกับหลังบัตรเครดิต	ใช้พิกัดข้อมูลจีพีเอสเปรียบเทียบกับตำแหน่งของร้าน
ช่องโหว่	ทุกคนสามารถใช้บัตรเครดิตได้ เพียงแต่เซ็นต์ชื่อให้มีความคล้ายกับเจ้าของบัตร	หากโทรศัพท์สมาร์ทโฟนหายหรือแบตเตอรีหมดจะไม่สามารถซื้อสินค้าได้
ภัย (Threat)	อาจมีผู้ไม่ประสงค์ดีนำบัตรเครดิตไปใช้โดยเจ้าของบัตรเครดิตไม่อนุญาต	-
จุดเด่น	รวดเร็ว	ปลอดภัย

ตาราง 2. เปรียบเทียบการซื้อด้วยบัตรเครดิตแบบออนไลน์กับการใช้แอพพลิเคชันใหม่

	ระบบเดิม	แอพพลิเคชันใหม่
การยืนยันตัวตนของเจ้าของบัตรเครดิต	รหัสบัตรเครดิต ข้อมูลหน้าบัตร และ Security Code 3 หลัก	ใช้พิกัดข้อมูลจีพีเอสเปรียบเทียบกับชื่อเมือง อำเภอและตำบลที่กำลังทำธุรกรรมปัจจุบัน
ช่องโหว่	ทุกคนสามารถซื้อสินค้าผ่านบัตรเครดิตได้ เพียงมีบัตรเครดิตและกรอกข้อมูลลงไป	หากโทรศัพท์สมาร์ทโฟนหายหรือแบตเตอรีหมดจะไม่สามารถซื้อสินค้าได้
ภัย (Threat)	อาจมีผู้ไม่ประสงค์ดีนำบัตรเครดิตไปใช้โดยเจ้าของบัตรเครดิตไม่อนุญาต	-
จุดเด่น	-	ปลอดภัย

เอกสารอ้างอิง

[1] ธนาคารแห่งประเทศไทย. "จำนวนบัตรพลาสติก". HTTP://WWW2.BOT.OR.TH/STATISTICS/DOWNLOAD/PS_PT_006_TH_ALL.XLS.

[2] ธนาคารแห่งประเทศไทย. "จำนวนเครื่องรับบัตร (EFTPOS TERMINAL)".HTTP://WWW2.BOT.OR.TH/STATISTICS/DOWNLOAD/PS_PT_007_TH_ALL.XLS

[3] ธนาคารแห่งประเทศไทย. "ขั้นตอนการใช้บัตรเครดิต". http://www.bot.or.th/Thai/FinancialLiteracy/creditcard/Pages/creditcard_4.aspx

[4] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอกนิกส์(องค์การมหาชน). "Focus Group Seminar เรื่อง Payment Card Standard". http://standard.etda.or.th/wp/?p=1

[5] บริษัท สนุก ช้อปปิ้ง จำกัด. "ชำระเงินผ่านบัตรเครดิตออนไลน์ (Credit Card)". http://sabuy.sanook.com/sites/help/seller/detail/30098

[6] Vandad Nahavandipoor. **"iOS 5 Programming Cookbook,"**. 1 st ed. New York : O'REILLY, 2011.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้