

การออกแบบรหัสเครือข่ายจากกราฟและการพัฒนารหัสแอลทีเชิงระบบ

NETWORK CODING DESIGN BASED ON GRAPH
AND SYSTEMATIC LT CODE DEVELOPMENT



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2559

KMITL-2016-EN-M-010-185

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

การออกแบบรหัสเครือข่ายจากกราฟและการพัฒนารหัสแอลทีเชิงระบบ

NETWORK CODING DESIGN BASED ON GRAPH
AND SYSTEMATIC LT CODE DEVELOPMENT



เลขหมู่.....
ลงทะเบียน 148734
ในเดือนปี
23 พ.ย. 2560

b. 00265360
i.

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2559

KMITL-2016-EN-M-010-185

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

NETWORK CODING DESIGN BASED ON GRAPH
AND SYSTEMATIC LT CODE DEVELOPMENT



A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF ENGINEERING IN TELECOMMUNICATIONS ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2016
KMITL-2016-EN-M-010-185

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



COPYRIGHT 2016



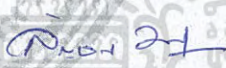


FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

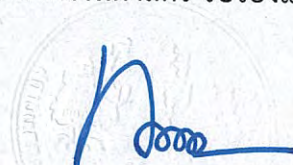
หัวข้อวิทยานิพนธ์ การออกแบบรหัสเครือข่ายจากกราฟและการพัฒนารหัสแอลทีเชิงระบบ
Thesis Title Network Coding Design based on Graph and Systemetic LT Code Development
นักศึกษา นายนคร เมืองบุญมา
รหัสประจำตัว 56601257
ปริญญา วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา วิศวกรรมโทรคมนาคม
อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.ณัฐกานต์ พุทธรักษ์
หมายเลขวิทยานิพนธ์ KMITL-2016-EN-M-010-185

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.พิสิฐ	บุญศรีเมือง	
ผศ.ดร.สุทธิชัย	นพนาศิพงษ์	
รศ.ดร.ลัญฉกร	วุฒิสิริทฤกุลกิจ	
ดร.เวธิต	ภาคพิสุทธิ	
ผศ.ดร.ณัฐกานต์	พุทธรักษ์	

วัน / เดือน / ปี ที่สอบ วันพฤหัสบดีที่ 6 ตุลาคม พ.ศ. 2559 เวลา 11.00-13.00 น.
สถานที่สอบ ณ อาคาร A ชั้น 5 ห้องประชุม 1

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

คณะวิศวกรรมศาสตร์ รับรองแล้ว



(รองศาสตราจารย์ ดร. คมสัน มาลีสี)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปเผยแพร่โดยไม่ขออนุญาต
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องขออนุญาตเผยแพร่เอกสารนี้แก่บุคคลอื่นที่มีการนำไปใช้
วันที่ 6 ตุลาคม พ.ศ. 2559

หัวข้อวิทยานิพนธ์	การออกแบบรหัสเครือข่ายจากกราฟ และการพัฒนารหัสแอลที่เชิงระบบ
นักศึกษา	นายนคร เมืองบุญมา
รหัสนักศึกษา	56601257
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมโทรคมนาคม
พ.ศ.	2559
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผศ.ดร. ญัฐกานต์ พุทธิรักษ์

บทคัดย่อ

เครือข่ายไร้สายมัลติคาสต์สำหรับการส่งข้อมูลไปยังกลุ่มของผู้รับผ่านโหนดส่งผ่านในเครือข่ายทั่วไปนั้น ถูกลดทอนประสิทธิภาพด้วยแบนด์วิธและความจุของระบบที่มีอย่างจำกัด การเพิ่มทราฟฟิค (Throughput) เป็นวิธีการหนึ่งที่จะเพิ่มประสิทธิภาพในการส่งข้อมูล ซึ่งเทคนิคการเข้ารหัสเครือข่ายสามารถช่วยเพิ่มค่าทราฟฟิคให้กับระบบได้ อย่างไรก็ตามการเข้ารหัสเครือข่ายเพียงอย่างเดียวนั้นจะช่วยเรื่องการเพิ่มค่าทราฟฟิคหรือไม่ขึ้นอยู่กับลักษณะของทอพอโลยีของระบบและความน่าเชื่อถือของการส่งข้อมูลในระบบเครือข่ายด้วย โดยเฉพาะอย่างยิ่งในเครือข่ายที่มีขนาดใหญ่ สมรรถนะของระบบจะถูกลดทอนด้วยความล่าช้าของข้อมูลที่ส่งมาถึงกลุ่มผู้รับหากมีเฟรมข้อมูลเสียหายเกิดขึ้น

วิทยานิพนธ์ฉบับนี้จึงนำเสนอการพัฒนาอัลกอริธึมและการสร้างรหัสเครือข่ายที่สามารถนำไปประยุกต์ใช้กับเครือข่ายไร้สายมัลติคาสต์เพื่อเพิ่มทราฟฟิคและลดความล่าช้าในการส่งข้อมูลซ้ำในกรณีที่มีเฟรมข้อมูลเกิดความเสียหายหรือสูญหาย ซึ่งได้แบ่งงานเป็นสองส่วน ส่วนแรกได้นำเสนออัลกอริธึมวิธีการเข้ารหัสแบบปรับตัวได้ (ANCR) โดยการเลือกแพ็กเก็ตเพื่อนำมาเข้ารหัส โดยพิจารณาจากคุณสมบัติไมเนอร์กกราฟที่แฝงอยู่ในทอพอโลยี ส่วนที่สองเป็นการสร้างรหัสเครือข่ายเชิงระบบ (SNC) โดยพัฒนารหัสแอลที่เชิงระบบซึ่งเป็นรหัสการแก้ไขความคลาดเคลื่อนชนิดหนึ่ง เพื่อลดความล่าช้าจากการส่งข้อมูลซ้ำเมื่อเกิดการสูญหายหรือเสียหาย และยังช่วยให้การส่งข้อมูลซ้ำนั้นสามารถทำได้จากโหนดข้างเคียงแทนที่จะต้องส่งจากโหนดผู้ส่งที่อยู่ห่างไกลออกไป สำหรับผลการทดลองที่ได้จากวิธีการเข้ารหัสแบบปรับตัวได้นั้นช่วยเพิ่มค่าทราฟฟิคให้สูงขึ้นและลดการใช้เวลาในการส่งอย่างเห็นได้ชัด โดยทราฟฟิคที่โหนดคอขวดเพิ่มขึ้นราว 35% และการใช้เวลาลดลงราว 30% สำหรับในรหัสเครือข่ายเชิงระบบช่วยเพิ่มความน่าเชื่อถือในการส่งข้อมูลให้สูงขึ้นด้วยการลดความล่าช้าของการส่งข้อมูลลงราว 40-70% และยังเพิ่มทราฟฟิคราว 8-19% เมื่อเทียบกับการส่งข้อมูลตามมาตรฐาน

Thesis Title NETWORK CODING DESIGN BASED ON GRAPH AND SYSTEMATIC LT CODE DEVELOPMENT

Student Mr. Nakhon Muangboonma

Student No. 56601257

Degree Master of Engineering

Program Telecommunications Engineering

Year 2016

Thesis Advisor Asst.Prof.Dr. Nattakan Puttarak

ABSTRACT

The wireless multicast network for delivering data to a set of destinations through relays in any network is degraded by a limited bandwidth and capacity regime. Increasing throughput is one of various techniques to improve network performance. Network coding technique can be used to increase the system throughput. However, the network coding might or might not increase throughput due to an unpredictable network topology and its reliability. Moreover, the performance of the network system especially in a large scale network is also degraded by a latency of retransmissions after some data frame has been lost.

This thesis proposes the algorithm development and construction of a network code that can be applied to a wireless multicast network in order to increase throughput and also capable to reduce a latency of retransmission of lost/erased data. This work is separated into 2 parts. The first part is an adaptive network coding-routing (ANCR) created to automatically select packets to construct a network code at a relay node before forwarding to destination based on the property of minors graph which is contained in the network topology. The second part is a systematic network code (SNC), which is developed from a kind of erasure code called systematic LT code. The objective of this code is to reduce a latency of retransmission when there are some lost/erased data and such retransmission can be made by neighbor nodes instead of transmitting from a remote source node. The results show that the ANCR technique can significantly increase throughput and also decrease timeslot usage. The throughput at a bottleneck relay node is increased by 35%, while the timeslot usage is decreased for more than 30%. In addition, the SNC technique can improve reliability and performance of a multicast network by

decreasing a latency of retransmission for 40-70 % and yet increasing throughput for more than 8-19% compared with a conventional method.



III
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

รายงานวิจัยฉบับสมบูรณ์นี้สำเร็จลุล่วงเป็นอย่างดี เนื่องจากการสนับสนุนจากบุคคลต่างๆ ลำดับแรกขอขอบพระคุณ ครอบครัวเมืองบุญมา สำหรับการสนับสนุนในทุกๆ ด้าน

ขอขอบคุณ ผศ.ดร.ณัฐกานต์ พุทธรักษ์ อาจารย์ผู้ควบคุมวิทยานิพนธ์ ที่คอยให้คำปรึกษาตลอดระยะเวลาในการทำวิจัย รวมถึงคณาจารย์ภาควิชาวิศวกรรมโทรคมนาคมที่ได้ประสิทธิ์ประสาทวิชาให้แก่ข้าพเจ้า

ขอขอบคุณสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) สำหรับทุนส่งเสริมนักวิจัยรุ่นใหม่

ขอบคุณพี่ๆ ในห้องแล็บปฏิบัติการด้านเทคโนโลยีด้านสื่อสารและการบันทึกข้อมูล สำหรับคำแนะนำต่างๆ ในการปรับปรุงงานวิจัยของข้าพเจ้า

นคร เมืองบุญมา



สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	I
บทคัดย่อภาษาอังกฤษ.....	II
กิตติกรรมประกาศ.....	IV
สารบัญ.....	V
สารบัญตาราง.....	VIII
สารบัญรูป.....	IX
บทที่ 1 บทนำ.....	1
1.1 ที่มาของงานวิจัย.....	1
1.2 ความมุ่งหมายและวัตถุประสงค์ของงานวิจัย.....	3
1.3 ขอบเขตของโครงการวิจัย.....	3
1.4 วิธีดำเนินการวิจัย.....	3
บทที่ 2 การทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง.....	5
2.1 โพรโตคอลควบคุมการใช้สื่อสัญญาณในเครือข่ายคอมพิวเตอร์.....	5
2.1.1 โพรโตคอลควบคุมการใช้สื่อสัญญาณ.....	5
2.1.2 โพรโตคอลสำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่.....	7
2.2 รหัสเครือข่าย.....	9
2.2.1 หลักมูลฐานของรหัสเครือข่าย.....	9
2.2.2 การประยุกต์ใช้รหัสเครือข่ายและงานวิจัยที่เกี่ยวข้อง.....	11
2.3 ทฤษฎีกราฟและการประยุกต์.....	17
2.3.1 ทฤษฎีกราฟ 4 สี.....	17
2.3.2 ทฤษฎีกราฟไมเนอร์.....	18
2.3.3 การเชื่อมโยงโครงสร้างรหัสพีชคณิตด้วยทอพอโลยี.....	20
2.4 รหัสน้ำพุ.....	27
2.4.1 รหัสแอสกี.....	28
2.4.2 การเข้ารหัสแอสกี.....	30
2.4.3 การถอดรหัสแอสกี.....	32
2.4.4 รหัสแอสกีเชิงระบบ.....	32

สารบัญ(ต่อ)

	หน้า
บทที่ 3 รหัสเครือข่ายแบบปรับตัวได้.....	34
3.1 อัลกอริธึมที่ได้นำเสนอ.....	34
3.1.1 แบบจำลองเครือข่าย.....	34
3.1.2 อัลกอริธึม ANCR.....	35
3.2 แบบจำลองช่องสัญญาณและการเข้ารหัสเครือข่าย.....	38
3.3 ผลการทดลอง.....	39
3.4 การวิเคราะห์ผลการทดลองและอัลกอริธึม.....	42
บทที่ 4 การพัฒนารหัสแอสที่เชิงระบบ.....	45
4.1 การออกแบบรหัสเครือข่ายเชิงระบบ.....	46
4.1.1 การเข้ารหัสเครือข่ายเชิงระบบ.....	46
4.1.2 กระบวนการตรวจสอบเมทริกซ์กำเนิด.....	50
4.1.3 การถอดรหัสเครือข่ายเชิงระบบ.....	53
4.2 การสร้างแผนการในการส่งข้อมูลซ้ำ.....	55
4.2.1 โหมดเฝ้าสังเกต.....	55
4.2.2 การวิเคราะห์อัตราเฟรมลบเลื่อนร่วม.....	59
4.3 การวัดผลและผลลัพธ์.....	60
4.3.1 ทอพอโลยีที่ใช้ทดสอบ.....	61
4.3.2 ผลลัพธ์.....	62
4.4 การวิเคราะห์ผลการทดลองและอัลกอริธึม.....	64
บทที่ 5 สรุปผลการวิจัยและข้อเสนอแนะ.....	66
5.1 ข้อเสนอแนะ.....	67
เอกสารอ้างอิง.....	68
ภาคผนวก.....	71
ภาคผนวก ก MATLAB Source code ของอัลกอริธึม ANCR.....	72
ภาคผนวก ข MATLAB Source code ของรหัส SNC.....	86

สารบัญ(ต่อ)

	หน้า
ภาคผนวก ค ผลงานที่ได้รับการตีพิมพ์ในวารสารและการประชุมวิชาการ.....	103
ข้อมูลประวัติผู้วิจัย.....	116



สารบัญตาราง

ตารางที่	หน้า
3.1 เปรียบเทียบฟิล์มเทียบกับแพ็คเกจมาตรฐาน.....	39
3.2 ค่าทรูพุดที่วัดได้.....	41



สารบัญรูป

รูปที่	หน้า
1.1 เครือข่ายแบบผีเสื้อที่ไม่มีการใช้รหัสเครือข่ายและเครือข่ายแบบผีเสื้อที่มีการใช้รหัสเครือข่าย.....	2
2.1 ประเภทของโพรโตคอล MAC	6
2.2 การค้นหาเส้นทางของโพรโตคอล AODV.....	7
2.3 โพรโตคอล AODV-BR เส้นทางหลักและเส้นทางสำรอง.....	8
2.4 รูปแบบทั่วไปของการเข้ารหัสเครือข่าย.....	9
2.5 ตัวอย่างการหาโอกาสในการเข้ารหัส.....	12
2.6 ตัวอย่างการเข้ารหัสเครือข่ายด้วยการเอ็กซ์คลูซีฟพอร์ระหว่าง 3 โหนด.....	14
2.7 ทอพอโลยีรูปดาวที่มีโหนดเฝ้าสังเกต.....	14
2.8 ฝั่งงานในการจำลองการส่งข้อมูลแบบเอ็กซ์คลูซีฟพอร์.....	16
2.9 แผนที่และความสัมพันธ์กราฟด้วยทฤษฎี 4 สี.....	18
2.10 การรวมเส้นเชื่อมและการตัดเส้นเชื่อมซึ่งเป็นการดำเนินการซึ่งใช้สำหรับกราฟไมเนอร์.....	19
2.11 กราฟไมเนอร์ในลักษณะต่างๆ (ก) กราฟไมเนอร์ K_3 (ข) กราฟไมเนอร์ $K_{3,3}$ (ค) กราฟไมเนอร์ K_4 (ง) กราฟไมเนอร์ K_5	19
2.12 กราฟไมเนอร์ K_4 (ก) ในเครือข่ายรูปผีเสื้อ (ข).....	21
2.13 กราฟเครือข่าย 2-minimal และกราฟต้นไม้ส่วนย่อย (subtree graph) ของเครือข่ายดังกล่าว.....	23
2.14 ข้อความคาดการณ์แบบ NC-Minor เมื่อเปรียบเทียบกับข้อความคาดการณ์แบบ Hadwiger.....	26
2.15 ช่องสัญญาณลบเลือนแบบไบนารี (Binary Erasure Channel, BEC).....	28
2.16 ความสัมพันธ์กราฟไบพาร์ไทท์ระหว่างโหนดข้อมูลและโหนดเข้ารหัส.....	28
2.17 เวกเตอร์ดีกรีแบบสุ่มเมื่อ $k = 10$ และ $f = 1$	30
2.18 เมทริกซ์กำเนิดของรหัสแอลที.....	31
2.19 ความสัมพันธ์เชิงระบบในเมทริกซ์ต้นกำเนิดของรหัสแอลที ด้วยอัตราส่วนร้อยละ (ก) 30% (ข) 50% (ค) 100%.....	33
2.20 ประสิทธิภาพของรหัสแอลทีเชิงระบบด้วยความสัมพันธ์เชิงระบบที่มีค่าแตกต่างกัน.....	33
3.1 เครือข่ายรูปผีเสื้อ.....	35
3.2 อัลกอริธึมของรหัสเครือข่ายแบบปรับตัวได้.....	37
3.3 ขั้นตอนวิธีที่การหาค่าของกราฟ.....	37
3.4 ไมเนอร์ K_4 ของเครือข่ายรูปผีเสื้อที่ได้จากกระบวนการหาค่าของกราฟ.....	38
3.5 ฟิลด์ของแพ็กเก็ตเอ็กซ์คลูซีฟพอร์เปรียบเทียบกับแพ็กเก็ตตามมาตรฐาน.....	38

สารบัญรูป(ต่อ)

รูปที่	หน้า
3.6 ค่าทรูพุดที่วัดได้ที่โหนดหมายเลข 3 (คอขวด) และโหนดหมายเลข 7 (ผู้รับ).....	40
3.7 จำนวนการเข้าใช้ช่องสัญญาณโดยมากที่สุดและโดยเฉลี่ยของระบบเครือข่ายที่ใช้อัลกอริธึม ANCR เปรียบเทียบกับการใช้เร้าตั้งโพรโตคอลแบบปกติ.....	41
3.8 ความสามารถในการลดการใช้งานช่องเวลาของเครือข่ายแบบ n-minimal.....	43
3.9 ความสามารถในการลดการใช้งานช่องเวลาของเครือข่ายแบบ n-minimal.....	44
4.1 การเปรียบเทียบระหว่างการกระจายตัวแบบโรบัสต์โซลิตอนและโซลิตอน.....	46
4.2 กระบวนการสุ่มโยนจากโหนดข้อมูลไปยังโหนดเข้ารหัส.....	47
4.3 เมทริกซ์ต้นกำเนิดทั่วไปที่ผ่านกระบวนการสุ่มโยน (Random throw).....	48
4.4 กระบวนการสร้างเมทริกซ์ต้นกำเนิดเชิงระบบของรหัสเครือข่ายเชิงระบบ.....	49
4.5 เมทริกซ์ต้นกำเนิดในรูปแบบเชิงระบบสำหรับรหัสเครือข่ายเชิงระบบ.....	50
4.6 ความสัมพันธ์กราฟไบพาร์ไทท์เชิงระบบสำหรับรหัสเครือข่ายเชิงระบบ.....	50
4.7 กราฟไบพาร์ไทท์ตัวอย่างในการพิจารณากระบวนการแอลที.....	51
4.8 การกระจายตัวของดีกรีในไบพาร์ไทท์กราฟระหว่างรหัสเครือข่ายเชิงระบบ รหัสแอลที และรหัสแอลทีเชิงระบบ.....	54
4.9 ประสิทธิภาพของรหัสเครือข่ายเชิงระบบเปรียบเทียบกับรหัสเครือข่ายทั่วไปและเครือข่ายที่ไม่มีการ เข้ารหัสในช่องสัญญาณแบบลบบเลื่อนได้ ซึ่งพิจารณาจากอัตราเฟรมลบบเลื่อนที่เกิดขึ้น.....	55
4.10 ทอพอโลยีที่ใช้ทดสอบคุณสมบัติของโหมดเผ้าสังเกต.....	56
4.11 แพ็กเก็ตที่แอบได้ยิน (Overheard) ด้วยคอมพิวเตอร์แล็ปท็อปหมายเลข 1.....	56
4.12 ขั้นตอนวิธีการส่งข้อมูลซ้ำด้วยโหนดข้างเคียงในรหัสเครือข่ายเชิงระบบ.....	57
4.13 การส่งแพ็กเก็ตเพื่อรักษาสถานะของการเชื่อมต่อและค่าอัตราการรับส่งข้อมูลสำเร็จ.....	58
4.14 การสร้างการเชื่อมต่อระหว่างโหนดผู้รับและโหนดข้างเคียง.....	59
4.15 อัตราส่วนร้อยละของความน่าจะเป็นที่จะเกิดเฟรมลบบเลื่อนร่วมในจำนวน 2-3 โหนดผู้รับ.....	60
4.16 เครือข่ายขนาดใหญ่และเครือข่ายรูปผีเสื้อ.....	61
4.17 ค่าทรูพุดที่วัดได้จากโหนดหมายเลข 3 และโหนดหมายเลข 6.....	62
4.18 การเปรียบเทียบค่าเฉลี่ยทรูพุดของโหนดหมายเลข 3 และหมายเลข 6 ระหว่างเครือข่ายที่มีรหัส เครือข่ายเชิงระบบ, เครือข่ายที่ใช้รหัสเครือข่ายทั่วไปและเครือข่ายที่ปราศจากการใช้รหัส เครือข่าย.....	63

สารบัญรูป(ต่อ)

รูปที่	หน้า
4.19 การเปรียบเทียบค่าเฉลี่ยของเวลาแฝงในการส่งข้อมูลของโหนดหมายเลข 3 และหมายเลข 6 ระหว่างเครือข่ายที่มีรหัสเครือข่ายเชิงระบบ, เครือข่ายที่ใช้รหัสเครือข่ายทั่วไปและเครือข่ายที่ปราศจากการใช้รหัสเครือข่าย.....	63
4.20 ความสามารถในการลดเวลาการส่งโดยรวมเมื่อเปรียบเทียบระหว่างระบบที่ส่งข้อมูลตามเร้าตั้งโพรโตคอลมาตรฐาน, ระบบที่มีรหัสเครือข่ายเชิงระบบ และระบบที่มีรหัสเครือข่ายเชิงระบบด้วยเงื่อนไขที่เหมาะสมที่สุด (ก) ในโหนดหมายเลข 3 (ข) ในโหนดหมายเลข 6.....	65



บทที่ 1

บทนำ

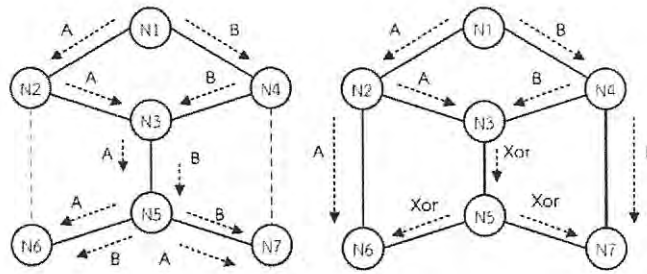
ในบทนี้จะกล่าวถึงที่มาและความสำคัญที่ทำให้เกิดงานวิจัยฉบับนี้ ที่ต้องการที่จะมุ่งเน้นไปที่การเพิ่มประสิทธิภาพของเครือข่ายในปัจจุบัน โดยเฉพาะอย่างยิ่งในเครือข่ายมัลติคาสต์ไร้สายที่ถูกลดทอนประสิทธิภาพด้วยเส้นทางคอขวด (Bottleneck) ซึ่งงานวิจัยนี้ได้ออกแบบอัลกอริทึมการเข้ารหัสซึ่งมีความยืดหยุ่นสามารถนำมาประยุกต์ใช้กับเครือข่ายไร้สายที่มีทอพอโลยีใดๆ ได้

1.1 ที่มาและความสำคัญของงานวิจัย

การสื่อสารข้อมูลผ่านระบบเครือข่ายในปัจจุบันนี้เป็นที่ทราบกันดีว่ามีแนวโน้มที่ต้องการความเร็วแม่นยำที่สูงขึ้น ในขณะที่ข้อมูลที่ต้องการส่งก็มีขนาดใหญ่ขึ้น ดังนั้นการติดต่อสื่อสารผ่านเครือข่ายไร้สายที่มีขนาดใหญ่มากและมีการเชื่อมต่อกันหลายโหนดจึงมีความจำเป็นอย่างยิ่งที่ต้องการความน่าเชื่อถือของข้อมูลในสภาวะการรบกวนของสิ่งแวดล้อมที่มีผลต่อความผิดพลาดในการส่งข้อมูลสูง เช่น อุณหภูมิสูงหรือความชื้นสูง เป็นต้น ปริมาณข้อมูลที่ส่งไปในช่วงเวลาหนึ่งหรือค่าทราฟฟิกในเครือข่ายที่ไม่มี ความน่าเชื่อถือนี้จะลดลง ในขณะที่ความผิดพลาดของข้อมูลก็อาจจะสูงขึ้นด้วย เพื่อเพิ่มทราฟฟิกพร้อมทั้งลดความผิดพลาดของบิตข้อมูลนั้น ทำให้เกิดวิธีการและเทคนิคหลายแบบเพื่อแก้ไขปัญหา วิธีหนึ่งที่ได้รับค่านิยมและมีประสิทธิภาพ คือ การใช้รหัสเครือข่าย (network coding) [1]

รหัสเครือข่ายได้รับการนำเสนอเพื่อที่จะพัฒนาสมรรถนะของเครือข่ายการสื่อสารแบบใช้สายและไร้สาย [1] [4] เนื่องจากรหัสเครือข่ายนั้นมีข้อดีในเรื่องของการเพิ่มค่าทราฟฟิก, ความทนทานของข้อมูล (robustness) และความปลอดภัย (security) เป็นต้น โดยการประยุกต์ใช้รหัสเครือข่ายในการสื่อสารแบบมัลติคาสต์ (multicast) นั้น ได้รับการศึกษาและพัฒนาในงานวิจัยหลายชิ้น เช่น ใน [7][8] ได้แสดงให้เห็นว่า รหัสเครือข่ายแบบเชิงเส้น (linear network code) ทำให้เกิดมีค่าทราฟฟิกสูงสุดในเครือข่าย ซึ่งมีค่าเท่ากับการไหลของข้อมูลที่สูงสุดระหว่างแหล่งกำเนิดสู่ปลายทางโหนดใดๆ ในเครือข่ายไม่ว่าจะเป็นเครือข่ายที่ได้รับการออกแบบไว้ (deterministic) [9] หรือแบบสุ่ม (randomized) [10] ซึ่งรหัสเครือข่ายแบบเชิงเส้นนั้น คือ การรวมตัวกันของแพ็กเก็ต (packets) ข้อมูลแบบเชิงเส้นที่มีการสุ่มค่าสัมประสิทธิ์จากฟิลด์จำกัดเดียวกัน (F_q) ซึ่งรหัสเครือข่ายชนิดนี้จะสามารถใช้ความจุของช่องสัญญาณเครือข่าย (network capacity) ด้วยความน่าจะเป็นเข้าใกล้ 1 หากขนาดของฟิลด์มีค่าใหญ่เพียงพอ [10]

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 1.1 เครือข่ายแบบผีเสื้อ (butterfly network) ที่ไม่มีการใช้รหัสเครือข่าย (ซ้าย)
และเครือข่ายแบบผีเสื้อที่มีการใช้รหัสเครือข่าย (ขวา)

รูปที่ 1.1 แสดงถึงการประยุกต์ใช้รหัสเครือข่ายในเครือข่ายรูปผีเสื้อ โดยโหนดผู้ส่ง (N1) ต้องการส่งแพ็กเก็ตข้อมูล A และ B ไปยังโหนดผู้รับ N6 และ N7 ตามลำดับ ผ่านโหนดส่งผ่าน N3 และ N5 ซึ่งเป็นเส้นทางคอคขวด โดยใช้รูปที่ 1.1 (ซ้าย) คือการส่งแบบไม่ใช้รหัสเครือข่าย ทำให้การส่งข้อมูล A และ B ผ่าน N3 ไปยัง N5 ต้องส่งข้อมูลผ่านเส้นทางคอคขวด ซึ่งทำให้โหนดปลายทางนั้นได้รับข้อมูลที่ล่าช้า ขณะที่ในรูปที่ 1.1. (ขวา) แสดงให้เห็นว่ารหัสเครือข่ายจะช่วยจัดการการส่งข้อมูลในเส้นทางที่เป็นคอคขวด โดยการส่งแพ็กเก็ตที่ได้รับการเข้ารหัสแล้วในรูปแบบของ $A \oplus B$ ($A \text{ XOR } B$) ภายในครั้งเดียวและใช้เทคนิคการแอบได้ยิน (Overhearing) ผ่านเส้นทาง N2-N6 และ N4-N7 ซึ่งทำให้โหนดที่อยู่ตรงกลางนั้นสามารถตัดสินใจว่าควรนำแพ็กเก็ตใดมาเอ็กซ์คลูซีฟออ์ (Exclusive-Or : XOR) กันระหว่างข้อมูลที่อยู่ภายใน ซึ่งทำให้จำนวนครั้งการส่งที่ใช้ในการส่งข้อมูลไปยังปลายทางเหลือเพียง 1 ครั้ง ในเส้นทาง N3-N5 และ N5-N6 และ N5-N7

อย่างไรก็ตามในการส่งข้อมูลผ่านเครือข่ายนั้น ยังคงมีการผิดพลาดเกิดขึ้นในช่องสัญญาณแบบไบนารีลบเลือนได้ (Binary Erasure Channel : BEC) ซึ่งความผิดพลาดที่เกิดขึ้นนั้นเป็นความผิดพลาดระดับเฟรมข้อมูล ซึ่งการแก้ไขความผิดพลาดนั้นมีรหัสแอลที (LT code) [11] ซึ่งเป็นหนึ่งในแนวคิดของรหัสน้ำพุ (Fountain code) ถูกนำเสนอเพื่อช่วยลดอัตราการลบเลือน (Frame Erasure Rate : FER) ที่เกิดขึ้นในช่องสัญญาณดังกล่าว โดยนำเฟรมข้อมูลมาทำการเข้ารหัสด้วยเมทริกซ์กำเนิด (Generator matrix) ก่อนที่จะส่งไปยังโหนดผู้รับซึ่งผลที่ได้นั้นช่วยลดการตอบกลับหรือการร้องขอการส่งข้อมูลซ้ำเนื่องจากมีเฟรมข้อมูลลบเลือนเกิดขึ้นในลำดับชั้นเครือข่าย (Network Layer) ซึ่งช่วยลดภาระให้โหนดผู้ส่งและโหนดระหว่างทาง อย่างไรก็ตาม สำหรับเครือข่ายแบบไร้สายนั้นจะมีความแตกต่างในการใช้และคุณสมบัติของรหัสเครือข่ายเนื่องจากธรรมชาติในการสื่อสารไร้สาย เช่น การกระจายสัญญาณ (broadcast transmission), การใช้สื่อสัญญาณร่วมกัน (medium-sharing), และสิ่งแวดล้อมที่เปลี่ยนแปลงในเวลา (time-varying environment) ดังนั้นการประยุกต์ใช้รหัสสำหรับช่องสัญญาณลบเลือนนั้นจึงมีได้หลากหลายมากขึ้น โดยเฉพาะอย่างยิ่งรหัสเครือข่าย โดยการออกแบบและสร้างรหัสเครือข่ายที่มีคุณสมบัติและโครงสร้างที่คุ้มค่าที่สุด (optimal) ก็ยังเป็นสิ่งที่น่าท้าทายเป็นอย่างมาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดังนั้น วิทยานิพนธ์ฉบับนี้จึงมีจุดประสงค์เพื่อที่จะช่วยเพิ่มค่าทรมุทให้แก่ระบบด้วยการเข้ารหัสเครือข่าย ซึ่งได้พัฒนาในเครือข่ายขนาดเล็กในระยะแรก และผลที่ได้ยังช่วยให้ลดระยะเวลาที่ใช้ในการส่งอีกด้วย นอกจากนี้ผู้วิจัยได้พัฒนาขั้นตอนวิธีในการเข้ารหัสเครือข่ายสำหรับเครือข่ายที่ขนาดใหญ่ขึ้น โดยอาศัยการแอบได้ยินจากโหนดข้างเคียง พร้อมทั้งได้เปรียบเทียบวิธีการเพิ่มสมรรถนะของระบบด้วยการวัดการเพิ่มขึ้นของค่าทรมุทโดยเฉลี่ย, ค่าเวลาของการส่งข้อมูลที่ลดลงโดยเฉลี่ย และอัตราการลบเลือนของเฟรมข้อมูล

1.2 ความมุ่งหมายและวัตถุประสงค์ของงานวิจัย

1.2.1 ออกแบบและสร้างรหัสเครือข่ายสำหรับระบบเครือข่ายไร้สายที่มีการเชื่อมต่อแบบมัลติคาสต์ที่สามารถกู้ข้อมูลที่สูญหายได้โดยไม่ต้องมีการเรียกซ้ำจากโหนดผู้ส่ง

1.2.2 ทดสอบประสิทธิภาพและสมรรถนะของรหัสและรูปแบบการส่งข้อมูลตามที่ได้ออกแบบในรูปแบบของค่าทรมุท และค่าเวลาการส่งรวม

1.3 ขอบเขตของโครงการวิจัย

1.3.1 เพื่อศึกษาลักษณะของการทำงานของโพรโตคอลการส่งข้อมูลในระบบไร้สาย ทั้งจากเราเตอร์ไปยังคอมพิวเตอร์และระหว่างเซ็นเซอร์โหนดในกลุ่มของเครือข่ายเซ็นเซอร์ไร้สาย

1.3.2 ศึกษารูปแบบการเข้ารหัสด้วยการเอ็ชคลูซีฟออร์ในระบบเครือข่ายไร้สาย

1.3.3 ศึกษารูปแบบเทคนิคทางทฤษฎีกราฟ พร้อมทั้งพัฒนาทฤษฎีในการเข้ารหัสด้วยเทคนิคดังกล่าว ในเครือข่ายที่มีเส้นทางคอบวุดเป็นข้อจำกัดของระบบ

1.3.4 พัฒนาความแข็งแรงของการส่งข้อมูลด้วยรหัสเครือข่ายเชิงระบบ พร้อมทั้งวิเคราะห์ความน่าจะเป็นของการเกิดเฟรมข้อมูลที่ผิดพลาดร่วมกัน เพื่อให้โหนดข้างเคียงนั้นสามารถช่วยส่งข้อมูลที่เสียไปแทนที่จะต้องส่งจากโหนดผู้ส่งซึ่งอยู่ห่างไกล

1.4 วิธีการดำเนินการวิจัย

รายงานวิจัยฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทหลักดังนี้

บทที่ 1 กล่าวถึงความเป็นมา, ความสำคัญของปัญหา, ทฤษฎีที่ใช้ในการทำวิจัยโดยคร่าว, วัตถุประสงค์ และขอบเขตของงานวิจัยรวมทั้งขั้นตอนวิธีการดำเนินงานวิจัย

บทที่ 2 การทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง ซึ่งประกอบด้วยอัลกอริธึมควบคุมการไหลของข้อมูลในเครือข่ายคอมพิวเตอร์, ทฤษฎีกราฟและการเข้ารหัสเครือข่ายด้วยการเอ็กซ์คลูซีฟออร์รวมถึงรหัสแอลที

บทที่ 3 ศึกษาและพัฒนารหัสเครือข่ายแบบปรับตัวได้ (The Adaptive Network Coding-Routing Based on Graph for Multicast Networks : ANCR) ซึ่งสามารถเลือกการเข้ารหัสด้วยรหัสเครือข่ายหรือการส่งข้อมูลด้วยเร้าติ้งโพรโทคอล (routing protocol) มาตรฐานได้

บทที่ 4 ศึกษาและพัฒนารหัสเครือข่ายเชิงระบบ (Systematic Network Code : SNC) สำหรับเครือข่ายที่มีขนาดใหญ่ และสร้างกลวิธีในการส่งข้อมูลซ้ำ

บทที่ 5 เป็นการสรุปงานวิจัยและข้อเสนอแนะ



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

การทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้อง

บทนี้กล่าวถึงทฤษฎีพื้นฐานที่เกี่ยวข้องกับงานวิจัย โดยเริ่มจากการศึกษาหลักการสื่อสารข้อมูลในระดับมูลฐานของโพรโทคอลการใช้สื่อสัญญาณในระบบคอมพิวเตอร์ ซึ่งมีหน้าที่หลัก คือจัดการการจราจรของข้อมูลในเครือข่าย รวมถึงงานวิจัยที่เพิ่มประสิทธิภาพเครือข่ายด้วยการแก้ไขและดัดแปลงการควบคุมการจราจรของข้อมูลด้วยการเข้ารหัสเครือข่ายเทคนิควิธีการหาเส้นทางสำรองในโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจ (Ad hoc On-Demand Distance Vector : AODV) [13] เพื่อลดความซับซ้อนในการเข้ารหัสเครือข่าย พร้อมกันนี้ยังศึกษาเทคนิคการหาคุณสมบัติกราฟไมเนอร์ในทฤษฎีกราฟ เพื่อช่วยในการเข้ารหัสระหว่างแพ็กเก็ตด้วยการเอ็กซ์คลูซีฟออร์ และสุดท้ายคือรหัสแอสที่ซึ่งมีส่วนช่วยให้การส่งข้อมูลในช่องสัญญาณแบบไบนารีลบบเลื่อนได้ให้มีความน่าเชื่อถือมากยิ่งขึ้น

2.1 โพรโทคอลควบคุมการใช้สื่อสัญญาณในเครือข่ายคอมพิวเตอร์

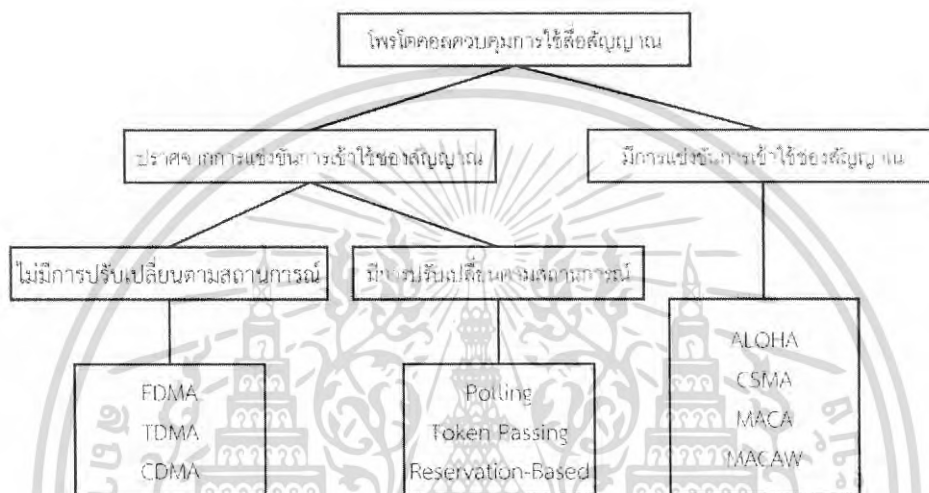
หัวข้อนี้เป็นการเรียงลำดับของโพรโทคอลที่ใช้ในงานวิจัย โดยเริ่มจากโพรโทคอลควบคุมการใช้สื่อสัญญาณ (Medium Access Control protocol : MAC) ในหัวข้อ 2.1.1 ซึ่งยกตัวอย่างโพรโทคอลดังกล่าวโดยจำแนกออกเป็นประเภท ถัดมาในหัวข้อ 2.1.2 นำเสนอโพรโทคอลพื้นฐานในโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจ ซึ่งถูกนำมาใช้งานอย่างแพร่หลายในเครือข่ายเซ็นเซอร์ไร้สาย (Wireless Sensor Network : WSN) รวมถึงคอมพิวเตอร์แล็บที่ข้อที่สามารถใช้งานโพรโทคอลดังกล่าวนี้ได้ ถัดมาได้มีโพรโทคอลสำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจแบบมีเส้นทางสำรอง (Ad hoc On-Demand Distance Vector with Backup routing : AODV-BR) ซึ่งเป็นงานวิจัยที่ได้พัฒนาเพื่อเพิ่มประสิทธิภาพการส่งข้อมูลในเครือข่ายที่มีโครงสร้างในรูปแบบตาข่าย (Mesh Network) ด้วยการสำรองเส้นทางที่โหนดส่งผ่าน (Relay node)

2.1.1 โพรโทคอลควบคุมการใช้สื่อสัญญาณ

โพรโทคอลควบคุมการใช้สื่อสัญญาณ [11] นั้นมีความจำเป็นอย่างมากในระบบการสื่อสารไร้สาย ซึ่งคลื่นสัญญาณนั้นสามารถถูกแพร่กระจายออกมาได้จากหลายผู้ส่งได้ตลอดเวลา เพื่อป้องกันการชนกันของการแพร่กระจายสัญญาณ จึงต้องมีการควบคุมดังกล่าวนี้ ซึ่งสามารถอธิบายได้ด้วยแบบจำลอง OSI (Open System Interconnection model) โดยโพรโทคอลการควบคุมดังกล่าวนี้ทำงานในลำดับชั้นที่ 2 ของแบบจำลอง OSI ซึ่งก็คือลำดับชั้นการเชื่อมประสานข้อมูล (Data link layer) ตามมาตรฐาน IEEE 802 และนอกจากนั้นโพรโทคอล MAC ซึ่งถูกแบ่งเป็นสองลำดับชั้นย่อย ได้แก่ ลำดับชั้นการควบคุมสื่อสัญญาณด้วยตรรกะ (Logical Link Control Layer) และลำดับชั้นควบคุมการเข้าถึงสื่อสัญญาณ (Medium Access Control Layer : MAC Layer) โดยหน้าที่หลักของ MAC นั้นทำหน้าที่ตัดสินใจว่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อไหร่ที่โหนดใดจะสามารถใช้สื่อสัญญาณ (Medium) ซึ่งแบ่งปันร่วมกันภายในเครือข่ายได้โดยปราศจากการชนกันของการแพร่กระจายสัญญาณ ในขณะที่เดียวกันก็สามารถเพิ่มประสิทธิภาพของการส่งเฟรมข้อมูล, ควบคุมการไหลของข้อมูลและยังช่วยแก้ไขข้อบกพร่องที่เกิดจากลำดับชั้นการส่งข้อมูลทางกายภาพ (Physical Layer) โดยในรูปที่ 2.1 แสดงให้เห็นถึงการจำแนกประเภทของโพรโตคอล MAC ในรูปแบบต่างๆ



รูปที่ 2.1 ประเภทของโพรโตคอล MAC

โพรโตคอล MAC ที่ใช้งานกันส่วนใหญ่อยู่นั้นอยู่ในรูปแบบได้ทั้งสองประเภท คือ โพรโตคอลที่ปราศจากการแข่งขันการเข้าใช้ช่องสัญญาณ (contention-free) และโพรโตคอลที่มีการแข่งขันการเข้าใช้ช่องสัญญาณเป็นหลัก (contention-based) โดยโพรโตคอลที่ปราศจากการแข่งขันการเข้าใช้ช่องสัญญาณนั้นจะทำให้โหนดต่างๆ ในเครือข่ายมั่นใจได้ว่าการเข้าใช้สื่อสัญญาณนั้นจะถูกใช้งานเพียงหนึ่งโหนดเท่านั้น ซึ่งในส่วนการจองช่องสัญญาณนั้นสามารถแบ่งแยกย่อยเป็นอีกสองชนิดคือ แบบคงที่ (fixed) และแบบที่มีการปรับเปลี่ยนตามสถานการณ์ (dynamic)

ส่วนในโพรโตคอลที่มีการแข่งขันการเข้าใช้ช่องสัญญาณเป็นหลัก (contention-based) จะอนุญาตให้โหนดนั้นๆ เข้าถึงการใช้งานทันทีที่มีการร้องขอ ซึ่งโพรโตคอลดังกล่าวนี้มีกลไกเพิ่มเติมที่ช่วยในการลดจำนวนของการชนกันและยังช่วยนำการส่งข้อมูลเหล่านั้นกลับมาได้อีกครั้งหลังจากเกิดการชนกันขึ้น ซึ่งมีโพรโตคอลที่เป็นที่นิยม ได้แก่ ALOHA และ CSMA (Carrier Sense Multiple Access)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.1.2 โพรโตคอลสำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่

2.1.2.1 โพรโตคอลสำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจ

โพรโตคอลสำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจ (Ad hoc On-Demand Distance Vector : AODV) [11] นั้นเป็นทั้งวิธีการค้นหาเส้นทางและรวมถึงส่งข้อมูลที่เกิดขึ้นเมื่อมีความต้องการ (on demand) เกิดขึ้นในเครือข่าย ซึ่งถูกนำมาใช้แพร่หลายในเครือข่ายเซ็นเซอร์ไร้สาย และยังมี ความแตกต่างจากโพรโตคอลแบบ OLSR (Optimized Link State Routing) ในส่วนที่ไม่จำเป็นต้องมีการส่งข้อมูลเพื่ออัปเดตสถานะของลิงค์ในเครือข่าย โดยโพรโตคอลนี้ใช้กลไกการกระจายสัญญาณ (Broadcast) ในการค้นหาเส้นทาง (Broadcast Routing) ซึ่งการสร้างเส้นทางในการส่งข้อมูลจากผู้ส่งไปยังปลายทางนั้นจะปรับเปลี่ยนตามความเหมาะสม

การสร้างเส้นทางเพื่อการส่งข้อมูลนั้นจะเกิดขึ้นก็ต่อเมื่อมีโหนดใดๆ ต้องการที่จะส่งข้อมูลไปยังโหนดอื่นๆ โดยทำการส่งแพ็กเก็ตร้องขอเส้นทาง (Route request : RREQ) ไปยังโหนดโดยรอบซึ่งประกอบด้วยแอดเดรสของผู้ส่ง, ผู้รับ, จำนวนฮอป (Hop), หมายเลขบรอดคาสต์ (Broadcast ID) เป็นต้น ซึ่งจะมีการส่งต่อกันไปเรื่อยๆ จนกระทั่งถึงผู้รับที่แท้จริง ที่ปลายทางผู้รับจะตอบกลับด้วยแพ็กเก็ตตอบกลับ (Route Reply : RREP) ไปยังผู้ส่งโดยตรงผ่านเส้นทางที่แพ็กเก็ต RREQ นั้นถูกส่งมา โดยจะถือว่าเส้นทางที่ถูกบรรจุมาในแพ็กเก็ต RREP ที่ได้รับตัวแรกนั้นเป็นเส้นทางที่ดีที่สุด ไรที่สุด และน่าเชื่อถือที่สุด ณ ขณะนั้น ซึ่งได้แสดงวิธีการค้นหาเส้นทางดังรูปที่ 2.2



รูปที่ 2.2 การค้นหาเส้นทางของโพรโตคอล AODV

จากรูปที่ 2.2 เมื่อโหนดผู้ส่งต้องการที่จะส่งข้อมูลไปยังโหนดปลายทาง ซึ่งจะเริ่มจากการแพร่กระจายแพ็กเก็ตร้องขอเส้นทางไปทุกทิศทาง ซึ่งการส่งต่อของแพ็กเก็ตดังกล่าวจะมีการนับจำนวนฮอป รวมทั้งระยะเวลาที่ส่งอีกด้วยเพื่อนำมาประกอบการพิจารณาหาเส้นทางที่ดีที่สุด ซึ่งจะตอบกลับมาในรูปของแพ็กเก็ตตอบกลับ

จากนั้นเมื่อมีเส้นทางระหว่างโหนดถูกตัดขาด ซึ่งอาจมีสาเหตุมาจากโหนดใดโหนดหนึ่งมีการเคลื่อนที่ โหนดตัวกลาง (Intermediate node) ที่อยู่ใกล้โหนดที่สุดจะทำหน้าที่รายงานโหนดผู้ส่งเกี่ยวกับ

เส้นทางที่เปลี่ยนแปลงนี้ผ่านแพ็กเก็ต RERR (Route Error : RERR) ซึ่งทำให้ผู้ส่งนั้นสามารถเริ่มต้นกระบวนการค้นหาเส้นทางใหม่เมื่อได้รับแพ็กเก็ตดังกล่าว

การใช้โพรโทคอล AODV ในการสร้างเส้นทางส่งข้อมูลและจะเกิดขึ้นก็ต่อเมื่อมีโหนดใดโหนดหนึ่งต้องการจะส่งข้อมูล และไม่จำเป็นต้องคอยอัปเดตตารางเร้าติง (Routing table) แต่อย่างไรก็ตามแต่ละโหนด จำเป็นจะต้องส่งแพ็กเก็ต HELLO เพื่อรักษาสถานการณ์ติดต่อซึ่งกันและกันอยู่ตลอดเวลา

2.1.2.2 โพรโทคอลสำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจแบบมีเส้นทางสำรอง

ในโพรโทคอลสำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจแบบมีเส้นทางสำรอง (Ad hoc On-Demand Distance Vector with Backup routing : AODV-BR) [14] เป็นการปรับปรุงประสิทธิภาพเดิมของโพรโทคอล AODV โดยมีการเพิ่มเส้นทางสำรองให้กับโหนดส่งผ่านระหว่างทาง โดยที่ไม่จำเป็นต้องเปลี่ยนแปลงขั้นตอนวิธีในการค้นหาเส้นทางด้วยแพ็กเก็ต RREQ ของผู้ส่ง โดยในแต่ละแพ็กเก็ต RREQ ที่ถูกส่งต่อกันไปนั้นจะมีหมายเลขค้อยกำกับซึ่งช่วยให้โหนดส่งผ่านที่อยู่ระหว่างทางนั้นสามารถจับแพ็กเก็ตที่ได้รับซ้ำกันได้ และเมื่อโหนดตัวกลางได้รับแพ็กเก็ต RREQ ที่มีหมายเลขกำกับที่ใหม่กว่าเข้ามาจะทำการบันทึกข้อมูลของฮอปปัจจุบันลงไปรวมกับข้อมูลก่อนหน้าที่มีอยู่แล้ว ซึ่งหมายความว่าโหนดที่เป็นตัวกลางนั้นจะทราบเส้นทางที่เป็นไปได้ทั้งหมดจากผู้ส่งไปยังผู้รับ และถ้าหากเส้นทางใดเส้นทางหนึ่งขาดการเชื่อมต่อ โหนดผู้ส่งก็จะผ่านแพ็กเก็ตข้อมูลไปยังเส้นทางที่เหลือทันที ซึ่งแสดงได้ดังรูปที่ 2.3



รูปที่ 2.3 โพรโทคอล AODV-BR เส้นทางหลัก (เส้นทึบ) และเส้นทางสำรอง (เส้นประ)

จากการทดสอบกับเครือข่ายที่มีลักษณะเป็นตาข่ายแสดงให้เห็นว่า AODV-BR เพิ่มภาระไปที่โหนดระหว่างกลางหรือโหนดส่งผ่านในการทำตารางเร้าติงเมื่อทำการเปรียบเทียบระหว่างโพรโทคอล AODV และผลที่ได้นั้น AODV-BR ช่วยเพิ่มอัตราการรับข้อมูลได้สูงขึ้นและยังช่วยเพิ่มการนำเชื่อถือให้กับการส่งข้อมูลในเครือข่ายไร้สายอีกด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2 รหัสเครือข่าย

การเข้ารหัสเครือข่าวนั้นเป็นกลวิธีหนึ่งในการเพิ่มประสิทธิภาพเครือข่าย ซึ่งสามารถวัดประสิทธิภาพได้ด้วยค่าทรูพุด และเวลาการส่งข้อมูลโดยรวมทั้งระบบ นอกจากนี้ยังต้องคำนึงถึงความซับซ้อนในการคำนวณและการเข้ารหัสและถอดรหัสอีกด้วย ซึ่งในหัวข้อนี้จะกล่าวถึงหลักการในการเข้ารหัส ถอดรหัส รวมถึงงานวิจัยที่เกี่ยวข้อง

2.2.1 หลักมูลฐานของรหัสเครือข่าย

โดยปกติแล้วในการส่งข้อมูลในระบบเครือข่าย แต่ละแพ็กเก็ตที่ถูกส่งออกไปจากแต่ละโหนดจะเป็นการคัดลอกข้อมูลที่ถูกลงเข้ามา สำหรับการเข้ารหัสเครือข่าย (Network Coding) นั้นจะอนุญาตให้มีการคำนวณก่อนที่จะมีการส่งแพ็กเก็ตออกไปผ่านช่องสัญญาณ ซึ่งในขาออกของโหนดนั้นๆ จะมีความสามารถในการผสมผสานแพ็กเก็ตที่เข้ามา (Mixing) หรือเรียกอีกอย่างหนึ่งว่า การเข้ารหัส (Encoding) และในส่วนขาเข้านั้นสามารถแยกแยะของแพ็กเก็ตที่ได้รับการผสมผสานได้ (Re-mixing) หรือเรียกอีกอย่างหนึ่งว่า การถอดรหัส (Decoding)

หลักการเข้ารหัสเครือข่าวนั้นอาศัยหลักการการพิจารณาทิศทางกรไหลของข้อมูลและลักษณะของเส้นทางร่วมกัน ซึ่งปัญหาที่เกิดขึ้นและต้องการแก้ไขนั้นคือ ปัญหาคอขวด (Bottle-neck) โดยรูปแบบทั่วไปของการเข้ารหัสเครือข่ายซึ่งสามารถเขียนให้อยู่ในลักษณะผลรวมเชิงเส้น (Linear combination) ซึ่งสามารถแสดงได้ดังรูปที่ 2.4



รูปที่ 2.4 รูปแบบทั่วไปของการเข้ารหัสเครือข่าย

สำหรับการเข้ารหัสเครือข่ายเหนือฟิลด์จำกัดนั้น [5] ได้กำหนดให้แพ็กเก็ตอักขระ A คือองค์ประกอบขนาด q ในฟิลด์จำกัด F_q ซึ่งขนาดฟิลด์ที่เล็กที่สุดที่จะสามารถมีได้คือ $F_2 = \{0, 1\}$ และยังกำหนดให้แพ็กเก็ตขาเข้า (Incoming packets) ณ โหนด s จำนวน r แพ็กเก็ต ในรูปคอลัมน์เวกเตอร์ $(p_1, p_2, \dots, p_r)^T$ ซึ่งสำหรับแพ็กเก็ตใดๆ p_i คือเวกเตอร์ที่มีขนาดความยาว m ดังนั้น $X_{I(s)}$ สามารถเขียนให้อยู่ในรูปของเมทริกซ์ขนาด $r \times m$ ในฟิลด์จำกัด F_q ในการเข้ารหัสเครือข่ายเชิงเส้นเฉพาะที่ (Local Linear Network Coding) สำหรับโหนด v ใดๆ สามารถแสดงได้ดังสมการ (1.1)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$X_{O(s)} = L_v X_{I(v)} \quad (1.1)$$

จากสมการ คอลัมน์เวกเตอร์ $X_{O(s)}$ คือแพ็กเก็ตขาออก (Outgoing packets) จากโหนด v ซึ่งจะมี ความสัมพันธ์เชิงเส้นกับ $X_{I(v)}$ และ L_v คือเมทริกซ์สัมประสิทธิ์จากฟิลด์จำกัด F_q ซึ่งสามารถเรียกได้อีก อย่างหนึ่งว่าเมทริกซ์ถ่ายโอนเฉพาะที่ (Local Transfer matrix) ที่โหนด v โดยแต่ละแถวของเมทริกซ์ ถ่ายโอนนั้นจะมีความเกี่ยวข้องโดยตรงกับเส้นเชื่อม (e) ขาออก $O(v)$ ของโหนด v เมื่อ $e \in O(v)$ หลังจากที่ถูกส่งผ่านไปยังแต่ละเส้นเชื่อมด้วยผลรวมเชิงเส้นของ r แพ็กเก็ตซึ่งในมุมมองของแต่ละ โหนด v จะสามารถเขียนได้ดังสมการที่ (1.2) เมื่อ G_v คือเมทริกซ์ถ่ายโอนครอบคลุม (Global Transfer matrix) แต่ละแถวของเมทริกซ์ถ่ายโอนนั้นจะมีความเกี่ยวข้องโดยตรงกับเส้นเชื่อมขาเข้า $I(v)$ ของโหนด v เมื่อ $e \in I(v)$

$$X_{I(v)} = G_v \begin{bmatrix} p_1 \\ \vdots \\ p_r \end{bmatrix} \quad (1.2)$$

สำหรับตัวแปร X คือเวกเตอร์ $|E| \times 1$ เมื่อ $|E|$ คือจำนวนเส้นเชื่อมที่สามารถใช้งานได้ในทุก โพลี โดยที่ p_i คือแพ็กเก็ตใดๆ ที่ถูกส่งผ่านเส้นเชื่อม e_i ซึ่ง X นั้นเปรียบเสมือนสถานะของเครือข่าย ณ ขณะนั้น และสำหรับแบบจำลองในรูปแบบมาตรฐานของสถานะเครือข่ายสำหรับผลรวมเชิงเส้นของ แพ็กเก็ตของโหนดผู้รับนั้นสามารถแสดงได้ดังสมการที่ (1.3) และ (1.4)

$$X = AX + BU \quad (1.3)$$

$$X_{I(t)} = C_t X \quad (1.4)$$

เมื่อ A คือเมทริกซ์ถ่ายโอนที่มีขนาด $|E| \times |E|$ ซึ่งมีความสัมพันธ์แบบเส้นเชื่อมต่อเส้นเชื่อม (edge-to-edge), $U = (p_1, p_2, \dots, p_r)^T$ ซึ่งก็คือเวกเตอร์ของแพ็กเก็ตขาเข้า, B คือเมทริกซ์ที่มีขนาด $|E| \times r$ ที่ได้จากการส่งผ่านสัมประสิทธิ์จากแต่ละแพ็กเก็ตขาเข้าผ่านเส้นเชื่อมใน E และ C_t คือเมทริกซ์ ฉาย (Matrix projection) ของ X ที่มีขนาด $|I(t)| \times |E|$ นอกจากนี้ยังสามารถระบุได้ถึงการรวมกัน ของแพ็กเก็ตผ่านเมทริกซ์ B ถัดมาในส่วนเมทริกซ์ A นั้นสามารถระบุได้ว่าแต่ละเส้นเชื่อมสามารถรวมกัน ได้อย่างไร และสุดท้าย C_t เป็นการระบุว่าแต่ละเส้นเชื่อมนั้นรวมกันที่โหนดผู้รับได้อย่างไร โดยเมทริกซ์ ถ่ายโอนครอบคลุมของโหนดผู้รับใดๆ t สามารถหาได้จากสมการ (1.5)

$$G_t = C_t(I - A)^{-1}B \quad (1.5)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ผลที่ตามมาจากการนำรหัสเครือข่ายมาประยุกต์ คือ สามารถเพิ่มทรูพุตให้กับเครือข่ายด้วยการส่งผ่านข้อมูลภายในกระแสของข้อมูลเพียงกระแสเดียว (Information stream) ผ่านเส้นทางคอ-ขวดด้วยการเอ็กซ์คลูซีฟออร์ (Exclusive-Or) แบบบิตต่อบิตระหว่างกระแสของข้อมูลที่มีจำนวนมากกว่า 2 กระแสขึ้นไปในฝั่งขาเข้า ซึ่งในหัวข้อที่ 2.2.2 จะเป็นการนำทฤษฎีดังกล่าวมาประยุกต์ใช้ในระบบเครือข่ายเสมือนจริง

2.2.2 การประยุกต์ใช้รหัสเครือข่ายและงานวิจัยที่เกี่ยวข้อง

เริ่มจากใน [1] Ahlswede, et.al. ได้แสดงให้เห็นถึงการผสมข่าวสารจากข้อความที่แตกต่างกันเพื่อทำให้ระบบนั้นเข้าใกล้ความจุของเครือข่ายมัลติคาสต์ด้วยการพิจารณาการสื่อสารระหว่างคูโหนด งานดังกล่าวทำให้เกิดผลงานตีพิมพ์ต่อเนื่อง เช่น ใน [4] การเอ็กซ์คลูซีฟออร์ในช่องสัญญาณ: การเข้ารหัสเครือข่ายไร้สายในเชิงปฏิบัติ (XORs in the air : Practical wireless network coding) [4] ซึ่ง Katti, et.al. ได้ขยายงานเดิมของ Wu, et.al. [2] โดยใช้วิธีการแอบไต่ยีนเพื่อให้ได้มาซึ่งข่าวสารจากโหนดข้างเคียงหรือโหนดที่อยู่ติดกัน (side information) และวิธีการเข้ารหัสแรกๆ นั้นถูกออกแบบมาเพื่อเพิ่มประสิทธิภาพสำหรับโครงสร้างเครือข่ายแบบตาข่าย ซึ่งมีโหนดตัวกลาง (Intermediate Node) หรือโหนดส่งผ่าน นำแพ็กเกตมากกว่า 2 แพ็กเกตจาก 2 ผู้ส่งขึ้นไปมารวมกันด้วยการเอ็กซ์คลูซีฟออร์เพื่อเพิ่มปริมาณข้อมูลในแต่ละครั้งที่ส่งออกไป ซึ่ง [4] ได้นำเสนอวิธีการในการเลือกแพ็กเกตต่างๆ มา เอ็กซ์คลูซีฟออร์ ซึ่งเรียกว่า ขั้นตอนวิธีโคป (COPE) ซึ่งประกอบด้วย โอกาสในการไต่ยีน (Opportunistic Listening), โอกาสในการเข้ารหัส (Opportunistic coding) และการรับรู้สถานะของโหนดข้างเคียง (Learning Neighbor State) ซึ่งสามารถอธิบายได้ดังนี้

ก. โอกาสในการไต่ยีน (Opportunistic Listening)

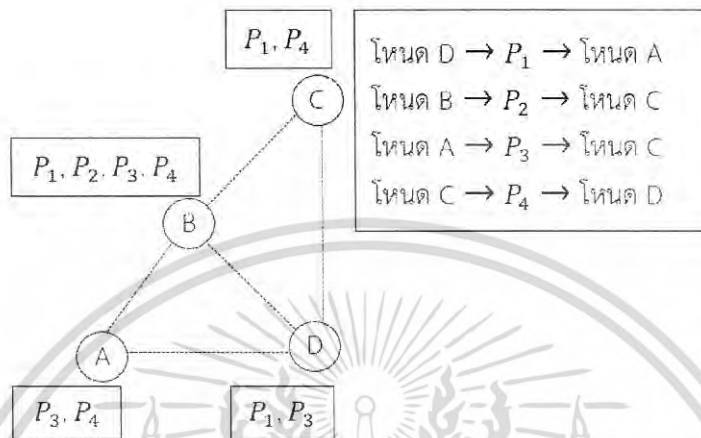
ด้วยธรรมชาติของการแพร่กระจายสัญญาณไร้สายนั้น ได้สร้างโอกาสมากมายให้กับโหนดที่อยู่ภายในรัศมีของการแพร่กระจายสัญญาณดังกล่าวในการรับรู้ โดยเฉพาะอย่างยิ่งเมื่อโหนดเหล่านั้นใช้เสาอากาศแบบรอบทิศทาง (Omni-directional antenna) ขั้นตอนวิธีโคปนั้นจะใช้ข้อได้เปรียบจากโหมดเฝ้าสังเกต (Monitor mode หรือ Promiscuous mode) ซึ่งทำให้แต่ละโหนดนั้นสามารถสอดแนมทุกๆ การสื่อสารในเครือข่ายไร้สายและยังสามารถเก็บข้อมูลที่แอบไต่ยีนไว้ในหน่วยความจำชั่วคราวได้ในระยะเวลาจำกัด T (ซึ่งมีค่าโดยปริยาย $T = 0.5$ วินาที) นอกจากนั้นแต่ละโหนดกระจายสัญญาณรายงานการรับรู้ (reception reports) ซึ่งรายงานเหล่านี้จะเป็นการแจ้งโหนดต่างๆ ที่อยู่ใกล้เคียงว่าโหนดที่ส่งรายงานเหล่านี้มีแพ็กเกตอะไรอยู่บ้าง

ข. โอกาสในการเข้ารหัส (Opportunistic coding)

คำถามสำคัญสำหรับหัวข้อนี้คือ จำเป็นจะต้องใช้แพ็กเกตใดบ้างในการนำมาเข้ารหัสเพื่อที่จะให้ได้ค่าทรูพุตที่สูงที่สุด ซึ่ง ณ โหนดใดโหนดหนึ่งนั้นอาจจะมีหลายตัวเลือกในการเข้ารหัส ซึ่งเงื่อนไขหลักใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การนำแพ็กเก็ตมาเข้ารหัสนั้นจะมุ่งเน้นไปที่จำนวนการส่งแพ็กเก็ตดั้งเดิมที่อยู่ในแพ็กเก็ตที่เข้ารหัสให้มากที่สุดในการส่งเพียง 1 ครั้ง และจะต้องพิจารณาว่าในฮอปถัดไปนั้นมีข้อมูลเพียงพอในการถอดรหัสหรือไม่



รูปที่ 2.5 ตัวอย่างการหาโอกาสในการเข้ารหัส [4]

ในรูปที่ 2.5 แสดงถึงตัวอย่างในการหาโอกาสในการเข้ารหัสในการติดต่อสื่อสารระหว่างโหนด A, B, C และ D เมื่อโหนด B มีทั้งหมด 4 แพ็กเก็ตได้แก่ $P_1, P_2, P_3,$ และ P_4 ในขณะที่โหนดข้างเคียงกับโหนด B ก็แอบได้ยินในบางแพ็กเก็ต ซึ่งปลายทางของแต่ละแพ็กเก็ตที่โหนด B จะส่งไปนั้นคือ $P_1 \rightarrow$ โหนด A, $P_2 \rightarrow$ โหนด C, $P_3 \rightarrow$ โหนด C, และ $P_4 \rightarrow$ โหนด D เมื่อโหนด B นำแพ็กเก็ต P_1 มาเพื่อพร้อมจะส่งไปยังโหนด A นั้น โหนดดังกล่าวก็จะมีตัวเลือกในการนำแพ็กเก็ต P_1 ไปเข้ารหัสกับแพ็กเก็ตอื่นๆที่อยู่ในแถวเรียงซึ่งเป็นหน่วยความจำสำรองของโหนด B ได้ดังนี้

1. $P_1 \oplus P_2$ ผลลัพธ์คือโหนด C สามารถถอดรหัสได้จากการนำแพ็กเก็ตเอ็กซ์คลูซีฟออร์ที่ได้จากโหนด B ($P_1 \oplus P_2$) มาเอ็กซ์คลูซีฟออร์กับแพ็กเก็ต P_1 ซึ่งมีอยู่แล้วในหน่วยความจำสำรองของโหนด C และสามารถอธิบายได้ดังสมการ $(P_1 \oplus P_2) \oplus P_1 = P_2$ แต่ A ไม่สามารถถอดรหัสได้เนื่องจากไม่มีแพ็กเก็ตที่สามารถถอดรหัสได้ในหน่วยความจำสำรอง

2. $P_1 \oplus P_3$ เป็นตัวเลือกที่ดีกว่าในตัวเลือกที่ 1. ด้วยโหนด A และ C นั้นสามารถถอดรหัสได้จากสมการ โหนด A: $(P_1 \oplus P_3) \oplus P_3 = P_1$, โหนด C: $(P_1 \oplus P_3) \oplus P_1 = P_3$

3. $P_1 \oplus P_3 \oplus P_4$ ถือเป็นตัวเลือกที่ดีที่สุดในการเข้ารหัส โดยการพิจารณาตัวเลือกจากแพ็กเก็ต P_1 ซึ่งกรณีนี้นั้นสามารถส่งแพ็กเก็ต 3 แพ็กเก็ตดั้งเดิมภายในการส่งเพียงครั้งเดียว ซึ่งโหนด A, B และ D สามารถถอดรหัสได้ โดยที่แต่ละโหนด สามารถถอดรหัสได้จากสมการที่ (2.1), (2.2) และ (2.3)

$$\text{โหนด A: } (P_1 \oplus P_3 \oplus P_4) \oplus P_3 \oplus P_4 = P_1 \quad (2.1)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$\text{โหนด B: } (P_1 \oplus P_3 \oplus P_4) \oplus P_1 \oplus P_4 = P_3 \quad (2.2)$$

$$\text{โหนด D: } (P_1 \oplus P_3 \oplus P_4) \oplus P_1 \oplus P_3 = P_4 \quad (2.3)$$

ตัวอย่างดังกล่าวนี้ ได้เน้นไปที่ประโยชน์ที่ได้รับจากการใช้เทคนิคการเข้ารหัสเครือข่าย ซึ่งแพ็กเกตจากการส่งแบบยูนิคาสต์ (unicast) หลายๆ แพ็กเกตนั้นอาจจะได้รับการเข้ารหัส ณ โหนดตัวกลางใดๆ ก็ได้ ขั้นตอนวิธีในการเข้ารหัสจะต้องทำให้แน่ใจว่าแพ็กเกตเข้ารหัสที่ถูกส่งออกไปนั้นสามารถถอดรหัสได้ โดยการส่งแพ็กเกต n แพ็กเกต P_1, \dots, P_n ไปยัง n ฮีโบลัดไป R_1, \dots, R_n โหนดตัวกลางจะต้องพิจารณาถึงการเข้ารหัสด้วยการเอ็กซ์คลูซีฟออร์ n แพ็กเกตด้วยกันได้ก็ต่อเมื่อ ฮีโบลัดไป R_i จะต้องมีแพ็กเกต $n-1$ เพื่อใช้ในการถอดรหัส

ค. การรับรู้สถานะของโหนดข้างเคียง (Learning Neighbor State)

การที่จะทราบว่าแต่ละโหนดนั้นมีแพ็กเกตโดยอยู่บ้าง อย่างที่อธิบายไปแล้วในหัวข้อโอกาสในการได้ยิน แต่ละโหนดในเครือข่ายนั้นจะมีกลไกที่คอยแจ้งโหนดข้างเคียงผ่านรายงานการรับรู้ อย่างไรก็ตามในแง่ของการถือครองช่องสัญญาณรายงานการรับรู้นั้นอาจจะล่าช้าหรือสูญหายได้ระหว่างการกระจายสัญญาณซึ่งส่งผลโดยตรงต่อการตัดสินใจในการเข้ารหัส ดังนั้นในแต่ละโหนดนั้นไม่อาจจะพึ่งพาการรับรายงานได้เพียงอย่างเดียวแต่จะต้องคาดเดาว่าโหนดข้างเคียงมีแพ็กเกตโดยอยู่ด้วย เพื่อที่จะคาดเดาได้อย่างมีประสิทธิภาพจำเป็นจะต้องใช้เทคนิคของการคำนวณการรั่วรั้ง ในการสื่อสารไร้สายนั้นมีโพรโตคอลในการหาความน่าจะเป็นในการส่งข้อมูล (delivery probability) ระหว่างคู่โหนดที่อยู่ใกล้เคียงกันเพื่อที่จะชี้วัดคุณภาพของเส้นทาง ในงานวิจัย [3] นั้นได้ทำการคำนวณความน่าจะเป็นในการส่งข้อมูลและกำหนดคุณภาพของเส้นทางด้วยค่าถ่วงน้ำหนักเท่ากับสมการที่ (3)

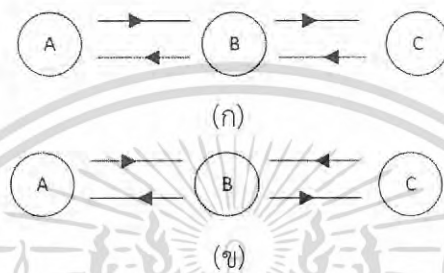
$$\text{ค่าถ่วงน้ำหนักของคุณภาพของเส้นทาง} = \frac{1}{\text{ความน่าจะเป็นในการส่งข้อมูล}} \quad (3)$$

ซึ่งค่าถ่วงน้ำหนักดังกล่าวนี้จะถูกกระจายสัญญาณไปยังทุกโหนดที่อยู่ในเครือข่าย และยังถูกนำไปใช้ในเร้าตั้งโพรโตคอล (Routing Protocol) ด้วยสถานะการเชื่อมโยง (link-state routing protocol) เพื่อใช้ในการคำนวณเส้นทางที่สั้นที่สุด

เทคนิคดังกล่าวถือเป็นต้นแบบของการเข้ารหัสซึ่งมุ่งเน้นไปที่โพรโตคอลการส่งข้อมูลในแบบมัลติคาสต์ ซึ่งแสดงตัวอย่างการเข้ารหัสเพิ่มเติมได้ดังรูปที่ 2.6 ซึ่งในการส่งรูปแบบที่ 1 (รูปที่ 2.6 (ก)) เป็นการส่งข้อมูลแบบธรรมดาตามมาตรฐานโหนด A และโหนด C ซึ่งต้องส่งข้อมูลระหว่างกันทั้งหมด 4 ครั้งคือ A-B, B-C, C-B และ B-A ถัดมาในวิธีการที่ 2 (รูปที่ 2.6 (ข)) โหนด B จะหยุดรอรับข้อมูลจากโหนด C และ

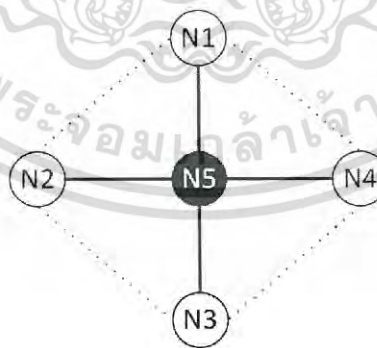
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

พิจารณาถึงปลายทางของทั้งสองแพ็กเก็ตว่าสามารถนำมาเอ็กซ์คลูซีฟออร์กันได้หรือไม่ โดยพิจารณาจากแพ็กเก็ตที่อยู่ในหน่วยความจำชั่วคราวของโหนด A และ B ด้วย จากนั้นโหนด B จะเป็นตัวกลางในการเข้ารหัสเครือข่ายด้วยการเข้ารหัสทั้งสองแพ็กเก็ตนี้จาก A และ B ก่อนที่จะทำการส่งแบบมัลติคาสต์ออกไปยังผู้รับทั้งสอง ในรูปแบบที่ 2. นั้นจะประหยัดการส่งลงได้ 3 จาก 4 ครั้ง ซึ่งผลประโยชน์ที่ได้จากการเข้ารหัสนั้นคือ coding gain = $\frac{4}{3}$



รูปที่ 2.6 ตัวอย่างการเข้ารหัสเครือข่ายด้วยการเอ็กซ์คลูซีฟออร์ระหว่าง 3 โหนด

นอกจากนี้ในงานวิจัย [4] ได้มีการประยุกต์นำโหนดเฝ้าสังเกต ซึ่งเป็นโหนดที่ช่วยให้โหนดที่อยู่ข้างเคียงนั้นสามารถแอบได้ยินหรือรับข่าวสารที่ไม่ได้ส่งถึงตัวเองโดยตรง ซึ่งจะต้องอยู่ในเครือข่ายและช่วงของการแพร่กระจายสัญญาณไร้สายเดียวกัน และยังสามารถนำข่าวสารเหล่านั้นมาประมวลผลเพื่อหาโอกาสที่จะนำข่าวสารซึ่งอยู่ในรูปของแพ็กเก็ตมาเข้ารหัสด้วยการเอ็กซ์คลูซีฟออร์ ซึ่งสามารถอธิบายความสัมพันธ์ระหว่างการรับส่งข้อมูลทั่วไปและการแอบได้ยินดังรูปที่ 2.7



รูปที่ 2.7 ทอพอโลยีรูปดาวที่มีโหนดเฝ้าสังเกต

ยกตัวอย่างจากความสัมพันธ์ในรูปที่ 2.7 โหนด N1 สามารถแอบได้ยินการส่งข้อมูลของ N2 และ N4 ซึ่งอยู่ในเครือข่ายเดียวกันและอยู่ในระยะทำการของการแพร่กระจายสัญญาณไร้สาย นอกจากนี้โหนด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

N2, N3 และ N4 สามารถทำได้ในรูปแบบที่คล้ายคลึงกัน เมื่อกำหนดให้ N1, N2, N3, N4 และ N5 แทน โหนดหมายเลขต่างๆ ในรูปที่ 2.7 โดยยกตัวอย่างด้วยการสมมติเหตุการณ์ที่เกิดขึ้นภายใน 1 รอบการวนซ้ำ (iteration) ดังนี้

N1 -> N2, N1 -> N4, N3 -> N4 และ N4 -> N2

เมื่อพิจารณาจากทอพอโลยี การส่งข้อมูลถึงกันนั้นจำเป็นต้องส่งผ่านโหนดศูนย์กลาง คือโหนด N5 เพราะฉะนั้นการส่งแต่ละแพ็กเก็ตไปที่โหนด N5 จะต้องใช้ทั้งหมด 4 ช่องเวลา (time slots) ดังนี้

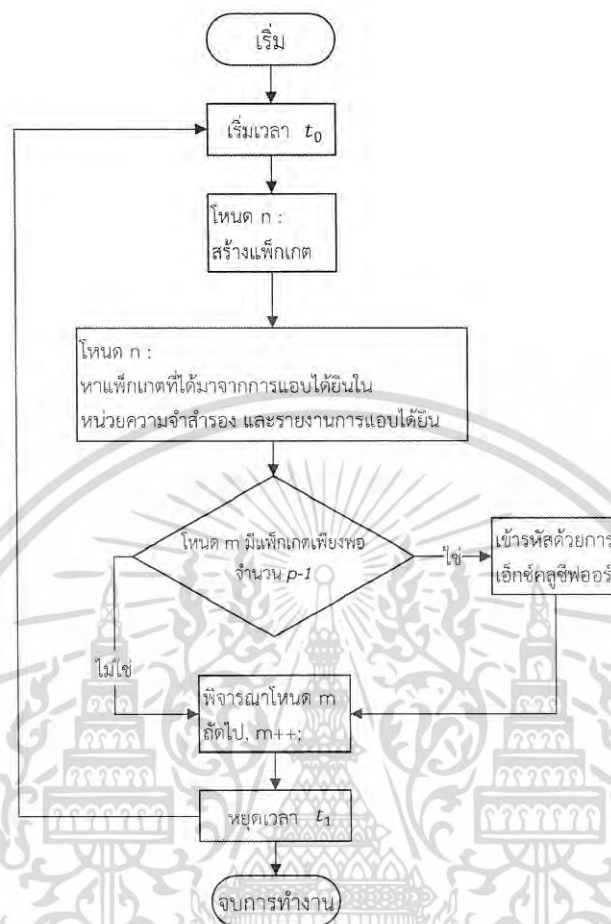
(N1 -> N5 (P_1), N1 -> N5 (P_2), N3 -> N5 (P_3), N4 -> N5 (P_4))

เมื่อ P_i แทนหมายเลขแพ็กเก็ต i
ตามเงื่อนไขในการกระจายสัญญาณ ดังนี้

1. ถ้าหากไม่มีการเอ็กซ์คลูซีฟเกิดขึ้น โหนด N5 จะทยอยส่งข้อมูลแต่ละแพ็กเก็ตให้กับโหนดผู้รับ ดังนี้ (P_1 -> N2, P_2 -> N4, P_3 -> N4, P_4 -> N2) ซึ่งช่องเวลาที่ได้นำมาพิจารณา คือความพร้อมในการรับข้อมูล

2. ถ้าหากมีการเอ็กซ์คลูซีฟเกิดขึ้น ยกตัวอย่างเช่นสร้าง $P_{xor1} = P_1 \oplus P_2$ ที่โหนด N5 โหนด N5 จะทำการส่งข้อมูลให้แก่โหนดผู้รับ ดังนี้ (P_{xor1} -> N2, N4) และส่งข้อมูลด้วยแพ็กเก็ตมาตรฐานอีกด้วย (P_3 -> N4, P_4 -> N2) เมื่อเปรียบเทียบแล้วพบว่า การส่งข้อมูลของโหนด N5 จะสามารถประหยัดได้ 1 ช่องเวลา (1-2 ช่องเวลาสำหรับเงื่อนไข) ซึ่งในแผนผังการดำเนินงานรูปที่ 2.8 จะแสดงขั้นตอนวิธีในการหาโอกาสที่จะนำมาเข้ารหัสของโหนดตัวกลาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.8 ผังงานในการจำลองการส่งข้อมูลแบบเอ็กซ์คลูซีฟออร์

ขั้นตอนวิธีเพื่อที่จะหาโอกาสในการเข้ารหัสแสดงดังผังรูปที่ 2.8 โดยเริ่มจากการสร้างแพ็กเก็ตในแต่ละโหนดข้อมูลใดๆ (N) จากนั้นก็จะเก็บแพ็กเก็ตที่สร้างไว้ในหน่วยความจำชั่วคราว เมื่อมีโหนดข้อมูลอื่นๆ มีการรับ-ส่ง แพ็กเก็ตเกิดขึ้น ด้วยคุณสมบัติของโหมดแฝงจะ使得โหนดข้างเคียงนั้นสามารถรับฟังข้อมูลนั้นได้ โดยยกตัวอย่างจากรูปที่ 2.7 ถ้าหากโหนดข้อมูล N2 ส่งแพ็กเก็ตไปยังโหนดส่งผ่าน N5 จากความสัมพันธ์โหนดข้อมูล N1 และโหนดข้อมูล N4 ก็จะสามารถได้รับข่าวสารนี้ด้วย ซึ่งโหนดที่อยู่รอบข้างโหนดส่งผ่าน N5 ต้องมีการส่งข้อมูลตอบกลับเป็นข้อมูลการได้ยินซึ่งรวมถึงแพ็กเก็ตที่ โหนดนั้นเองสร้างมาและนำมาไว้ในหน่วยความจำชั่วคราวด้วยรายงานการรับรู้ ซึ่งภายในช่วงเวลานี้เองโหนดส่งผ่าน N5 จะรวบรวมข้อมูลภายในช่วงเวลานี้และนำมาตัดสินใจว่าแพ็กเก็ตใดควรที่จะนำมาเอ็กซ์คลูซีฟออร์กัน จากนั้นเมื่อผู้รับได้รับแพ็กเก็ตที่ได้เข้ารหัสไว้โดยการเอ็กซ์คลูซีฟออร์ จะเริ่มทำการถอดรหัสโดยตรวจสอบดูว่าแพ็กเก็ตเอ็กซ์คลูซีฟออร์ นั้นเกิดจากการเอ็กซ์คลูซีฟออร์ระหว่างแพ็กเก็ตใดบ้าง จากนั้นโหนดก็จะตรวจสอบหน่วยความจำชั่วคราว (Temporary memory) เพื่อหาโอกาสที่จะถอดรหัสได้หรือไม่ ดังสมการที่ (4)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$P_n = P_{xor} \oplus (P_1 \oplus P_2 \oplus P_3 \dots) \quad (4)$$

เมื่อ P_n คือ แพ็กเก็ตที่ต้องการจะนำมาถอดรหัส และ P_{xor} คือแพ็กเก็ตที่ได้รับการเอ็กซ์คลูซีฟออร์แล้ว ในงานวิจัย [4] ได้นำเสนอแนวคิดที่สามารถเพิ่มประสิทธิภาพในเครือข่ายไร้สายหรือแม้กระทั่งในเครือข่ายไวแมกซ์ (WiMAX) ซึ่งสามารถทำงานร่วมกับโพรโตคอลควบคุมการใช้สื่อสัญญาณได้หลายรูปแบบ และได้ทดสอบกับเครือข่ายแบบตาข่ายโดยมีจำนวนโหนด 20 โหนด ซึ่งผลที่ได้นั้นช่วยเพิ่มทราฟฟิกของการส่งข้อมูลโดยรวมและยังช่วยลดเวลาในการส่งข้อมูล ด้วยการเข้ารหัสเครือข่ายด้วยการเอ็กซ์คลูซีฟออร์อีกทั้งยังเพิ่มประสิทธิภาพในการถือครองช่องสัญญาณอีกด้วย

นอกจากนี้ยังมีงานอื่นๆที่น่าสนใจและศึกษาประสิทธิภาพของการแอบได้ยิน เช่น ใน [6] Paschos, et.al. ได้ศึกษาช่องสัญญาณการกระจายสัญญาณในเครือข่ายขนาด 1 ฮอป ซึ่งในฝั่งผู้รับการได้มาซึ่งข่าวสารจากโหนดข้างเคียงจะทำให้เทคนิคการเข้ารหัสเครือข่ายนั้นมีประสิทธิภาพ โดยการทดลองได้ทดสอบในระบบที่สามารถคาดเดาได้ (deterministic system) ซึ่งข้อมูลต่างๆ ที่อยู่ในโหนดผู้รับนั้นจะถูกประกาศให้โหนดอื่นๆ ทราบด้วยรายงานการรับรู้ และระบบที่ไม่สามารถคาดเดาได้หรือระบบสุ่ม (stochastic system) โหนดตัวกลางที่ทำหน้าที่เข้ารหัสนั้นจะตัดสินใจเข้ารหัสผ่านเทคนิคการควบคุมแบบสุ่มโดยอาศัยพื้นฐานจากข้อความตอบกลับเชิงลบ (Negative Acknowledgement : NACK) ซึ่งผลที่ได้ชี้ว่าการเข้ารหัสเครือข่ายโดยอาศัยการแอบได้ยินเพื่อให้ได้ข่าวสารจากโหนดข้างเคียงใน [4] นั้นความน่าจะเป็นของการรับข้อมูลหรือคุณภาพของเส้นทางจะต้องมากเพียงพอเพื่อให้การเข้ารหัสเครือข่ายมีประสิทธิภาพสูงสุด

2.3 ทฤษฎีกราฟและการประยุกต์

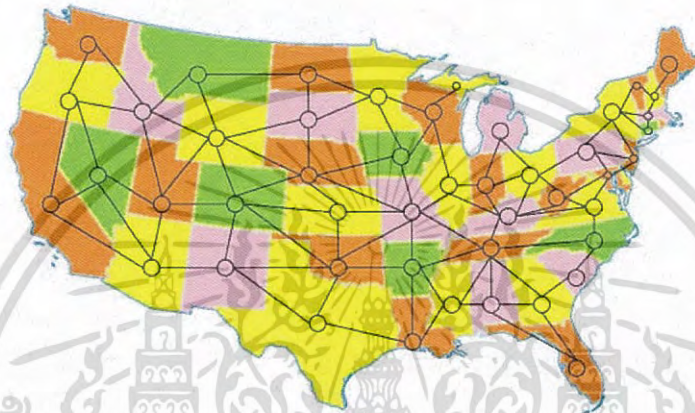
ในส่วนของหัวข้อนี้จะเป็นการนำเสนอเรื่องการใช้ทฤษฎีกราฟที่นำมาประยุกต์ใช้กับการเข้ารหัสเครือข่าย ซึ่งแบ่งเป็นหัวข้อย่อย 3 หัวข้อ เริ่มต้นที่หัวข้อ 2.3.1 เป็นการบรรยายคุณลักษณะของกราฟ 4 สี และเชื่อมโยงไปยังทฤษฎีกราฟไมเนอร์ ในหัวข้อ 2.3.2 ซึ่งถูกนำมาประยุกต์ใช้ภายหลัง และในหัวข้อ 2.3.3 จะเป็นการสร้างข้อความคาดเดาเพื่อใช้ในการเข้ารหัสเครือข่าย

2.3.1 ทฤษฎีกราฟ 4 สี

ทฤษฎีกราฟ 4 สี (4 Colors theorem) [15] นั้นเกิดมาจากการตั้งคำถามเกี่ยวกับการสร้างแผนที่ด้วยการระบายสีประเทศแต่ละประเทศในแผนที่โดยมีเงื่อนไขให้ประเทศที่ติดกันนั้นจะต้องมีสีที่แตกต่างกัน หรือคำถามเกี่ยวกับจำนวนวันที่จะต้องกำหนดให้กับผู้เข้าประชุม โดยที่ผู้เข้าประชุมทุกคนต้องการที่จะเข้าประชุมเพียงวันใดวันหนึ่ง โดยในคำถามแรกแสดงตัวอย่างได้ดังรูปที่ 2.9 ซึ่งแทนด้วยแผนที่รัฐต่างๆ ของประเทศสหรัฐอเมริกา ซึ่งแต่ละรัฐนั้นแทนโหนดในกราฟและยังมีลักษณะเป็นกราฟระนาบอีกด้วย และสำหรับการระบายสีให้กับแต่ละโหนดในกราฟระนาบ G ใดๆ เมื่อกำหนดให้ $G = (V, E)$ ซึ่งมี V

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

และ E คือจุดยอด/โหนด (Vertex) และเส้นเชื่อม (Edge) ตามลำดับ โดยที่จุดยอดที่ได้รับการระบายสี (coloring vertex) จะเป็นการระบายสีจากเซตของจุดยอดไปยังเซตของสี (S) ซึ่งแทนด้วย $c : V \rightarrow S$, และ $c(v) \neq c(w)$ เมื่อ c และ w คือจุดยอดที่อยู่ติดกัน โดยจะเรียกสมาชิกของเซต S ว่าจำนวนสี และสนใจขนาดของสีหรือขนาดของเซต S ที่เล็กที่สุดซึ่งเป็นเลขจำนวนเต็ม k โดยสำหรับกราฟ G ใดๆ แล้วจะเรียกว่ากราฟ k สี (k -colorable)



รูปที่ 2.9 แผนที่และความสัมพันธ์กราฟด้วยทฤษฎี 4 สี

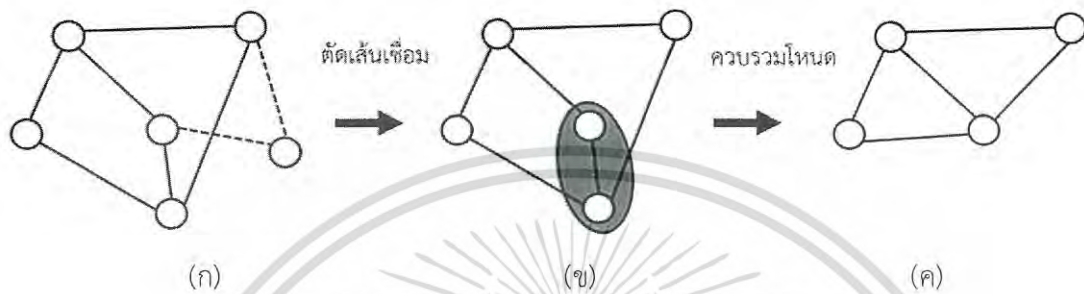
โดยกราฟระนาบ (Planar graph) นั้นจะมีความต้องการสีอย่างน้อย 4 สี ซึ่งกราฟระนาบก็คือกราฟที่สามารถลากเส้นเชื่อมไปยังจุดต่างๆ กันได้โดยที่ไม่มีเส้นเชื่อมทับกัน นอกจากนี้ยังสามารถหาจำนวนสีของกราฟได้จากอัลกอริธึมกริดดี้ (Greedy Algorithm) ซึ่งมีขั้นตอนดังนี้

1. เริ่มจากทุกจุดยอด v ใดๆ (ที่ยังไม่ได้กำหนดสี)
2. กำหนดสีให้จุดยอด v_i ด้วยสี c_j โดยที่ไม่ขัดแย้งกับสีของโหนดข้างเคียง เมื่อ $i \in (1, n), j > 0$ เมื่อ n คือจำนวนจุดยอดทั้งหมด
3. ทำซ้ำข้อ 2. จนกว่าทุกจุดยอดจะได้รับการกำหนดสี

2.3.2 ทฤษฎีกราฟไมเนอร์

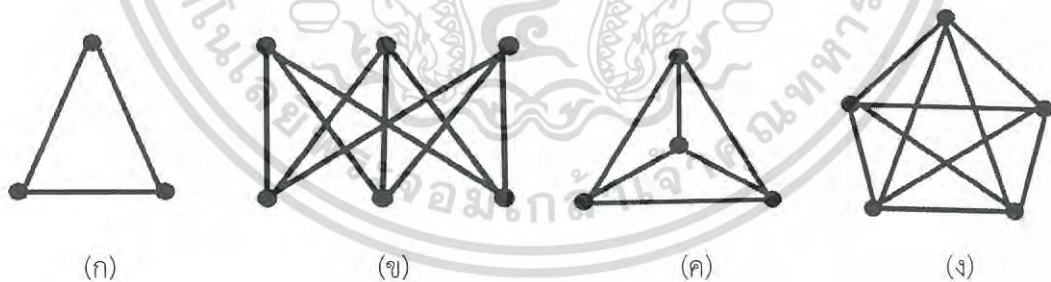
ทฤษฎีกราฟไมเนอร์ (Graph minors theorem) [15] เป็นการขยายแนวคิดของกราฟย่อย ซึ่งมีประโยชน์ในการสร้างแบบจำลองพื้นฐานเพื่อใช้ในการเชื่อมความสัมพันธ์ระหว่างกราฟในกราฟย่อยคือชุดของผลลัพธ์ที่ได้เกิดจากการดำเนินการลบเส้นเชื่อมจากกราฟ G เดิม ผลที่ได้คือกราฟไมเนอร์ M รูปที่ 2.10 (ค) ซึ่งได้จากการหดตัวของกราฟ (contraction) ของเส้นเชื่อมที่อยู่ในกราฟ G โดยที่การหดตัวนั้นจะประกอบไปด้วยการดำเนินการตัดและการลบเส้นเชื่อม ในรูปที่ 2.10 แสดงให้เห็นถึงการหดตัวของเส้นเชื่อม uv ใดๆ ในกราฟ G เมื่อ u และ v คือโหนดใดๆ ในกราฟ G ซึ่งใน รูปที่ 2.10 (ก) คือการตัดเส้น

เชื่อม และ รูปที่ 2.10 (ข) คือการควบรวมโหนด ซึ่งปกติแล้วหลังจากการดำเนินการอย่างเป็นลำดับเพื่อให้ได้กราฟไมเนอร์ โหนดในกราฟไมเนอร์ M ที่ได้จะมีลักษณะการเชื่อมต่อทั้งโหนดใหม่ที่ได้และเส้นเชื่อม และ จะมีความสอดคล้องกับกราฟ G เดิม



รูปที่ 2.10 การรวมเส้นเชื่อม (ก) และการตัดเส้นเชื่อม (ข) ซึ่งเป็นการดำเนินการซึ่งใช้สำหรับกราฟไมเนอร์ (ค)

แนวคิดของกราฟไมเนอร์ ได้ถูกอธิบายไว้ในบริบทของกราฟไม่แสดงทิศทาง (undirected graph) ในขณะที่เครือข่ายมัลติคาสต์ในงานวิจัยนี้จำลองด้วยกราฟแสดงทิศทาง (directed network) ซึ่งกราฟไมเนอร์นั้นคือกราฟที่มีลักษณะเป็นกราฟสมบูรณ์ ซึ่งแต่ละโหนดนั้นจะสามารถเชื่อมโยงไปยังโหนดอื่นๆ ที่เหลือทุกโหนด ซึ่งมีลักษณะต่างๆ ดังรูปที่ 2.11



รูปที่ 2.11 กราฟไมเนอร์ในลักษณะต่างๆ (ก) กราฟไมเนอร์ K_3 (ข) กราฟไมเนอร์ $K_{3,3}$ (ค) กราฟไมเนอร์ K_4 (ง) กราฟไมเนอร์ K_5

เมื่อกล่าวถึงเครือข่ายมัลติคาสต์ G ประกอบด้วยไมเนอร์ M หมายความว่าในเครือข่ายมีคุณสมบัติของกราฟไม่มีทิศทางวางซ้อนอยู่กับกราฟ G ซึ่งได้มาจากการที่ไม่สนใจจุดเริ่มต้นของแต่ละเส้นเชื่อมใน G ซึ่งมี M เป็นกราฟไมเนอร์ และในมุมมองของการออกแบบอัลกอริธึมที่มีประสิทธิภาพ การทดสอบว่า

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

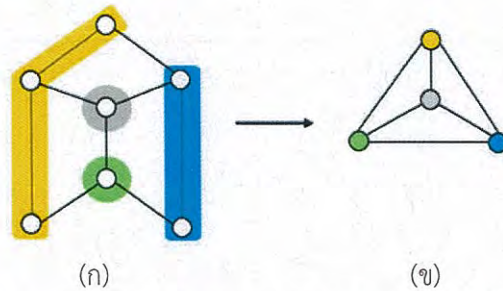
กราฟ G มีกราฟไมเนอร์ M ขนาดคงที่ที่สามารถทำได้โดยมีประสิทธิภาพภายในเวลา $O(n^3)$ เมื่อ n คือจำนวนโหนดในกราฟ G [21]

2.3.3 การเชื่อมโยงโครงสร้างรหัสพีชคณิตด้วยทอพอโลยี

การเชื่อมโยงโครงสร้างรหัสพีชคณิตด้วยทอพอโลยี [22] เป็นเทคนิคที่มุ่งเน้นไปที่ความสัมพันธ์ระหว่างการเข้ารหัสเชิงพีชคณิตและทฤษฎีกราฟในเชิงลึกในบริบทของการเข้ารหัสเครือข่าย ซึ่งเป้าหมายคือ การจำแนกคุณลักษณะของกราฟระหว่าง : (1) ลักษณะจำเพาะของทอพอโลยีของเครือข่าย (network topology) และลักษณะโครงสร้างที่แฝงตัวอยู่ (2) ความจำเป็นรวมถึงการคำนึงถึงผลประโยชน์ที่ได้รับ และความซับซ้อนของการเข้ารหัสเครือข่าย เครื่องมือที่เกี่ยวข้องกับกราฟไมเนอร์ นั้นเป็นที่รู้จักกันดีและมีประสิทธิภาพพอที่จะเชื่อมโยงคุณสมบัติของกราฟด้วยโครงสร้างที่แฝงตัวอยู่ในเครือข่าย [15] ตัวอย่างงานวิจัยที่มีชื่อเสียงคือทฤษฎีของ Kuratowski ซึ่งได้ระบุไว้ว่า กราฟจะเป็นกราฟระนาบได้ก็ต่อเมื่อไม่มีส่วนประกอบของกราฟไมเนอร์ K_5 และ $K_{3,3}$ เท่านั้น [15] ดังที่แสดงในรูปที่ 2.11 ลักษณะโครงสร้างของกราฟย่อยที่แฝงตัวอยู่หรือกราฟไมเนอร์ M ของกราฟ G ได้มาจากการลบและหรือการหดตัวกันในขอบเขตของเส้นเชื่อมใดๆ ในกราฟ G ซึ่งถูกควมรวมเรียกว่า “ซูเปอร์-โหนด” โดยกราฟไมเนอร์ K_4 ได้จากกราฟรูปสี่เหลี่ยมซึ่งเป็นทอพอโลยีของเครือข่ายที่ทราบกันดีว่าการใช้รหัสเครือข่ายจะมีประสิทธิภาพดีกว่าการเร้าตั้ง ซึ่งในทางทฤษฎีกราฟเรียกว่าทรีแพคกิ้ง (Tree packing) [16] ซึ่งภายหลัง ได้มีการพิสูจน์แล้ว [22] ด้วยใช้ตัวอย่างขัดแย้งว่า ในทุกๆ เครือข่ายที่มีการส่งข้อมูลแบบมัลติ-คาสต์ที่มีการเข้ารหัสเครือข่ายจะมีประสิทธิภาพดีกว่าการใช้เร้าตั้งโพรโตคอลตามมาตรฐานนั้นจะต้องมีคุณสมบัติกราฟไมเนอร์ K_4 แฝงอยู่ ซึ่งกราฟดังกล่าวนี้เป็นกราฟสมบูรณ์ที่มี 4 โหนดในรูปที่ 2.12 (ข)

ในงานวิจัย [22] ได้นำเสนอ ข้อความคาดการณ์แบบ NC-Minor ซึ่งเชื่อมโยงการเข้ารหัสเครือข่ายเข้ากับทฤษฎีกราฟไมเนอร์ โดยเริ่มจากเครือข่ายมัลติคาสต์ที่ต้องการขนาดฟิลด์ที่แน่นอนสำหรับการเข้ารหัสซึ่งต้องประกอบด้วยจำนวนกลุ่มของกราฟไมเนอร์ (Clique) ที่เกี่ยวข้อง และยังได้พิสูจน์อีกว่าข้อความคาดการณ์แบบ NC-Minor นั้นมีความคล้ายคลึงกันกับข้อความคาดการณ์แบบ Hadwiger ซึ่งเป็นทฤษฎีที่รู้จักกันดีในทฤษฎีกราฟ ซึ่งข้อความคาดเดา NC-Minor นี้สามารถแสดงให้เห็นถึงเครือข่ายที่ปราศจากกราฟไมเนอร์ K_{q+2} ซึ่งการเข้ารหัสบนฟิลด์ F_q นั้นเพียงพอสำหรับกรณีที่มามีค่า q เท่ากับ $q = 2, 3, 4$ สำหรับค่า q ที่มีค่าสูงกว่านั้น และสำหรับเครือข่ายที่ปราศจากกราฟไมเนอร์ K_q การเข้ารหัสบนฟิลด์ $F_{q \log(q)}$ นั้นถือว่าเพียงพอ โดยสรุปแล้ว [22] แสดงให้เห็นว่า ในเครือข่ายมัลติคาสต์ที่ต้องการการเข้ารหัสเครือข่ายที่มีประสิทธิภาพเข้าถึงค่าความจุจะต้องมีคุณสมบัติไมเนอร์ K_4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.12 กราฟไมเนอร์ K_4 (ก) ในเครือข่ายรูปสี่เหลี่ยม (ข)

2.3.3.1 ข้อความคาดการณ์แบบ Hadwiger

ข้อความคาดการณ์แบบ Hadwiger (Hadwiger Conjecture) [17][18] ซึ่ง Hugo Hadwiger ได้คิดค้นขึ้นในปี 1943 เป็นหัวข้อที่รู้จักกันดีในแง่ของผลกระทบและการจำแนกความจำเป็นของจำนวนสีที่ใช้ในการระบายสีกราฟด้วยการเสนอเหตุผลพื้นฐานที่ได้สอดคล้องกับโครงสร้างที่อยู่ภายในโครงสร้างของกราฟไมเนอร์ ข้อความคาดการณ์นี้ได้ผ่านการพิสูจน์ในหลายกรณี รวมถึงทฤษฎีที่มีชื่อเสียงอย่าง ทฤษฎีบทกราฟสี่สี (Four Color Theorem) แต่ก็ยังคงมีการเปิดกว้างในการหารูปแบบทั่วไป

นิยาม 1 : ข้อความคาดการณ์แบบ Hadwiger กำหนดให้กราฟ G ใดๆ ที่มีการระบายสีด้วย q สีจะประกอบด้วยไมเนอร์ K_q โดยที่ K_q คือกราฟสมบูรณ์ที่มี q โหนด

กราฟ G นั้นสามารถระบายได้ด้วยจำนวน q สี เมื่อ q เป็นจำนวนสีที่น้อยที่สุดที่ต้องการในการระบายสีกราฟ G ซึ่งโหนดที่อยู่ใกล้กันจะถูกระบายสีที่แตกต่างกันเสมอ และเมื่อกรณีที่ $q = 5$ ข้อความคาดการณ์แบบ Hadwiger จะอ้างถึงทฤษฎีบทกราฟสี่สี (Four Color Theorem) ที่ระบุว่าในทุกๆ กราฟระนาบจะมีจำนวนสีที่ต้องใช้อย่างมากที่สุด 4 สี ดังนั้นกราฟระนาบจะไม่มีทั้งคุณสมบัติของกราฟไมเนอร์ K_5 และ $K_{3,3}$ เป็นส่วนประกอบ

ในความเป็นจริงสำหรับค่า $q \leq 6$ ข้อความคาดการณ์แบบ Hadwiger ถูกพิสูจน์แล้วว่าเป็นจริง [19] และสำหรับค่า q ใดๆ ที่มีค่าสูงกวานั้น ผลลัพธ์ที่เป็นที่รู้จักกันดีคือ ทุกๆ กราฟที่มี q สี (กราฟที่มีการระบายสีด้วย q สี) จะมีจำนวนกลุ่มของกราฟไมเนอร์เป็นจำนวน $O\left(\frac{q}{\log q}\right)$ โหนด [20] ดังนั้นจุดอ่อนของข้อความคาดการณ์นี้ก็ยังคงเป็นปัญหาเปิด : ในสำหรับทุกกราฟที่มี q สี ซึ่งประกอบด้วย $K_{[cq]}$ เป็นกราฟไมเนอร์โดยที่ค่า c เป็นค่าคงที่ใดๆ ที่มีน้อยกว่า 1 สำหรับการเชื่อมต่อข้อความคาดการณ์แบบ NC-Minor กับข้อความคาดการณ์แบบ Hadwiger ยังพิจารณาข้อความข้างล่างนี้ที่มีความหนักแน่นมากกว่าข้อบกพร่องของข้อความคาดการณ์แบบ Hadwiger ซึ่งมีนิยามดังกล่าว

นิยาม 2 : ข้อความคาดการณ์แบบ Hadwiger ที่มีขอบพร้อม ทุกกราฟที่มีการระบายสีด้วย q สีจะประกอบด้วยไมเนอร์ K_{q-1}

2.3.3.2 ข้อความคาดการณ์แบบ NC-Minor

ข้อความคาดการณ์แบบ NC-Minor (NC-Minor Conjecture) มีที่มาจาก การสังเกตการเข้ารหัสบนฟิลด์ขนาดใหญ่และข้อความคาดการณ์นี้มีเส้นเชื่อมมากมายซึ่งเป็นคุณสมบัติที่ต้องการในเครือข่ายมัลติคาสต์ ซึ่งจะเห็นได้อย่างชัดเจนในการรวมกันของเครือข่าย [23] ตัวอย่างคือ เมื่อการเข้ารหัสเครือข่ายมีประสิทธิภาพเหนือกว่าส่งผ่านข้อมูลด้วยการเร้าตั้ง ซึ่งในมุมมองของทฤษฎีกราฟคือ ทรีแพกกิ้ง (tree packing) นอกจากนี้ในมุมมองของกราฟไมเนอร์สามารถระบุจุดเชื่อมต่อระหว่างระหว่างกลุ่มของกราฟไมเนอร์ และยังสามารเขียนในรูปแบบของกราฟไมเนอร์ สำหรับเครือข่ายกราฟ G ที่มีเส้นเชื่อมมากมายใดๆ ได้ด้วย ในหัวข้อนี้ได้กำหนดนิยามของข้อความคาดการณ์ดังกล่าว พร้อมทั้งนำเสนอขั้นตอนวิธีเพื่อหาคุณสมบัติกราฟไมเนอร์ในกราฟ G ใดๆ ในหัวข้อที่ 2.3.3.3

นิยาม 3 : ข้อความคาดการณ์แบบ NC-Minor หากเครือข่ายมัลติคาสต์ G ไม่มีกราฟไมเนอร์ K_{q+2} เป็นส่วนประกอบแล้ว การเข้ารหัสบนฟิลด์จำกัด $F_{f(q)}$ นั้นเพียงพอที่จะทำให้เกิดค่าทรูพุดที่เหมาะสมที่สุดใน กราฟ G เมื่อ $f(q)$ คือค่าของเลขยกกำลังของจำนวนเฉพาะที่น้อยที่สุดที่มีค่ามากกว่า q

2.3.3.3 การกระจายการไหลแบบมัลติคาสต์และกราฟต้นไม้ย่อย

การกระจายการไหลแบบมัลติคาสต์ (Multicast Flow Decomposition) และกราฟต้นไม้ย่อย (Subtree Graphs) ได้สร้างความเท่ากันระหว่างข้อความคาดการณ์แบบ NC-Minor และข้อความคาดการณ์แบบ Hadwiger ด้วยการนำเครื่องมือที่มีประโยชน์บางส่วนจากงานวิจัยของการเข้ารหัสเครือข่ายเพื่อจัดการการไหลของข้อมูลแบบมัลติคาสต์และเชื่อมโยงปัญหาการกำหนดรหัสเข้ากับการจำแนกสีกราฟ เทคนิคการกระจายการไหลแบบมัลติคาสต์ (Information flow decomposition) ถูกนำเสนอครั้งแรกโดย Fragouli และ Soljannin [25] โดยกำหนดให้กราฟ G เป็นเครือข่ายแบบ 2-minimal และอาจรวมเป็นกราฟต้นไม้ย่อยด้วยการแยกเป็นกราฟต้นไม้ย่อย a, b, c และ d ซ้ำๆ ดังวิธีการต่อไปนี้

1. เริ่มต้นจากพิจารณาเส้นเชื่อมที่เชื่อมโยงออกจากโหนดแหล่งกำเนิด หรือโหนดอื่นๆ ที่มีดีกรีขาเข้าเป็น 0 และดีกรีขาออกมากกว่า 1 และแทนโหนดทั้งสองด้วย u และ v ตามลำดับ

2. พิจารณาโหนด w ซึ่งเป็นโหนดที่เชื่อมต่อโดยตรงกับโหนด v ผ่านดีกรีขาออกทั้งหมดว่ามีดีกรีขาเข้ามากกว่า 1 หรือมีดีกรีขาออกเท่ากับ 0 หรือไม่

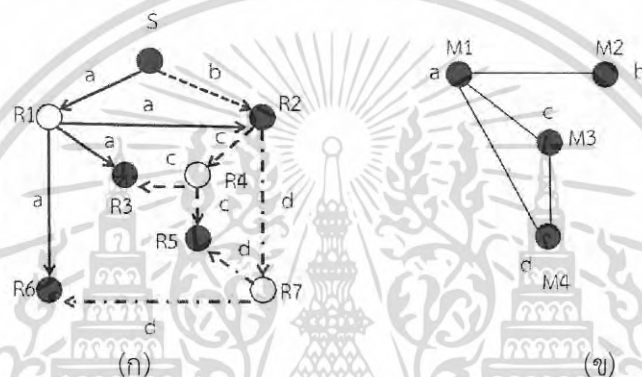
- 2.1 ควบรวมเส้นเชื่อมจากโหนดระหว่าง u และ v และระหว่างโหนด v และ w ใดๆ ที่มีเงื่อนไขดังกล่าวเข้าเป็น 1 โหนดในกราฟไมเนอร์ M

- 2.2 ลบเส้นเชื่อมที่ได้ทำการรวบรวมไปแล้วในข้อ 2.1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3. ทำซ้ำในขั้นตอนที่ 2 จนกว่าจะไม่มีเส้นเชื่อมใดๆ ให้เพิ่มอีก

โดยกราฟ G คือกราฟที่มีการลดรูปเส้นเชื่อม กล่าวคือเส้นเชื่อมระหว่างคูโหนดใดๆ จะสามารถมีได้เพียง 1 เส้นเชื่อมเท่านั้น ซึ่งทุกๆ การพิจารณาคูโหนดในขั้นตอนดังกล่าวส่งผลให้ผลลัพธ์ที่ได้ในรูปแบบของกราฟไมเนอร์มีลักษณะเฉพาะตัว นอกจากนี้ยังสังเกตได้ว่าทิศทางการไหลของข้อมูลระหว่างกราฟ G และกราฟไมเนอร์ M ซึ่งถือว่าเป็นกราฟต้นไม้ย่อยชนิดหนึ่งในทฤษฎีกราฟนั้นมีความสัมพันธ์กัน ดังตัวอย่างที่จะแสดงดังในรูปที่ 2.13



รูปที่ 2.13 กราฟเครือข่าย 2-minimal (ก) และกราฟต้นไม้ส่วนย่อย (subtree graph) ของเครือข่ายดังกล่าว (ข)

ในรูปที่ 2.13 (ก) แสดงกราฟเครือข่าย 2-minimal ที่มีโหนด S เป็นโหนดแหล่งกำเนิด โหนด $R1, R2, R3, R4$ และ $R5$ คือโหนดส่งผ่าน และโหนด $R6, R7$ เป็นโหนดผู้รับ และในรูปที่ 2.13 (ข) คือผลลัพธ์ที่ได้จากเทคนิคการกระจายการไหลแบบมัลติคาสต์ ซึ่งมีขั้นตอนดังนี้

1. ให้ G คือกราฟที่กำลังพิจารณาและ M คือกราฟไมเนอร์ที่ได้ โดยเริ่มจากคูโหนดระหว่างโหนดแหล่งกำเนิดกับโหนดใดๆ ก็ตามที่เชื่อมต่อไปยังโหนดแหล่งกำเนิดโดยตรงที่มีดีกรีขาเข้าเท่ากับ 1 เช่น คูโหนดแหล่งกำเนิด S และโหนดส่งผ่าน $R1$ ที่มีดีกรีขาเข้าเพียง 1
2. พิจารณาทุกๆ ดีกรีขาออกของโหนดส่งผ่าน $R1$ ว่าไปยังโหนดใดๆ ที่มีดีกรีขาเข้าเป็น 1 หรือไม่ เช่น โหนดที่เชื่อมโยงกับโหนดส่งผ่าน $R1$ ได้แก่ โหนดส่งผ่าน $R2, R3$ และโหนดผู้รับ $R6$ โดยทั้งสามโหนดนั้นไม่มีดีกรีขาเข้าเท่ากับ 1 แต่มีดีกรีขาออกมากกว่า 0
3. ทำการควบรวมเส้นเชื่อมที่เชื่อมโยงจากโหนด S ไปยังโหนดส่งผ่าน $R1$ และจากโหนดส่งผ่าน $R1$ ไปยัง โหนด $R2, R3, R6$ เป็น 1 โหนด (โหนด $M1$) ในกราฟไมเนอร์ M พร้อมทั้งตัดเส้นเชื่อมที่พิจารณาแล้วในกราฟ G
4. พิจารณาคูโหนดแหล่งกำเนิด S และโหนดส่งผ่าน $R2$ ซึ่งตอนนี้มีดีกรีขาเข้าเท่ากับ 1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5. พิจารณาทุกๆ ดิกรีขาออกของโหนดส่งผ่าน R2 ว่าไปยังโหนดใดๆ ที่มีดิกรีขาเข้าเป็น 1 หรือไม่ ซึ่งโหนดที่เชื่อมโยงกับโหนดส่งผ่าน R2 ได้แก่ โหนดส่งผ่าน R4 และโหนดผู้รับ R7 ซึ่งทั้งคู่มีดิกรีขาเข้าเท่ากับ 1 ซึ่งไม่สามารถควบรวมได้ ในขั้นตอนนี้ทำได้เพียงควบรวมเส้นเชื่อมจากโหนดแหล่งกำเนิด S ไปยังโหนดส่งผ่าน R2 เท่านั้น และเพิ่มโหนด M2 ลงไปในกราฟไมเนอร์ M

6. พิจารณาโหนด R2 และโหนดส่งผ่าน R4 เช่นเดียวกันกับที่ผ่านมา โดยโหนดส่งผ่าน R4 เชื่อมโยงไปยังโหนดส่งผ่าน R3 มีดิกรีขาเข้าเท่ากับ 1 แต่มีดิกรีขาออกเท่ากับ 0 และโหนด R5 ซึ่งมีดิกรีขาเข้าเท่ากับ 2 สามารถควบรวมเส้นเชื่อมระหว่างโหนดดังกล่าวนี้ได้ โดยเพิ่มเป็นโหนด M3 ในกราฟไมเนอร์ M

7. สุดท้ายพิจารณาโหนด R2 และโหนดผู้รับ R7 โดยโหนดผู้รับ R7 เชื่อมโยงไปยังโหนดส่งผ่าน R5 และโหนดผู้รับ R6 ซึ่งทั้งคู่มีดิกรีขาเข้าเท่ากับ 1 และดิกรีขาออกเท่ากับ 0 โดยสามารถควบรวมได้ และเพิ่มโหนด M4 ในกราฟไมเนอร์ M

ถัดมาเป็นทฤษฎีบทเสริมสองบท ซึ่งจะเป็นการสร้างความสัมพันธ์ระหว่างฟิลต์ที่ต้องการขั้นต่ำในการเข้ารหัสและจำนวนสีในกราฟต้นไม้ส่วนย่อย (subtree graph)

ทฤษฎีบทเสริม 1 : ถ้าหากมีการเข้ารหัสบนฟิลต์จำกัด F_q แล้วกราฟต้นไม้ย่อยของกราฟจะสามารถมีสีได้ $q + 1$ สี

พิสูจน์ : สำหรับการไหลของข้อมูลจากแหล่งกำเนิดสองแหล่ง เวกเตอร์ในการเข้ารหัสจะถูกเลือกจาก $F_q \times F_q$ แต่ละเวกเตอร์เข้ารหัสจะต้องมีคุณสมบัติเป็นอิสระเชิงเส้นจากเวกเตอร์ใดเวกเตอร์หนึ่งดังนี้ $\{(0, 1), (1, 0), (1, 1 = \alpha^0), (1, \alpha), \dots, (1, \alpha^{q-2})\}$ เมื่อ α คือองค์ประกอบพื้นฐานใน F_q ดังนั้นการแก้ปัญหาของการเข้ารหัสจะเป็นไปได้ ด้วยจำนวน $q + 1$ เวกเตอร์ตามที่ระบุไว้ข้างบนระบายนีของแผนภาพต้นไม้ย่อยของกราฟด้วย $q + 1$ สี ตามเวกเตอร์การเข้ารหัสนั้นจะเป็นการแก้ปัญหการเข้ารหัสที่เป็นไปได้ โดยแผนภาพต้นไม้ย่อยที่อยู่ข้างกันจะต้องมีสีต่างกัน มิฉะนั้นแล้วจะสามารถลบเส้นเชื่อมเส้นใดเส้นหนึ่งจากสองเส้นนั้นออกได้โดยที่ไม่มีผลกระทบใดๆ กับการแก้ปัญหการเข้ารหัส ซึ่งจะขัดแย้งกับความเป็นจริงที่ว่าเครือข่ายคือ 2-minimal ■

ทฤษฎีบทเสริม 2 : ถ้ากราฟต้นไม้ย่อยของกราฟ H สามารถระบายสีได้ด้วย $q + 1$ สีแล้วจะมีวิธีการเข้ารหัสบนฟิลต์จำกัด F_q (เมื่อ q เป็นจำนวนเฉพาะ)

พิสูจน์ : สำหรับสีจำนวน $q + 1$ สีใดๆ ซึ่งแต่ละสีนั้นสอดคล้องกับเวกเตอร์เข้ารหัสจาก $\{(0, 1), (1, 0), (1, 1 = \alpha^0), (1, \alpha), \dots, (1, \alpha^{q-2})\}$ เมื่อ α คือองค์ประกอบพื้นฐานในฟิลต์จำกัด F_q สังเกตว่าเวกเตอร์ 2 เวกเตอร์ใดๆ จากเซตนี้เป็นอิสระเชิงเส้นต่อกัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อมีสมมติฐานว่าเครือข่ายมัลติกราฟที่หวัข้อนี้เป็นแบบไม่เป็นวงกลม (acyclic) และอาจกำหนดเวกเตอร์เข้ารหัสให้แต่ละแผนภาพต้นไม้ย่อยในการเรียงเรียงลำดับแบบทอพอโลยี ซึ่ง ณ ช่วงเวลาของการกำหนดเวกเตอร์เข้ารหัสดังกล่าวสำหรับแผนภาพต้นไม้ย่อยที่มีโหนดรากที่ v นั้นทุกเส้นเชื่อมต่อกับโหนด v จะได้รับการกำหนดเวกเตอร์เข้ารหัสทั้งหมด

อ้างอิงจากจำนวนสีของ H ที่เป็นไปได้คือ $q + 1$ สี สามารถกำหนดแต่ละแผนภาพต้นไม้ย่อยด้วยเวกเตอร์เข้ารหัสซึ่งสอดคล้องกับจำนวนสีของ H แล้ว รหัสดังกล่าวนี้มีความเป็นไปได้เนื่องจากแต่ละแผนภาพต้นไม้ย่อยมีรากอยู่ที่โหนดแหล่งกำเนิดหรือโหนดที่มีดีกรีเข้าเท่ากับ 2 สำหรับกรณีที่สอง โหนดรากจะปรากฏได้ในทั้งสองแผนภาพต้นไม้ย่อยที่อยู่ติดกันใน H ดังนั้นเวกเตอร์เข้ารหัสของเส้นเชื่อมที่เข้ามาจึงมีความเป็นอิสระเชิงเส้นต่อกัน ดังนั้นเวกเตอร์เข้ารหัสจึงสามารถสร้างได้โดยการรวมกันเชิงเส้นของเวกเตอร์จากเส้นเชื่อมที่เชื่อมต่อเข้ามา ■

2.3.3.4 ข้อความคาดการณ์แบบ NC-Minor และความเท่ากันกับข้อความคาดการณ์แบบ Hadwiger

จากข้อความคาดการณ์แบบ NC-Minor ในหัวข้อ 2.3.3.2 แสดงให้เห็นว่าข้อความคาดการณ์นี้เกือบจะมีความเท่าเทียมกับข้อความคาดการณ์แบบ Hadwiger ในหัวข้อ 2.3.3.1 โดยใช้เทคนิคของการกระจายการไหลแบบมัลติกราฟในหัวข้อ 2.3.3.3 จากการเท่ากันนี้แสดงให้เห็นว่าข้อความคาดการณ์แบบ NC-Minor นั้นมีความถูกต้อง ในแง่ของความเป็นอิสระและสามารถใช้งานได้อย่างกว้างขวาง โดยมีบทพิสูจน์ที่น่าสนใจแสดงให้เห็นถึงความเพียงพอต่อขนาดพิดในกราฟไมเนอร์ต้องห้ามขนาดเล็ก (small minor forbidden) ซึ่งกราฟต้องห้าม (Forbidden graphs) นั้นก็คือคุณสมบัติกราฟที่ได้จากกระบวนการในรูป 2.13 ซึ่งแฝงอยู่ในกราฟ G นั่นเอง ในบางบทพิสูจน์นั้นได้สรุปผลที่ได้จากการพิสูจน์งานที่เกี่ยวข้องกับการเข้ารหัสเครือข่ายและงานวิจัยบางส่วนได้รับการพิสูจน์ขึ้นใหม่ ซึ่งในหัวข้อนี้จะระบุเฉพาะเงื่อนไขที่เพียงพอสำหรับข้อความคาดการณ์แบบ NC-Minor ที่ทำให้มีความเท่าเทียมกันกับข้อความคาดการณ์ Hadwiger โดยจะพิจารณาเฉพาะ กรณีที่ q เป็นจำนวนเฉพาะก่อน ซึ่งโดยทั่วไปแล้วค่าของ q จะมีคุณลักษณะพิเศษดังเช่นรูปที่ 2.14

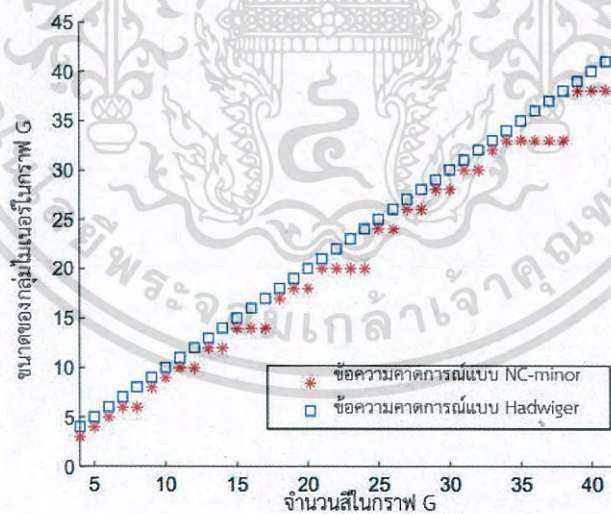
ทฤษฎีบท 1 สำหรับกราฟ H ง่าย ๆ จะมีเครือข่าย 2-minimal ที่ซึ่ง H เป็นแผนภาพต้นไม้ย่อยของกราฟ

พิสูจน์ : สำหรับแต่ละโหนดใน H สามารถสร้างโหนดส่งผ่าน เพื่อเชื่อมต่อกับแหล่งข้อมูล ได้โดยตรง สำหรับทุกเส้นเชื่อมใน H สามารถสร้างผู้รับซึ่งเชื่อมต่อกับหนดส่งผ่าน 2 ตัวซึ่งสอดคล้องกับ 2 โหนดที่ติดกันใน H ■

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทฤษฎีบท 2 (ข้อความคาดการณ์แบบ NC-Minor \Rightarrow ข้อความคาดการณ์แบบ Hadwiger ที่มีข้อบกพร่อง) หากการเข้ารหัสบนฟิลด์จำกัด F_q นั้นเพียงพอสำหรับเครือข่ายที่ปราศจากไมเนอร์ K_{q+2} เสมอแล้วทุกกราฟที่ระบายสีได้ $q + 2$ สีจะมีไมเนอร์ K_{q+1}

พิสูจน์ : จากทฤษฎีบทที่ 1 สำหรับกราฟ H ใดๆ ซึ่งเป็นกราฟที่มีได้ $q + 2$ สีนั้น สามารถสร้างเครือข่าย 2-minimal G และมี H เป็นกราฟต้นไม้ย่อยและสามารถอ้างได้ว่า G จะต้องไมเนอร์ K_{q+2} เพราะว่า ถ้าหาก G เป็นเครือข่ายที่ปราศจากไมเนอร์ K_{q+2} การเข้ารหัสบนฟิลด์ F_q จะเพียงพอด้วยข้อความคาดการณ์แบบ NC-Minor จากทฤษฎีบทเสริม 1 H เป็นกราฟที่สามารถระบายสีได้ $(q + 1)$ สีซึ่งขัดแย้งกับความเป็นจริงที่ว่าจำนวนสีที่สามารถมีได้คือ $q + 2$ ดังนั้น G จะประกอบด้วยไมเนอร์ K_{q+2} เพื่อที่จะให้การพิสูจน์สมบูรณ์จะแสดงให้เห็นว่า H ประกอบด้วยไมเนอร์ K_{q+2} เท่านั้น และกำหนดให้ G' แทนกราฟย่อยของ G ซึ่งสามารถลดรูปไปสู่ K_{q+2} เมื่อระบุให้แต่ละผู้รับมีดีกรีเข้าเท่ากับ 2 ดังนั้นในลำดับของการลดรูปจาก G' ไปสู่ K_{q+1} สำหรับทุกผู้รับใน G' ที่อย่างน้อยหนึ่งในสองของเส้นเชื่อมที่อยู่ติดกันถูกลดรูป โดยจะเห็นว่าหลังจากการลดรูปของเส้นเชื่อมหนึ่งที่ติดกันสำหรับผู้รับใน G' กราฟที่ถูกลดรูปนั้นยังคงเหมือนกับ H บวกกับโหนดที่แหล่งข้อมูลที่เชื่อมต่อเข้ากับแต่ละโหนดใน H ขณะที่แหล่งกำเนิดจะปรากฏอย่างมากในหนึ่งองค์ประกอบของการลดรูปกราฟ สามารถสรุปได้ว่า H มีกราฟไมเนอร์ K_{q+1} ■



รูปที่ 2.14 ข้อความคาดการณ์แบบ NC-Minor

เมื่อเปรียบเทียบกับข้อความคาดการณ์แบบ Hadwiger [22]

ทฤษฎีบทต่อไปนี้จะแสดงความสัมพันธ์ของกราฟไมเนอร์ของเครือข่ายมัลติคาสต์กับไมเนอร์ของกราฟต้นไม้อย่างซึ่งจะมีบทบาทสำคัญต่อไปในการพิสูจน์อื่นๆ

ทฤษฎีบท 3 : (ข้อความคาดการณ์แบบ Hadwiger \Rightarrow ข้อความคาดการณ์แบบ NC-Minor) หากทุกกราฟที่มี $q + 2$ สีประกอบด้วยกราฟไมเนอร์ K_{q+2} แล้วการเข้ารหัสบนฟิลด์จำกัด F_q นั้นเพียงพอสำหรับเครือข่ายที่ปราศจากกราฟไมเนอร์ K_{q+2}

พิสูจน์ : กำหนดให้ G เป็นเครือข่ายมัลติคาสต์ซึ่งปราศจากกราฟไมเนอร์ K_{q+2} หากกราฟต้นไม้อยู่ของ G คือ H มีกราฟไมเนอร์ K_{q+2} เป็นองค์ประกอบเช่นเดียวกับกับกราฟ G ดังนั้น H จะไม่มีไมเนอร์ K_{q+2} จากข้อความคาดการณ์แบบ Hadwiger จำนวนสีของ H จะต้องมีจำนวนน้อยกว่า $q + 2$ ดังนั้น H สามารถระบายสีได้ด้วยจำนวน $q + 1$ สีและจากทฤษฎีบทเสริมที่ 2 ทำให้เข้ารหัสบนฟิลด์ F_q ได้ ■

บทพิสูจน์ 1 : ในเครือข่ายซึ่งปราศจากกราฟไมเนอร์ K_q ขนาดของฟิลด์ที่เล็กที่สุดที่ต้องการสำหรับการมัลติคาสต์ที่มีสองการไหลของข้อมูล 2 ทางจะถูกจำกัดด้วยขอบเขตบนคือ $O(q \log q)$

พิสูจน์ : งานวิจัยที่เกี่ยวกับข้อความคาดการณ์แบบ Hadwiger แสดงให้เห็นว่ากราฟที่ปราศจากกราฟไมเนอร์ K_q สามารถถูกระบายสีได้จำนวน $O(q \log q)$ สี [24] โดยทฤษฎีที่ 3 จะเห็นว่ากราฟต้นไม้อยู่ H นั้นปราศจากไมเนอร์ K_q ด้วย ดังนั้น H สามารถถูกระบายสีได้จำนวน $O(q \log q)$ สี จากบทแทรก 2 ขนาดของฟิลด์ที่ต้องการต่ำที่สุดจะเป็นลำดับของ $O(q \log q)$ ■

บทพิสูจน์ 2 : (ข้อความคาดการณ์แบบ NC-Minor เป็นจริงสำหรับ $q = 2, 3, 4$) การเข้ารหัสบนฟิลด์ F_2, F_3, F_4 นั้นเพียงพอสำหรับเครือข่ายที่ปราศจากกราฟไมเนอร์ K_4 ปราศจากกราฟไมเนอร์ K_5 และปราศจากกราฟไมเนอร์ K_6 ตามลำดับ

พิสูจน์ : โดยบทพิสูจน์นี้จะเหมือนกันกับทฤษฎีบท 3 และความถูกต้องของข้อความคาดการณ์แบบ Hadwiger สำหรับค่า $q + 2 = 4, 5, 6$ [23] ■

2.4 รหัสน้ำพุ

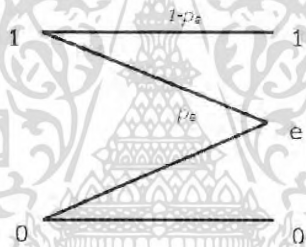
รหัสน้ำพุ (Fountain code) [26] เป็นรหัสที่มีความหนาแน่นในกราฟต่ำซึ่งเหมาะกับช่องสัญญาณที่มีความลบเลือน (Erasure Channel) เช่น ในเครือข่ายอินเทอร์เน็ต เมื่อจำนวนไฟล์ข้อมูลนั้นถูกส่งออกไปด้วยแพ็กเก็ตจำนวนมาก โดยข้อมูลที่ได้รับในช่องสัญญาณนี้แบ่งออกเป็น 2 ประเภทคือ 1. ข้อมูลที่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สามารถนำมาใช้ในการประมวลผลได้ และ 2. ข้อมูลที่ไม่สามารถนำมาประมวลผลใดๆ ได้ ซึ่งมาตรฐานการส่งข้อมูลทั่วไปนั้นผู้ส่งจะแบ่งไฟล์ข้อมูลเพื่อให้เหมาะสมกับขนาดของแพ็กเก็ต และส่งไปยังผู้รับ จนกว่าผู้รับจะได้รับข้อมูลที่ครบถ้วน ซึ่งในหัวข้อที่จะนำเสนอถัดไปนี้เป็นหนึ่งในแนวคิดของรหัสน้ำพุ ซึ่งก็คือ รหัสแอลทีที่ได้รับการพัฒนาขึ้นเพื่อช่วยลดอัตราการลบเลือนของข้อมูลที่เกิดขึ้นในช่องสัญญาณดังกล่าว และรหัสแอลทีเชิงระบบ (Systematic LT code) เพื่อปรับปรุงสมรรถนะของการเข้ารหัสและถอดรหัสรวมถึงอัตราการลบเลือนด้วย

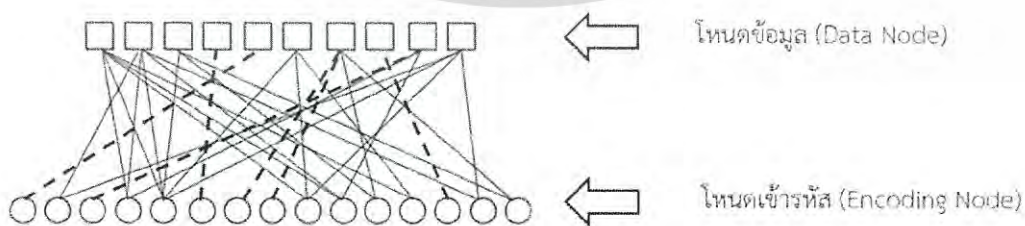
2.4.1 รหัสแอลที

รหัสแอลที (LT code) [11] เป็นรหัสที่ป้องกันการลบเลือนได้ และนำไปใช้ในช่องสัญญาณแบบไบนารีลบเลือนได้ (Binary erasure channel : BEC) ซึ่งความพิเศษของรหัสแอลที คือมีความยืดหยุ่นของอัตรารหัส (code rate) ซึ่งมีอัตรารหัสที่ต่ำ (rateless code) และมีค่าความน่าจะเป็นที่บิตหรือเฟรมนั้นถูกลบเลือนเท่ากับ p_e มีลักษณะดังรูปที่ 2.15 ซึ่งถือว่าข้อมูล e ที่ได้มานั้นไม่สามารถนำมาใช้ประโยชน์ได้



รูปที่ 2.15 ช่องสัญญาณลบเลือนแบบไบนารี (Binary Erasure Channel : BEC)

โดยกำหนดให้โหนดข้อมูล (Data node) แทนข้อมูลที่ต้องการจะนำไปเข้ารหัสและโหนดเข้ารหัส (Encoding node) แทนข้อมูลที่ได้รับการเข้ารหัสแล้ว ในการเข้ารหัสโดยอาศัยความสัมพันธ์ระหว่างโหนดทั้งสองแบบด้วยกราฟไบพาร์ไทท์ (Bipartite graph) แสดงดังรูปที่ 2.16



รูปที่ 2.16 ความสัมพันธ์กราฟไบพาร์ไทท์ระหว่างโหนดข้อมูลและโหนดเข้ารหัส

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

นิยาม 4 กฎของการถอดรหัส: ถ้าหากมีอย่างน้อย 1 โหนดเข้ารหัสที่มีดีกรีเท่ากับ 1 ซึ่งโยงไปยังโหนดข้อมูลโหนด (k_i) โดโหนดหนึ่ง การถอดรหัสสามารถทำได้ทันที เนื่องจากโหนดเข้ารหัสนั้นเกิดจากการเอ็กซ์คลูซีฟออร์กันระหว่างข้อมูลในโหนดข้อมูล และเมื่อมีเพียงโหนดข้อมูลหนึ่งโหนดเชื่อมโยงมาจึงเสมือนว่าโหนดเข้ารหัสนั้นได้คัดลอกข้อมูลจากโหนดข้อมูลมาโดยตรง

จากนิยามที่ 4 โหนดเข้ารหัสที่มีดีกรีเพียง 1 นั้นจะเป็นการคัดลอกค่าจากโหนดข้อมูลมาโดยตรง และถ้าหากมีดีกรีมากกว่า 1 ขึ้นไปจะนำข้อมูลจากโหนดข้อมูลมาเอ็กซ์คลูซีฟออร์ก่อนจะนำไปเก็บค่าในโหนดเข้ารหัส โดยที่จำนวนของโหนดเข้ารหัสนั้นสามารถสร้างได้จากข้อมูลที่มีจำกัด นอกจากนี้ยังสามารถสร้างในขณะที่ส่งข้อมูลได้อีกด้วยและในการถอดรหัสก็สามารถทำได้ด้วยกระบวนการเดียวกัน โดยการใช้การเอ็กซ์คลูซีฟออร์เพื่อนำข้อมูลของโหนดข้อมูลกลับมาในผู้รับ การสร้างรหัสแอลทีนั้นเริ่มต้นจากการสร้างฟังก์ชันการกระจายข้อมูลแบบโรบัสต์โซลิตอน (Robust soliton distribution : RSD) ซึ่งเป็นการพัฒนามาจากการกระจายข้อมูลแบบโซลิตอน (Soliton distribution : SD) ซึ่งเป็นรูปแบบการกระจายตัวของฟังก์ชันความหนาแน่นของความน่าจะเป็น (Probability Density Function : PDF) ซึ่งใน [11] ได้พิสูจน์แล้วว่าไม่สามารถนำมาใช้จริงได้ในเชิงปฏิบัติเนื่องจากจำนวนดีกรี 1 ที่ได้นั้นมีจำนวนน้อยเกินไป ซึ่งทำให้มีโอกาสในการถอดรหัสนั้นน้อยเมื่อนำมาประยุกต์ใช้ในช่องสัญญาณแบบไบนารีลบบเลื่อนได้ แต่อย่างไรก็ตามการสร้างการกระจายแบบโรบัสต์โซลิตอนจำเป็นต้องผ่านการสร้างการกระจายแบบโซลิตอน ซึ่งแสดงได้ดังสมการที่ (5) เมื่อกำหนดให้ k คือจำนวนของโหนดข้อมูลทั้งหมด และ $\rho(d)$ คือฟังก์ชันการกระจายตัวแบบโซลิตอน เมื่อ d คือดีกรีการกระจายข้อมูล

$$\rho(d) = \begin{cases} \frac{1}{k}, & d = 1 \\ \frac{1}{d(d-1)}, & d = 2, \dots, k \end{cases} \quad (5)$$

จากสมการที่ (5) นั้นความสัมพันธ์แบบโรบัสต์โซลิตอนสามารถหาได้จากสมการที่ (6) ซึ่งมีส่วนเพิ่มเติมคือ δ ซึ่งแทนค่าความน่าจะเป็นที่ฝั่งรับไม่สามารถถอดรหัสได้ ฟังก์ชัน $\tau(d)$ และในส่วน β และ R นั้นหาได้จากสมการที่ (6.1), (6.2) และ (6.3) ตามลำดับ

$$\mu(d) = \frac{\rho(d) + \tau(d)}{\beta} \quad (6)$$

$$\tau(d) = \begin{cases} \frac{R}{ik}, & i = (1, \frac{k}{R} - 1) \\ \frac{R}{k} \ln \frac{R}{\delta}, & i = \frac{k}{R} \\ 0, & i = (\frac{k}{R} + 1, k) \end{cases} \quad (6.1)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$\beta = \sum_{d=1}^k \rho(d) + \tau(d) \quad (6.2)$$

$$R = c \ln \frac{k}{\delta} \sqrt{k} \quad (6.3)$$

โดยที่ R คือค่าที่ช่วยให้เพิ่มจำนวนดีกรี 1 ในการกระจายแบบโรบัสโซลิตอน และ c คือค่าจำนวนจริงที่เหมาะสม โดยที่ $c > 0$ และผลลัพธ์ที่ได้จากสมการที่ (5) และ (6) นั้นคือเวกเตอร์ที่มีขนาดเท่ากับ k ซึ่งเป็นขนาดเดียวกับจำนวนของโหนดข้อมูล

ตัวอย่างต่อไปนี้เป็นวิธีการสร้างรหัสแอลทีด้วยค่า $k = 10$ โดยเริ่มจากการแทนค่าในสมการที่ (5) เพื่อให้ได้ $\rho(\cdot)$ ซึ่งผลลัพธ์จะอยู่ในรูปของเวกเตอร์ของความน่าจะเป็นขนาดเท่ากับ $[1 \times 10]$

$$\rho = [0.1000 \quad 0.5000 \quad 0.1667 \quad 0.0833 \quad 0.0500 \quad 0.0333 \quad 0.0238 \quad 0.0179 \quad 0.0139 \quad 0.0111]$$

จากนั้นหาเวกเตอร์ของความน่าจะเป็น $\mu(\cdot)$ จากสมการที่ (6), (6.1), (6.2) และ (6.3) โดยสมมติค่า c ที่เหมาะสมคือ 1 และ $\delta = 0.8$ โดยการหาค่า c ที่เหมาะสมนั้นจะกล่าวอีกครั้งในบทที่ 4 ซึ่งผลลัพธ์จะอยู่ในรูปของเวกเตอร์ของความน่าจะเป็นขนาดเท่ากับ $[1 \times 10]$ เช่นเดียวกัน

$$\mu = [0.2609 \quad 0.6130 \quad 0.0525 \quad 0.0263 \quad 0.0158 \quad 0.0105 \quad 0.0075 \quad 0.0056 \quad 0.0044 \quad 0.0035]$$

ในการแปลงจากฟังก์ชันความหนาแน่นของความน่าจะเป็นทั้ง $\rho(\cdot)$ และ $\mu(\cdot)$ ให้กลับไปอยู่ในรูปของข้อมูลดิบ (raw data) โดยผลลัพธ์ที่ได้จะเรียกว่า เวกเตอร์ดีกรี (vector of degree) ดังรูปที่ 2.17

```
ideal_degVector =
  2   2   6   1   2   2  10   9   7   2

robust_degVector =
  2   2   1   2   2   1   2   1   3   2
```

รูปที่ 2.17 เวกเตอร์ดีกรีแบบสุ่มเมื่อ $k = 10$ และ $f = 1$

2.4.2 การเข้ารหัสแอลที

วิธีการดังต่อไปนี้เป็นวิธีการเข้ารหัสแอลทีด้วยเวกเตอร์ดีกรีที่ได้จากฟังก์ชันการกระจายแบบโรบัสโซลิตอนคือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1. ลำดับสมาชิกในเวกเตอร์ดิกิริลำดับที่ 1 จนถึง k นั้นเชื่อมโยงกับลำดับของโหนดเข้ารหัสโดยตรง ซึ่งหมายความว่าแต่ละโหนดเข้ารหัสใดๆ k_i จะมีค่าดิกิริเท่ากับ v_i เมื่อ v_i คือค่าลำดับที่ i^{th} ในเวกเตอร์ดิกิริโดย $i \in \{1, k\}$

2. ให้แต่ละโหนดข้อมูล k_i เลือกโหนดเข้ารหัสแบบสุ่ม ตามจำนวนดิกิริที่โหนดนั้นมีอยู่ด้วยความน่าจะเป็นแบบยูนิฟอร์ม (uniform) ซึ่งผลที่ได้จากกระบวนการนี้ จะได้ความสัมพันธ์ในรูปแบบกราฟไอบาร์ไทท์ดังรูปที่ 2.16 นอกจากนี้ยังสามารถเขียนความสัมพันธ์กราฟไอบาร์ไทท์ให้อยู่ในรูปของความสัมพันธ์เชิงเมทริกซ์ได้อีกด้วย ซึ่งจะเรียกเมทริกซ์ที่ได้นี้ว่า เมทริกซ์กำเนิด (generator matrix) G ซึ่งมีขนาด $[k \times N]$ ดังรูปที่ 2.18

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

รูปที่ 2.18 เมทริกซ์กำเนิดของรหัสแอลที

สำหรับการเข้ารหัสแอลทีนั้น สามารถทำได้โดยกำหนดให้เวกเตอร์ D_t ซึ่งมีขนาด $[1 \times k]$ หรือ $[1 \times 10]$ ซึ่งเป็นการนำแต่ละบิตในเวกเตอร์แทน 1 โหนดข้อมูล และนำไปคูณกับเมทริกซ์ต้นกำเนิดในรูปที่ 2.18 ซึ่งมีขนาด $[10 \times 15]$ ผลลัพธ์ที่ได้นั้นจะได้ เวกเตอร์ของคำรหัส E ขนาด $[1 \times N]$ ซึ่งสามารถเขียนได้ดังสมการที่ (7)

$$E = D_t \times G \quad (7)$$

การเข้ารหัสแอลทีนั้นสามารถสร้างได้ทันทีในขณะที่กำลังโอนถ่ายข้อมูล โดยเปลี่ยนมุมมองจากเดิมที่สนใจโหนด k_i เป็นโหนดเข้ารหัส N_j โดยที่ $j \in \{0, N\}$ นั้นจะเข้ารหัสตามจำนวนดิกิริที่มี ซึ่งก็คือก่อนที่ผู้ส่งจะส่งข้อมูลเข้ารหัสนั้นโหนดเข้ารหัสจะได้เมทริกซ์กำเนิดเป็นตัวอ้างอิงว่าจะต้องนำโหนดข้อมูลโหนดใดมาเอ็กซ์คลูซีฟออร์

2.4.3 การถอดรหัสแอลที

ในส่วนของ การถอดรหัสนั้น โหนดผู้รับจะนำโหนดเข้ารหัสที่ได้รับมาจากช่องสัญญาณมาพิจารณาว่า เกิดจากการนำแพ็กเก็ตซึ่งแทนด้วยโหนดข้อมูลใดบ้างมาเอ็กซ์คลูซีฟออ์กัน ซึ่งการเข้ามาของข้อมูลแต่ละครั้ง โหนดผู้ส่งจะต้องตรวจสอบดูแพ็กเก็ตก่อนหน้าที่ได้รับมาทั้งหมด ว่าสามารถนำมาสร้างผลรวมเชิงเส้นที่สามารถนำมาถอดรหัสในแพ็กเก็ตปัจจุบันได้หรือไม่ โดยสามารถจำแนกการถอดรหัสได้เป็น 2 รูปแบบ คือ

1. การถอดรหัสทันที การถอดรหัสแบบนี้ทำได้ทันทีเมื่อผู้รับรับโหนดเข้ารหัสที่มีดีกรีเท่ากับ 1

2. การถอดรหัสโดยตรง จะเป็นการนำโหนดข้อมูลที่ทราบอยู่แล้วภายในหน่วยความจำสำรอง ซึ่งถ้าหากโหนดเข้ารหัสที่เพิ่งได้รับเข้ามานั้นเกิดจากการเอ็กซ์คลูซีฟออ์กันระหว่างข้อมูลในโหนดข้อมูลจำนวน l โหนด การที่จะสามารถถอดรหัสได้นั้นจะต้องรู้อย่างน้อยจำนวน $l - 1$ โหนดข้อมูล เป็นต้น

2.4.4 รหัสแอลทีเชิงระบบ

การรหัสแอลทีในหัวข้อ 2.4.1 ที่ซึ่งถูกออกแบบโดย Luby [11] รหัสดังกล่าวมีส่วนช่วยเพิ่มประสิทธิภาพการส่งข้อมูลในช่องสัญญาณแบบไบนารีลบเลือนได้ ซึ่งในงานวิจัย [27] ได้นำเสนอรหัสแอลทีเชิงระบบ (Systematic LT code) ซึ่งจะมีการเพิ่มกระบวนการขจัดแบบเกาส์เซียน (Gaussian elimination) หลังจากที่ได้เมทริกซ์ต้นกำเนิดในขั้นตอนการสร้างรหัสแอลที ซึ่งได้มีการศึกษาในงานวิจัย [28] โดยวัดประสิทธิภาพของความสัมพันธ์เชิงระบบ (systematic connection) ที่อยู่ในเมทริกซ์กำเนิดนั้นโดยวัดเป็นอัตราส่วนร้อยละของความสัมพันธ์เชิงระบบซึ่งได้แก่ 10%, 30%, 50% และ 100% โดยในรูปที่ 2.19 แสดงให้เห็นถึงความสัมพันธ์เชิงระบบในเมทริกซ์ต้นกำเนิดของรหัสแอลที

งานวิจัย [28] ได้ทดสอบประสิทธิภาพของรหัสแอลทีเชิงระบบด้วยการถอดรหัสแบบซอฟต์แวร์ ซึ่งในรูปที่ 2.20 แสดงให้เห็นถึงประสิทธิภาพของรหัสแอลทีเชิงระบบด้วยความสัมพันธ์เชิงระบบที่มีค่าแตกต่างกันนำมาเปรียบเทียบกับรหัสแอลที ผลลัพธ์ที่ได้นั้นชี้ให้เห็นว่ารหัสแอลทีให้ผลลัพธ์ที่แย่ที่สุดในทุกค่าอัตรารหัส ในขณะที่รหัสแอลทีเชิงระบบที่มีความสัมพันธ์เชิงระบบ 100% ให้ผลลัพธ์ที่ดีที่สุดเมื่อเทียบกับรหัสแอลทีเชิงระบบที่มีความสัมพันธ์เชิงระบบที่เหลือ

บทที่ 3

รหัสเครือข่ายแบบปรับตัวได้

ในหัวข้อนี้ได้นำเสนอรหัสเครือข่ายแบบปรับตัวได้ (The Adaptive Network Coding-Routing Based on Graph for Multicast Networks : ANCR) โดยพิจารณาจากเครือข่ายมัลติคาสต์รูปผีเสื้อ (Butterfly Network) ซึ่งมีคุณสมบัติ 2-minimal และยังได้นำเสนออัลกอริธึมการเข้ารหัสเครือข่ายแบบปรับตัวได้ โดยที่โหนดส่งผ่านทั้งหมดสามารถที่จะส่งข้อมูลโดยใช้เส้นทางที่ดีที่สุดโดยโพรโตคอล AODV และ AODV-BR ประกอบกับการคำนวณเชิงพีชคณิตก่อนที่จะกำหนดเส้นทาง นอกจากนี้หัวข้อนี้ยังได้รับแรงบันดาลใจมาจาก [23] ในหัวข้อ 2.3.3 ซึ่งได้นำเสนอและพิสูจน์ว่ากราฟไมเนอร์ K_4 ในทุกทอพอโลยีนั้นช่วยลดเวลาในการคำนวณรหัสเครือข่าย อีกทั้งยังนำเสนอความสัมพันธ์ระหว่างรหัสพีชคณิตและเครือข่ายโทโลยี และยังกล่าวว่ารหัสเครือข่ายสามารถนำมาประยุกต์ในเราต์ติ้งหลายรูปแบบโดยเฉพาะถ้าหากทอพอโลยีนั้นมีคุณลักษณะกราฟไมเนอร์ K_4 ดังนั้นการสร้างอัลกอริธึมรหัสเครือข่ายแบบปรับตัวได้มีแรงบันดาลใจเพื่อจะเพิ่มความจุให้กับเครือข่ายโดยเพิ่มค่าทรูพุตและยังลดระยะเวลาในการส่งในแต่ละโหนดส่งผ่านด้วย

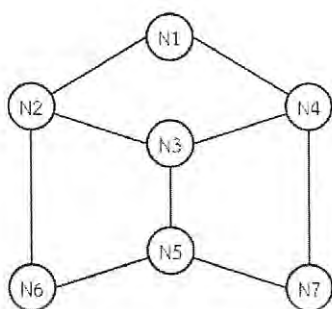
3.1 อัลกอริธึมที่ได้นำเสนอ

ในหัวข้อนี้อัลกอริธึมในการเข้ารหัสเครือข่ายแบบปรับตัวได้ ซึ่งในหัวข้อ 3.1.1 แสดงให้เห็นลักษณะของทอพอโลยีที่ได้นำใช้ในการพิจารณา และพัฒนารหัสเครือข่ายแบบปรับตัวได้ และแสดงถึงกรรมวิธีการเลือกแพ็กเกตนำมาเข้ารหัสก่อนที่จะส่งออกไปยังช่องสัญญาณในหัวข้อที่ 3.1.2

3.1.1 แบบจำลองเครือข่าย

เริ่มจากพิจารณากราฟเครือข่ายรูปผีเสื้อ $G(V, E)$ ซึ่งเป็นเครือข่ายแบบ 2-minimal เมื่อ V และ E เป็นจุดยอด (Vertex) และเส้นเชื่อม (Edge) ตามลำดับ ดังที่แสดงในรูปที่ 3.1 ทอพอโลยีเครือข่ายนี้ประกอบด้วยโหนดผู้ส่ง 1 โหนด (N_1), โหนดส่งผ่าน 4 โหนด (N_2, N_3, N_4, N_5), และโหนดผู้รับ 2 โหนด (N_6, N_7) ในการจำลองการส่งข้อมูลในเครือข่ายนั้นได้มีพื้นฐานมาจากเครือข่ายไร้สายที่ใช้เราต์ติ้งโพรโตคอล AODV [13] ซึ่งมีความอิสระในการหาเส้นทาง ด้วยการแพร่กระจายแพ็กเกตร้องขอเส้นทาง RREQ ไปในทุกทิศทางและเพื่อหาเส้นทางที่ดีที่สุดที่โหนดผู้ส่งซึ่งเป็นโหนดแหล่งกำเนิดจะประเมินจากแพ็กเกตตอบกลับ RREP ที่ส่งกลับมาเร็วที่สุด และเพื่อที่จะได้จำนวนเส้นทางมากกว่าหนึ่งเส้นทางเพื่อที่จะได้นำมาคำนวณ ได้ใช้เทคนิคและแนวคิดของ AODV-BR [14] ที่มีการค้นหาเส้นทางสำรองในกรณีที่เส้นทางหลักไม่สามารถใช้งานได้ ซึ่งเส้นทางสำรองเหล่านั้นนั้นจะต้องมีความแตกต่างเชิงเวลาของแพ็กเกตตอบกลับที่ใกล้เคียงกับเส้นทางหลัก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.1 เครือข่ายรูปสี่เหลี่ยม

ในส่วนของอัลกอริธึมที่นำเสนอในหัวข้อนี้ จะแตกต่างจากอัลกอริธึมโคปใน [6] ซึ่งเป็นการใช้การใช้โหมดเฝ้าสังเกต ในการแอบได้ยินข้อมูลที่ส่งกันภายในเครือข่าย และแต่ละโหนดจำเป็นต้องรอรับรายงานการรับรู้ จากโหนดข้างเคียงเพื่อทำการตัดสินใจในการเข้ารหัสด้วยการเอ็ชคูลูซีฟออร์ โดย ANCR จะให้โหนดแหล่งกำเนิดนั้นทำหน้าที่รวบรวมความรู้ของเส้นทางที่ได้รับจากโพรโตคอล AODV และ AODV-BR ประกอบกับทอพอโลยีที่โหนดนั้นได้เรียนรู้มา และนำความรู้เหล่านั้นมาพิจารณาด้วยทางทฤษฎีกราฟ เพื่อตัดสินใจว่าแพ็กเก็ตไหนควรจะนำไปเข้ารหัสเครือข่าย ณ ที่โหนดส่งผ่านโหนดใด

3.1.2 อัลกอริธึม ANCR

อัลกอริธึม ANCR นั้นประกอบด้วย 2 ขั้นตอน ซึ่งในรูปที่ 3.2 แสดงให้เห็นถึงการทำงานในภาพรวม โดยขั้นตอนแรกจะเป็นการเลือกแพ็กเก็ตที่จะส่งออกไปจากหน่วยความจำสำรองว่ามีความเกี่ยวเนื่องกันหรือไม่ และขั้นตอนที่สองจะเป็นการคำนวณด้วยการใช้เทคนิคการหาค่าของกราฟเพื่อหาคุณสมบัติที่แฝงอยู่ในทอพอโลยี

ขั้นตอน I : การเลือกแพ็กเก็ต ขั้นตอนนี้ได้อธิบายอัลกอริธึมการเลือกแพ็กเก็ตเพื่อนำมาสร้างรหัสเครือข่ายก่อนที่จะส่งออกไปอย่างเหมาะสม โดยหลังจากที่โหนดผู้ส่งเสร็จสิ้นกระบวนการส่งแพ็กเก็ตร้องขอเส้นทาง และแพ็กเก็ตตอบกลับ RREP จากนั้นเส้นทางหลัก (primary path) และเส้นทางสำรอง (secondary path) จะถูกสร้างขึ้นในทุกโหนดส่งผ่านซึ่งเชื่อมโยงถึงโหนดผู้ส่ง และโหนดผู้ส่งจะทำการหาเส้นทางจากแพ็กเก็ตอย่างน้อยสองแพ็กเก็ตในแถวเรียง (queue) ในหน่วยความจำสำรอง โดยกำหนดให้

P_m คือแพ็กเก็ตมัลติคาสต์ (Multicast packet)

P_u คือแพ็กเก็ตยูนิคาสต์ (Unicast packet)

d_{p_u} คือเซตของผู้รับของแพ็กเก็ตยูนิคาสต์

d_{p_m} คือเซตของผู้รับของแพ็กเก็ตมัลติคาสต์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ซึ่งแพ็กเกตที่นำมาพิจารณานั้นสามารถเป็นได้ทั้ง P_m หรือ P_u และเงื่อนไขในการสร้างรหัสเครือข่ายแบบปรับตัวได้นั้น คือ หนึ่งในสองแพ็กเกตนั้นจะต้องเป็น P_m ที่สามารถระบุถึงกลุ่มผู้รับได้โดยอัตโนมัติ โดยเงื่อนไขที่สอดคล้องสำหรับการพิจารณาแพ็กเกตจำนวน 2 แพ็กเกตนั้นสามารถเป็นได้ 2 กรณี คือ

1. สองแพ็กเกตที่กำลังพิจารณาอยู่คือ P_m และ P_u ความสัมพันธ์ระหว่าง d_{pu} และ d_{pm} จะต้องอยู่ในรูป $d_{pu} \in d_{pm}$
2. สองแพ็กเกตนั้นเป็น P_m ทั้งคู่ และกำหนดให้ d_{pm}^1 และ d_{pm}^2 เป็นเซตผู้รับที่ 1 และเซตผู้รับที่ 2 ของทั้งสองแพ็กเกต

เมื่ออยู่ในสองเงื่อนไขดังกล่าวแล้ว โหนดผู้ส่งจะใช้ข้อมูลดังกล่าวในการหัตตัวของกราฟเพื่อหาลักษณะที่แฝงตัวอยู่ในทอพอโลยี

ขั้นตอนที่ II : การหัตตัวของกราฟ หลังจากสองแพ็กเกตได้รับเลือกจากขั้นตอนแรกจากนั้น โหนดผู้ส่งจะใช้เทคนิคการหัตตัวของกราฟ (contraction) โดยกำหนดให้

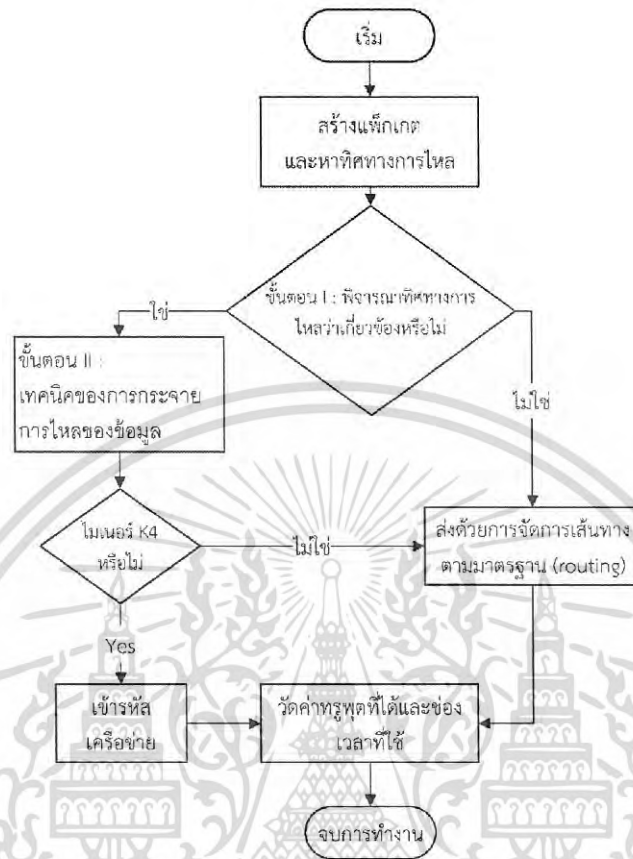
F_i คือ เซตของทิศทางกราฟไหลของข้อมูลของแพ็กเกต i^{th}

f_{pi}, f_{si} คือเส้นทางหลักและเส้นทางสำรองตามลำดับของแพ็กเกต i^{th}

ภายใน F_i ประกอบไปด้วยทิศทางกราฟไหลที่เป็นไปได้ทั้งหมดจากโหนดแหล่งกำเนิดถึงโหนดผู้รับในแพ็กเกตที่ i^{th} ซึ่งรับรู้มาจากการบวนการเรียนรู้ด้วยโพรโตคอล AODV และ AODV-BR สำหรับโครงข่ายสื่อสารไร้สายเคลื่อนที่

ถัดมาพิจารณา $f_{pi}, f_{si} \in F_i$ และ $f_{pj}, f_{sj} \in F_j$ ของแพ็กเกตที่ i^{th} และ j^{th} ตามลำดับ โดยจะต้องมีความสัมพันธ์ซึ่งกันและกัน โดยถ้าหากแพ็กเกต i^{th} และ j^{th} นั้นอยู่ในกราฟไมเนอร์เดียวกัน โหนดผู้ส่งจะดำเนินการตามอัลกอริธึมในรูปที่ 3.3 ซึ่งเป็นการหัตตัวของกราฟ เมื่อกระบวนการดังกล่าวเสร็จสิ้น ผลลัพธ์ที่ได้จากอัลกอริธึมดังกล่าวจะอยู่ในรูปของกราฟไมเนอร์ โดยภายในประกอบด้วยกลุ่มของโหนดที่จะนำมาเข้ารหัสเครือข่ายด้วยการเอ็ชคูลูซีฟออร์ โดยผลลัพธ์ที่โหนดผู้ส่งนั้นสนใจคือ กราฟไมเนอร์ที่มีลักษณะเป็น K_4 ตามที่ได้กล่าวในหัวข้อ 2.3.3 ผลที่ตามมาได้คือแพ็กเกตเข้ารหัสจะถูกสร้างในโหนดที่อยู่ในไมเนอร์เดียวกันก่อนที่จะส่งผ่านดังที่แสดงในรูปที่ 3.4

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

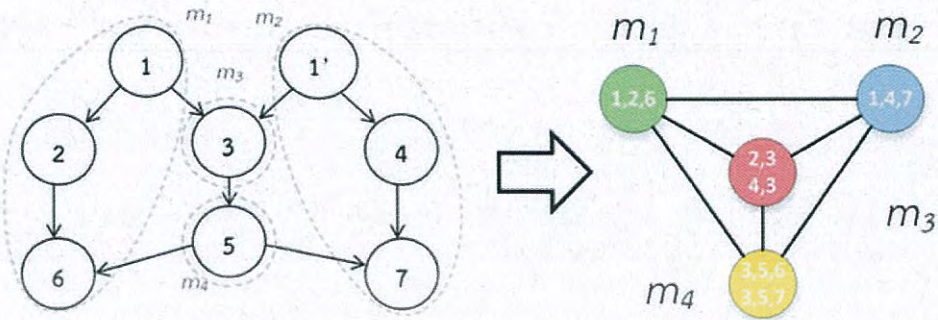


รูปที่ 3.2 อัลกอริธึมของรหัสเครือข่ายแบบปรับตัวได้

function DECOMPOSITION (*Graph G, Flow F*)
 minor $m = 1$; Graph node G_i ;
 for each $f_i \in F$ do
 for each pair $f_i(a, b) \in f_i$ do
 Let O_b be out degree of b .
 for each $O_b \in deg^-(b)$ do
 if O_b is receiver then
 minor(m) = [a, b, O_b] ; $m++$;
 if $deg^+(O_b) = 1$ then
 minor(m) = [a, b] ; $m++$;
 else
 minor(m) = [a, b, O_b] ; $m++$;
 return minor m ;

รูปที่ 3.3 อัลกอริธึมการหาค่าของกราฟ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.4 กราฟไมเนอร์ K_4 ของเครือข่ายรูปผีเสื้อที่ได้จากกระบวนการหดตัวของกราฟ

3.2 แบบจำลองช่องสัญญาณและการเข้ารหัสเครือข่าย

หัวข้อนี้ได้จำลองระบบการส่งผ่านลำดับชั้นการส่งข้อมูลทางกายภาพ ผ่านช่องสัญญาณรบกวนเกาส์เซียนขาวบวก (Additive white Gaussian noises : AWGN) และกำหนดให้รับสัญญาณที่รับได้คือ $y = x + n$ เมื่อ x คือข้อมูลที่ถูส่ง, n คือ สัญญาณรบกวน AWGN $n \sim N(0, \sigma)$ และ y คือข้อมูลที่ปรากฏอยู่ในฝั่งผู้รับ ถ้าหากโหนดผู้รับได้รับแพ็กเกตเอ็กซ์คลูซีฟออร์ ก็จะเริ่มทำการถอดรหัสด้วยอีกแพ็กเกตหนึ่งที่ถูกส่งผ่านมาจากเส้นทางอื่น

อย่างไรก็ตาม ถ้าหากแพ็กเกตนั้นไม่พบในแถวเรียงลำดับ (queue) ผู้รับจะรอดด้วยระยะเวลา t_d และเมื่อกระบวนการ รหัสเครือข่ายแบบปรับตัวได้เสร็จสิ้น โหนดผู้ส่ง S_1 จะเพิ่มข้อมูลลงในฟิลด์ "เซตที่อยู่ของโหนดที่จะทำการเข้ารหัส (coding node addr set)" อัดโนมิตีอีกทั้งยังเพิ่มฟิลด์ "หมายเลขของแพ็กเกตที่นำมาเข้ารหัส (encode packet ID set)" เพื่อระบุว่าแพ็กเกตใดบ้างที่นำมาเข้ารหัสด้วยการเอ็กซ์คลูซีฟออร์ ซึ่งฟิลด์ของแพ็กเกตเอ็กซ์คลูซีฟออร์นั้นแสดงดังรูป 3.5 และตารางที่ 3.1 แสดงการเปรียบเทียบแพ็กเกตมาตรฐานและแพ็กเกตเอ็กซ์คลูซีฟออร์ เพื่อที่จะได้นำแพ็กเกตมาถอดรหัสได้อย่างถูกต้อง โดยการถอดรหัสนั้นใช้สมการที่ (8)

$$d_a = d_x \oplus (d_{n1} \oplus d_{n2} \oplus \dots) \tag{8}$$

เมื่อ d_a คือข้อมูลที่แท้จริงที่โหนดผู้รับต้องการ, d_x คือแพ็กเกตเอ็กซ์คลูซีฟออร์ และ d_n คือข้อมูลของแพ็กเกตที่ถูกส่งโดยโหนดผู้ส่งซึ่งใช้กราฟไมเนอร์ในการกำหนด

หมายเลข แพ็กเกต	โหนดผู้ส่ง	กลุ่มผู้รับ	หมายเลข โหนดเข้ารหัส	หมายเลข แพ็กเกตที่ เข้ารหัส	ข้อมูลที่ได้รับ การเข้ารหัส
--------------------	------------	-------------	-------------------------	-----------------------------------	--------------------------------

รูปที่ 3.5 ฟิลด์ของแพ็กเกตเอ็กซ์คลูซีฟออร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไมอนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

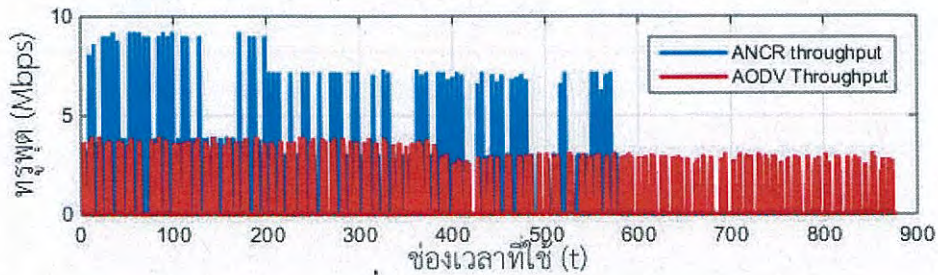
ตารางที่ 3.1 เปรียบเทียบฟิลด์กับแพ็กเก็ตมาตรฐาน

แพ็กเก็ตมาตรฐาน	แพ็กเก็ตเอ็กซ์คลูซีฟออร์
หมายเลขแพ็กเก็ต	หมายเลขแพ็กเก็ต
หมายเลขโหนดผู้ส่ง	หมายเลขโหนดผู้ส่ง
หมายเลขของกลุ่มผู้รับ	หมายเลขของกลุ่มผู้รับ
-	หมายเลขของโหนดเข้ารหัส
-	หมายเลขแพ็กเก็ตที่นำมาเข้ารหัส
ข้อมูล	ข้อมูลที่ได้จากการเอ็กซ์คลูซีฟออร์

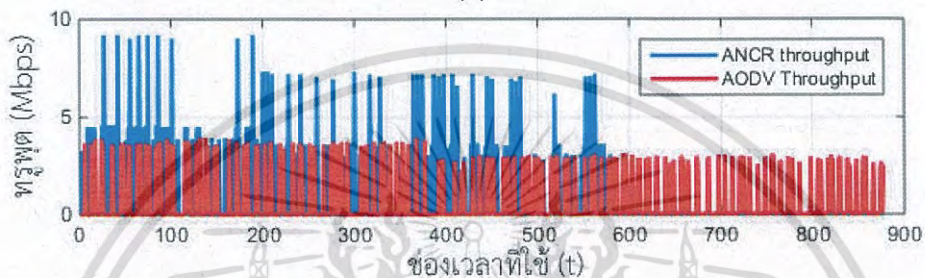
3.3 ผลการทดลอง

เพื่อที่จะศึกษารูปแบบของระบบที่ใช้การเข้ารหัสเครือข่ายร่วมกับเร้าตั้งโพรโตคอล เปรียบเทียบกับระบบที่มีเร้าตั้งโพรโตคอลเพียงอย่างเดียว และเพื่อวัดประสิทธิภาพของอัลกอริธึมรหัสเครือข่ายแบบปรับตัวได้ (ANCR) ผู้วิจัยได้ทำการประยุกต์ใช้อัลกอริธึมนี้กับเครือข่ายรูปผีเสื้อดังที่แสดงในรูปที่ 3.1 อัลกอริธึมรหัสเครือข่ายแบบปรับตัวได้ (ANCR) นั้นถูกนำมาใช้เพื่อช่วยตัดสินใจในเงื่อนไขที่เหมาะสมโดยสามารถเลือกว่าแพ็กเก็ตข้อมูลแบบใดที่ควรนำมาเข้ารหัสเครือข่าย ซึ่งจะพิจารณาแพ็กเก็ตก่อนที่จะทำการส่งข้อมูลออกไปจำนวน 2 แพ็กเก็ต หรือมากกว่าที่อยู่บนหัวแถวของแถวเรียงลำดับ และถ้าหากไม่สามารถเข้ารหัสด้วยรหัสเครือข่ายได้ด้วยเงื่อนไขตามผังงานที่ 3.2 โหนดผู้ส่งจะใช้เร้าตั้งโพรโตคอลตามมาตรฐาน ซึ่งได้แก่ AODV และ AODV-BR [13] [14] ในการส่งข้อมูลเพื่อป้องกันการเกิดการเข้ารหัสที่สูญเปล่าในแง่ของจำนวนครั้งการส่งที่เทียบเท่ากับการส่งข้อมูลตามมาตรฐานซึ่งเสียทรัพยากรในการเข้ารหัสและถอดรหัส โดยอัลกอริธึมในหัวข้อนี้มีเป้าหมายเพื่อที่จะเพิ่มค่าทราฟฟิคในโหนดผู้รับซึ่งส่งผลต่อค่าทราฟฟิคโดยรวมของระบบ และยังลดระยะเวลาการส่งข้อมูลซึ่งถูกลดประสิทธิภาพด้วยเส้นทางคอคขวดด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ก)



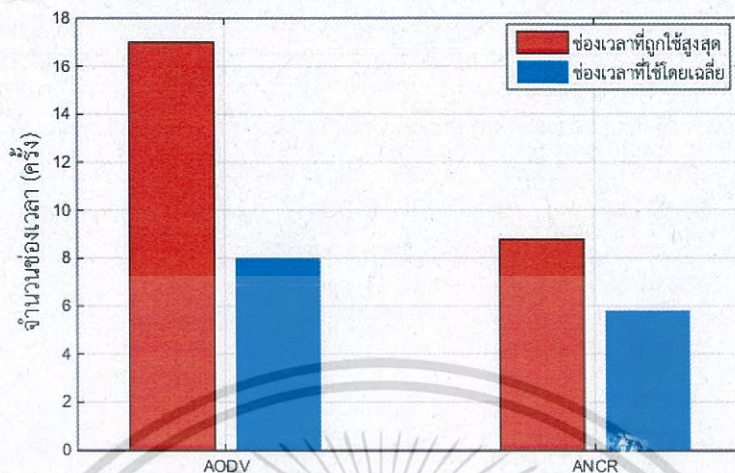
(ข)

รูปที่ 3.6 (ก) ค่าทราฟฟิคที่วัดได้ที่โหนดหมายเลข 3 (โหนดคอขวด) และ (ข) โหนดหมายเลข 7 (โหนดผู้รับ)

ผลจากการจำลองแสดงให้เห็นดังรูปที่ 3.6 ซึ่งแสดงถึงค่าทราฟฟิคที่วัดได้ที่โหนดหมายเลข 3 (โหนดคอขวด) และโหนดหมายเลข 7 (โหนดผู้รับ) ด้วยความเปลี่ยนแปลงในแง่ของการใช้ช่วงเวลาระหว่างระบบที่ใช้การเข้ารหัสเครือข่ายร่วมกับเราต์ติ้งโพรโทคอล และระบบที่ใช้เราต์ติ้งโพรโทคอลเพียงอย่างเดียว ผลลัพธ์ที่ได้ชี้ให้เห็นว่าเครือข่ายที่มีการใช้การเข้ารหัสเครือข่ายร่วมกับเราต์ติ้งโพรโทคอลให้ค่าทราฟฟิคมากกว่า ไม่เฉพาะโหนดหมายเลข 3 ซึ่งเป็นโหนดคอขวดที่มีการเพิ่มขึ้นของค่าทราฟฟิค แต่ยังเพิ่มขึ้นในโหนดผู้รับ (หมายเลข 6 และ 7) อย่างเห็นได้ชัดอีกด้วย ซึ่งในตารางที่ 3.2 ได้แสดงถึงการเพิ่มขึ้นของค่าทราฟฟิคดังกล่าว โหนดส่งผ่านโดยส่วนใหญ่ได้รับประโยชน์จากอัลกอริธึม ANCR เนื่องจากโหนดเหล่านี้ได้มีค่าทราฟฟิคที่เพิ่มขึ้นอย่างเห็นได้ชัดเมื่อเทียบกับการส่งในรูปแบบทั่วไป ซึ่งตารางที่ 3.2 แสดงให้เห็นอย่างชัดเจนว่าโหนดหมายเลข 3 มีค่า ทราฟฟิคเพิ่มมาประมาณ 36% และโหนดผู้รับค่าทราฟฟิคเพิ่มขึ้นประมาณ 45%

นอกจากนี้ ในงานวิจัยได้กำหนดให้มีการวัดค่า การเข้าใช้งานช่องสัญญาณ (Time slot) ของระบบเครือข่ายซึ่งการเข้าใช้งานช่องสัญญาณ 1 ช่องนั้น หมายถึงเริ่มตั้งแต่การส่งแพ็กเก็ตร้องขอช่องสัญญาณเพื่อส่ง (Request to Send : RTS) และเคลียร์ช่องสัญญาณเพื่อส่ง (Clear to Send : CTS) ตลอดจนการส่งข้อมูลจนแล้วเสร็จในช่วงการเชื่อมต่อ (session) นั้นๆ และการส่งแพ็กเก็ตตอบกลับว่าได้รับข้อมูลครบถ้วน ซึ่งรหัสเครือข่ายแบบปรับตัวได้ (ANCR) นี้มีส่วนช่วยลดการเข้าใช้ช่องสัญญาณดังกล่าว ด้วยการส่งข้อมูลที่ถูกรวมไว้ด้วยการเอ็กคลูซีฟออร์ จะเสมือนว่าเป็นการส่งข้อมูล 2 ในช่วงการเชื่อมต่อในครั้งเดียว โดยที่ระบบนั้น จะไม่นับการได้ข้อมูลจากการแอบได้ยิน (Overhearing)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไมอนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.7 จำนวนการเข้าใช้ช่องสัญญาณโดยมากที่สุดและโดยเฉลี่ยของระบบเครือข่ายที่ใช้อัลกอริธึม ANCR เปรียบเทียบกับการใช้เร้าติงโพรโตคอลแบบปกติ (AODV)

ตารางที่ 3.2 ค่าทรูพุดที่วัดได้

โหนด	AODV หรือ AODV-BR	ANCR	ค่าทรูพุดที่เพิ่มขึ้น
	ค่าทรูพุดเฉลี่ย (Mbps)	ค่าทรูพุดเฉลี่ย (Mbps)	
โหนดผู้ส่ง 1	0.00	0.00	0.00 %
โหนดส่งผ่าน 2	6.99	6.92	-01.03 %
โหนดคอขวด 3	7.40	11.64	36.42 %
โหนดส่งผ่าน 4	6.27	7.17	12.48 %
โหนดส่งผ่าน 5	5.56	6.60	15.79 %
โหนดผู้รับ 6	6.62	13.12	47.54 %
โหนดผู้รับ 7	6.51	12.84	49.27 %

ผลลัพธ์ในรูปที่ 3.7 ได้แสดงให้เห็นว่าระบบที่มีอัลกอริธึมรหัสเครือข่ายแบบปรับตัวได้อยู่ด้วยนั้นทำให้ระบบใช้จำนวนช่องสัญญาณน้อยกว่าการใช้งานเร้าติงโพรโตคอลเพียงอย่างเดียวทั้งแบบค่าการใช้ช่องสัญญาณมากที่สุดและค่าเฉลี่ยซึ่งเป็นจำนวนที่ใช้เพื่อส่งจำนวนแพ็กเกตในปริมาณเท่ากัน ในรูปที่ 3.6 และ 3.7 แสดงให้เห็นถึงรายละเอียดของการทดสอบว่าอัลกอริธึม ANCR ใช้จำนวนการส่งข้อมูลประมาณ 550 ครั้งเพื่อที่จะส่งแพ็กเกตให้สำเร็จ และในขณะที่ระบบที่มีเพียงโพรโตคอลโครงข่ายสื่อสารไร้สายเคลื่อนที่เฉพาะกิจ (AODV) เพียงอย่างเดียวใช้ประมาณ 850 ครั้งซึ่งแสดงให้เห็นว่าอัลกอริธึมดังกล่าวนี้ช่วยลดจำนวนการส่งข้อมูลได้ประมาณ 35%

3.4 การวิเคราะห์ผลการทดลองและอัลกอริธึม

ในหัวข้อนี้ได้วิเคราะห์ถึงความต้องการของระบบเครือข่าย เพื่อที่จะทำให้อัลกอริธึมรหัสเครือข่ายแบบปรับตัวนั้นได้มีประสิทธิภาพสูงที่สุด โดยเริ่มจากการกำหนดตัวแปรต่างๆดังนี้

p คือ จำนวนเส้นทางที่เป็นไปได้ทั้งหมดจากโหนดผู้ส่งไปจนถึงโหนดผู้รับ

h คือ จำนวนฮอปที่สั้นที่สุดในเครือข่ายจากโหนดผู้ส่งไปจนถึงโหนดผู้รับ

f คือ จำนวนทิศทางไหลของข้อมูลที่สามารถส่งได้ในขณะนั้น

T คือ ค่าทรูพุดโดยรวมของทั้งระบบในหน่วยบิตต่อวินาที (bps)

ซึ่งได้กำหนดฟังก์ชันจุดประสงค์ (Objective function) ในสมการที่ (9) โดยกำหนด τ , δ คือ เวลาที่ใช้ในการส่งแพ็กเกตจำนวนหนึ่งในหน่วยวินาที (sec) และจำนวนข้อมูลทั้งหมดที่ใช้ส่งในหน่วยบิต (bit) ตามลำดับ ซึ่งสามารถหาได้จากสมการที่ (9.1) และ (9.2)

$$\text{Maximize : } T = \frac{\delta \text{ (bits)}}{\tau \text{ (sec)}} \quad (9)$$

$$\tau = \sum_{i=1}^h t_i \quad (9.1)$$

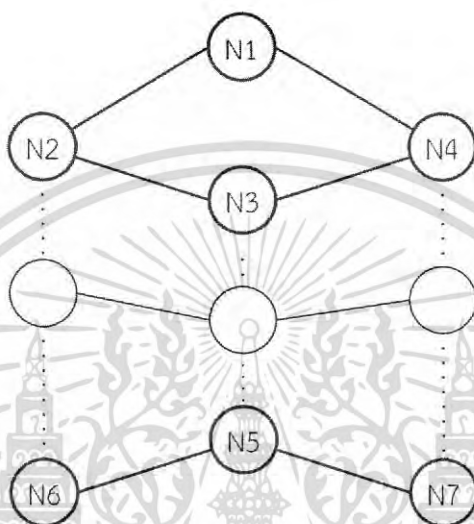
$$\delta = \sum_{j=1}^m d_j \quad (9.2)$$

จากสมการที่ (9.1) และ (9.2) เมื่อ t_i คือเวลาในการเดินทางของแพ็กเกตใดๆ ผ่านฮอปที่ i^{th} ซึ่ง h คือจำนวนฮอปทั้งหมดที่จะต้องส่งข้อมูลไปจนถึงผู้รับ และ d_j คือขนาดของแพ็กเกตที่ j^{th} ใดๆ ที่โหนดผู้ส่งนั้นนำมาพิจารณาในขั้นตอน i : การเลือกแพ็กเกต นอกจากนี้ผลลัพธ์ที่ได้จากการทดลองได้ชี้ให้เห็นว่ารหัสเครือข่ายแบบปรับตัวได้นั้นสามารถช่วยลดจำนวนการใช้ช่องเวลาได้ ดังที่แสดงให้เห็นไปแล้วในรูปที่ 3.6 และ 3.7 ซึ่งถัดมาผู้วิจัยได้กำหนดให้ ค่า δ ในสมการที่ (9) เกิดจากผลรวมของแพ็กเกตจำนวน m และ d_j ในสมการที่ (9.2) มีค่าคงที่

ในการเปรียบเทียบประสิทธิภาพ ผู้วิจัยได้ทดสอบกับเครือข่ายที่มีลักษณะ n -minimal โดยที่ค่า $n = 1, 2, 3, 4$ ซึ่งในรายละเอียด เครือข่ายแบบ 1-minimal คือเครือข่ายที่แต่ละโหนดนั้นสามารถส่งข้อมูลได้โดยตรงภายใน 1 ฮอป ซึ่งรหัสเครือข่ายแบบปรับตัวได้นั้นไม่สามารถเพิ่มประสิทธิภาพของระบบได้อีก ในขณะที่เครือข่ายแบบ 2-minimal คือเครือข่ายที่มีลักษณะดังเช่นเครือข่ายรูปผีเสื้อในรูปที่ 3.1 ซึ่งในส่วนเครือข่ายแบบ 2-minimal และ n -minimal นั้นสามารถอธิบายได้ดังสมการที่ (10) โดยเป็นการเพิ่มโหนดจำนวน 3 โหนด ระหว่างกลุ่มโหนด N2, N3, N4 และกลุ่มโหนด N5, N6, N7 เพื่อให้ได้เครือข่ายที่มีลักษณะ n -minimal และสอดคล้องกับเครือข่ายเดิมที่ใช้วัดประสิทธิภาพก่อนหน้านี้ใน

รูปที่ 3.1 โดยกำหนดให้ v คือจำนวนโหนดทั้งหมดในเครือข่ายแบบ n -minimal และ n คือขนาดของเครือข่ายแบบ n -minimal

$$v = 3n + 1 \quad (10)$$



รูปที่ 3.8 ลักษณะเครือข่ายแบบ n -minimal ที่สอดคล้องกับสมการที่ (10)

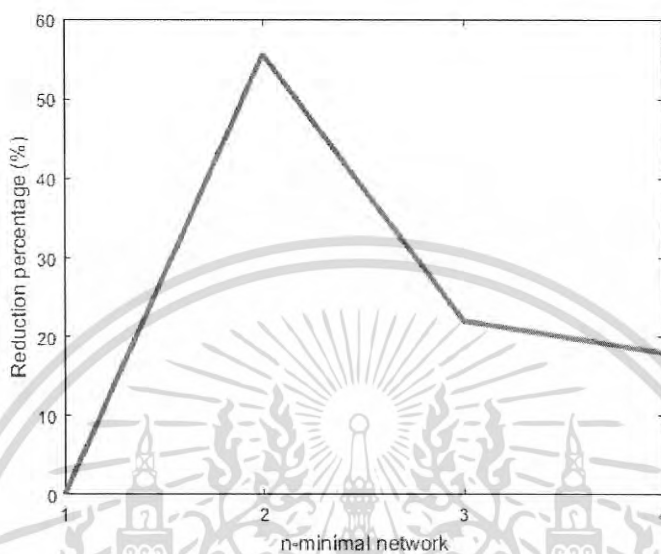
สำหรับเกณฑ์ในการพิจารณาถึงประสิทธิภาพของรหัสเครือข่ายแบบปรับตัวได้ เริ่มจากการกำหนดแพ็กเก็ตที่จะนำมาใช้พิจารณาจำนวน 2 แพ็กเก็ต และพิจารณาถึงจำนวนเส้นทางที่สามารถเพิ่มประสิทธิภาพด้วยรหัสเครือข่ายเชิงระบบ P_{ANCR} รวมถึงจำนวนเส้นทางที่เป็นไปได้ทั้งหมด p จากโหนดผู้ของทั้ง 2 แพ็กเก็ตนี้ ผลลัพธ์นั้นสามารถคำนวณได้จากสมการที่ (11)

$$\varepsilon = \frac{p}{P_{ANCR}} \times 100\% \quad (11)$$

จากสมการที่ (11) ค่า ε คือ ค่าอัตราส่วนร้อยละของการลดการใช้ช่องเวลาในเครือข่ายแบบ n -minimal ที่รหัสเครือข่ายสามารถปรับปรุงประสิทธิภาพได้ ซึ่งผลลัพธ์นั้นสามารถแสดงได้ดังรูปที่ 3.9 ซึ่งพิจารณาจากสมการที่ (9) โดยสามารถจำแนกถึงความแตกต่างของระบบที่มีและไม่มีรหัสเครือข่ายแบบปรับตัวได้ ด้วยการพิจารณาได้จากตัวแปร τ ซึ่งก็คือเวลารวมในการส่ง 2 แพ็กเก็ตที่โหนดผู้ส่งนั้นกำลังพิจารณา พร้อมทั้งยังกำหนดให้เวลา t ของการส่งข้อมูลจากฮอปหนึ่งไปยังอีกฮอปหนึ่งมีค่าเท่ากัน ดังนั้นการวัดประสิทธิภาพของระบบที่ใช้รหัสเครือข่ายแบบปรับตัวได้สามารถวัดได้จากจำนวนการใช้ช่องเวลาที่ใช้ในการส่ง 2 แพ็กเก็ต ผลที่ได้นั้นแสดงให้เห็นว่าในเครือข่าย 2-minimal ให้ความสามารถใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การลดการใช้ช่องเวลาได้มากที่สุดถึง 55% ซึ่งสอดคล้องกับข้อพิสูจน์ในทางทฤษฎี ในขณะที่เครือข่าย 3-minimal และ 4-minimal มีการลดลงดังกล่าวเพียง 22% และ 18% ตามลำดับ



รูปที่ 3.9 ความสามารถในการลดการใช้งานช่องเวลาของเครือข่ายแบบ n -minimal

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

การพัฒนารหัสแอลทีเชิงระบบ

ในการส่งข้อมูลของเครือข่ายมัลติคาสต์หรือแม้แต่เครือข่ายเซ็นเซอร์ไปยังโหนดผู้รับหลายโหนด ปัญหาคอขวดยังคงเป็นปัญหาสำคัญซึ่งเป็นสาเหตุให้เกิดการตกหล่นของแพ็กเก็ตในขณะที่ยังส่ง และเกิดเวลาแฝงที่ใช้ในการส่งข้อมูลเพิ่มขึ้น ซึ่งหัวข้อที่ 2.2 ได้นำเสนอรหัสเครือข่ายซึ่งได้ช่วยเพิ่มค่าทูลูพุตให้แก่ระบบด้วยการพิจารณาแพ็กเก็ตที่ได้รับและสร้างแพ็กเก็ตใหม่ซึ่งเกิดจากเอ็กซ์คลูซีฟออร์กัันระหว่างข้อมูลในแพ็กเก็ตนั้นๆ โดยกระบวนการสร้างรหัสเครือข่ายนั้นยังขึ้นอยู่กับแพ็กเก็ตที่ตอบสนองจากโหนด โดยรอบอีกด้วย ถัดมาในบทที่ 3 ได้พิจารณาเครือข่ายมัลติคาสต์ที่มีลักษณะ 2-minimal และได้นำเสนอ รหัสเครือข่ายแบบปรับตัวได้หรืออัลกอริธึม ANCR เพื่อแก้ปัญหาคอขวดในเครือข่ายรูปผีเสื้อ ซึ่งขั้นตอนวิธีในบทที่ 3 นั้นใช้แพ็กเก็ตตอบสนองจากโหนดใกล้เคียงเช่นเดียวกับขั้นตอนวิธีโคป แต่อย่างไรก็ตามทั้งสองขั้นตอนวิธีดังกล่าวนี้ยังไม่เพียงพอที่จะทำงานได้อย่างเหมาะสมในเครือข่ายขนาดใหญ่ ซึ่งมีการส่งข้อมูลไกลเกินกว่า 2 ฮีอป

เมื่ออยู่ในเงื่อนไขที่เหมาะสม การส่งผ่านแพ็กเก็ตเอ็กซ์คลูซีฟออร์กัันไปยังกลุ่มของโหนดผู้รับผ่านช่องสัญญาณไบนารีลบบเลื่อนได้นั้น ยังมีข้อบกพร่องและยังลดประสิทธิภาพโดยรวมเมื่อยังพบแพ็กเก็ตลบเลื่อน (erased packet) อยู่ในลำดับชั้นของการส่งข้อมูลในลำดับที่สูงขึ้นไป ซึ่งทำให้โหนดผู้ส่งนั้นต้องเผชิญกับข้อความตอบกลับเชิงลบ (Negative Acknowledgement : NACK) จากโหนดผู้รับ และถ้าหากมีการร้องขอให้ส่งแพ็กเก็ตที่สูญหายไปยังโหนดผู้ส่งจะทำให้ระยะเวลาการส่งแพ็กเก็ตเหล่านั้นเพิ่มขึ้นเกือบสองเท่าตัว โดยปัญหานี้สามารถแก้ไขได้โดยประยุกต์การใช้รหัสเพื่อป้องกันการลบเลื่อนในฝั่งโหนดผู้ส่งด้วยรหัสแอลทีดังที่กล่าวมาแล้วในหัวข้อ 2.4.1 แต่รหัสดังกล่าวก็ยังไม่สามารถป้องกันการเกิดแพ็กเก็ตลบเลื่อนได้ทั้งหมด ทำให้เวลาแฝงจากการส่งข้อมูลนั้นยังคงอยู่ จึงต้องอาศัยกระบวนการการส่งข้อมูลซ้ำ (Retransmission) ด้วยโอกาสการแอบได้ยิน (Opportunistic Overhearing) ซึ่งช่วยลดภาระให้กับโหนดผู้ส่งและช่วยลดเวลาแฝงในการส่งจากโหนดดังกล่าวและจะกล่าวในหัวข้อ 4.2.1

ในบทนี้ได้นำเสนอการพัฒนารหัสแอลทีเชิงระบบเพื่อสร้างรหัสเครือข่ายเชิงระบบ สำหรับเครือข่ายขนาดใหญ่ซึ่งเป็นการพัฒนาต่อยอดมาจากแนวคิดการสร้างเมทริกซ์กำเนิดของรหัสแอลที และรหัสแอลทีเชิงระบบ (systematic LT code) นำมาผสมผสานกับรูปแบบกระบวนการส่งข้อมูลซ้ำ ซึ่งได้พัฒนาและปรับปรุงกระบวนการสร้างเมทริกซ์กำเนิดของรหัสเครือข่ายเชิงระบบรวมถึงกระบวนการส่งข้อมูลซ้ำซึ่งช่วยลดเวลาแฝงของการส่งข้อมูลซ้ำให้กับระบบโดยรวม ซึ่งมีความสามารถในการเพิ่มทูลูพุตอีกด้วย นอกจากนี้ยังได้วิเคราะห์ประสิทธิภาพของรหัสเครือข่ายเชิงระบบในแง่ของอัตราของเฟรมลบเลื่อนร่วม (mutual erased frame : MEF) ที่สามารถขจัดได้การประยุกต์รหัสเครือข่ายเชิงระบบนั้นทำให้โหนดผู้รับสามารถเชื่อถือโหนดข้างเคียงให้ทำการส่งแพ็กเก็ตที่สูญหายเหล่านั้นได้ทันทีโดยไม่ต้องรอจากโหนดผู้ส่งต้นทางซึ่งอยู่ห่างไกลออกไป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1 การออกแบบรหัสเครือข่ายเชิงระบบ

ในหัวข้อนี้จะกล่าวถึงการสร้างรหัสเครือข่ายเชิงระบบ (Systematic Network code) ซึ่งได้ปรับเปลี่ยนขั้นตอนการสร้างกราฟไปพาร์ไทท์และเมทริกซ์กำเนิดจากรหัสแอลที่ดั้งเดิม ก่อนที่จะนำไปสู่รูปแบบเชิงระบบโดยผ่านกระบวนการขจัดแบบเกาส์เซียน (Gaussian elimination) ซึ่งรหัสเครือข่ายเชิงระบบนั้นสามารถลดความซับซ้อนในการถอดรหัสเมื่อเทียบกับรหัสแอลที่

4.1.1 การเข้ารหัสเครือข่ายเชิงระบบ

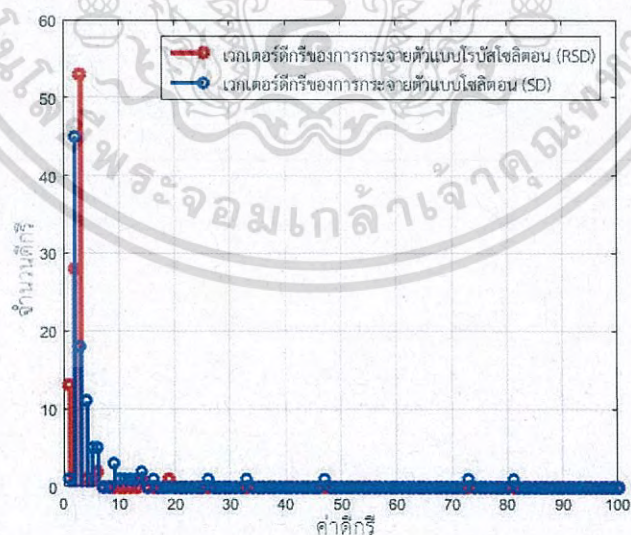
ขั้นตอนการเข้ารหัสเครือข่ายเชิงระบบ (Encoding) มีขั้นตอนดังต่อไปนี้

1. เริ่มจากการหาฟังก์ชันความหนาแน่นของความน่าจะเป็น (Probability Density Function : PDF) ของการกระจายตัวแบบโรบัสโซลิตอน $\mu(d)$ ในสมการที่ (5), (6) ตามลำดับซึ่งต้องกำหนดตัวแปรที่เกี่ยวข้อง ได้แก่ k, c, δ เพื่อที่จะได้เวกเตอร์ของความน่าจะเป็นที่มีขนาด $[1 \times k]$

เพื่อให้เห็นภาพที่ชัดเจนยิ่งขึ้น ผู้วิจัยได้ยกตัวอย่างสร้างเวกเตอร์ดีกรีของการกระจายตัวของ $\mu(d)$ ด้วยค่า $k = 100, c = 1$ และ $\delta = 0.8$ ซึ่งสามารถแสดงให้เห็นในรูปแบบของเลขจำนวนเต็ม และเปรียบเทียบกับลักษณะการกระจายตัวเมื่อเทียบกับกระจายตัวแบบโซลิตอน ดังรูปที่ 4.1

เวกเตอร์ดีกรีของการกระจายตัวแบบโรบัสโซลิตอน

$\mu(d) = [1 \ 1 \ 3 \ 3 \ 3 \ 3 \ 1 \ 3 \ 1 \ 2 \ 1 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 3 \ 3 \ 3 \ 2 \ 2 \ 1 \ 4 \ 3 \ 3 \ 2 \ 2 \ 3 \ 19 \ 2 \ 2 \ 3 \ 1 \ 3 \ 3 \ 14 \ 3 \ 3 \ 2 \ 3 \ 3 \ 3 \ 3 \ 2 \ 3 \ 3 \ 3 \ 2 \ 3 \ 3 \ 3 \ 3 \ 1 \ 1 \ 2 \ 2 \ 3 \ 6 \ 5 \ 3 \ 2 \ 3 \ 3 \ 3 \ 3 \ 1 \ 3 \ 3 \ 2 \ 1 \ 3 \ 2 \ 2 \ 3 \ 3 \ 3 \ 3 \ 2 \ 6 \ 3 \ 1 \ 3 \ 3 \ 1 \ 3 \ 2 \ 3 \ 3 \ 3 \ 2 \ 2]$



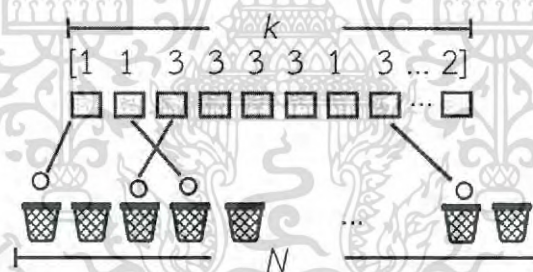
รูปที่ 4.1 การเปรียบเทียบระหว่างการกระจายตัวแบบโรบัสโซลิตอนและโซลิตอน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จากการเปรียบเทียบจะเห็นว่า เวกเตอร์ดีกรีของการกระจายตัวแบบโรบัสโซลิตอน $\mu(d)$ ประกอบด้วยค่าดีกรีเท่ากับ 1 จำนวนมากกว่า เวกเตอร์ดีกรีของการกระจายตัวแบบโซลิตอน $\rho(d)$ ซึ่งจะทำให้มีจำนวนค่าดีกรีที่สูงใน $\rho(d)$ โดยส่งผลให้เกิดความยากลำบากในการถอดรหัส และมีโอกาสที่จะถอดรหัสไม่ได้อีกด้วย ซึ่งผู้วิจัยจะกล่าวอีกครั้งในกระบวนการตรวจสอบเมทริกซ์กำเนิดในหัวข้อ 4.1.2

2. แปลงข้อมูลในรูปของเวกเตอร์ของความน่าจะเป็น จากข้อ 1. ให้อยู่ในรูปของเวกเตอร์ของค่าจำนวนเต็มโดยอาศัยการสุ่มแบบยูนิฟอร์ม (Uniform) ผลลัพธ์ที่ได้เป็นเวกเตอร์ขนาดเดียวกันกับเวกเตอร์ของความน่าจะเป็น ซึ่งจะเรียกว่า เวกเตอร์ดีกรี (vector of degree : V)

3. สร้างความสัมพันธ์ในรูปแบบของกราฟไบพาร์ไทท์ระหว่างโหนดข้อมูลและโหนดเข้ารหัส โดยการนำเวกเตอร์ดีกรี ผ่านกระบวนการที่เรียกว่า “กระบวนการสุ่มโยน (Random throw)” และสามารถสร้างเมทริกซ์ต้นกำเนิดในรูปแบบทั่วไป (Generator Matrix) โดยจะเริ่มจากค่าสมาชิกในเวกเตอร์ดีกรี v_i โดยที่ $v \in V$ และ $i \in \{1, k\}$ โดย v_i คือค่าที่ระบุจำนวนเส้นเชื่อมที่ออกจากโหนดข้อมูลไปยังโหนดเข้ารหัส จากนั้นแต่ละโหนดข้อมูลจะทำการสุ่มโหนดเข้ารหัสที่มีจำนวน N โหนด สามารถเปรียบเทียบได้โดยสมมติให้โหนดข้อมูลมีบอลอยู่จำนวน v_i โดยที่สุ่มโยนไปที่โหนดเข้ารหัสซึ่งแทนด้วยตะกร้า N_j ใดๆ เมื่อ $j \in \{1, N\}$ ดังรูปที่ 4.2 โดยใช้การสุ่มด้วยความน่าจะเป็นแบบยูนิฟอร์ม (Uniform)



รูปที่ 4.2 กระบวนการสุ่มโยนจากโหนดข้อมูลไปยังโหนดเข้ารหัส

เนื่องจากการสร้างความสัมพันธ์ลักษณะดังกล่าวเกิดจากสุ่มด้วยความน่าจะเป็นแบบยูนิฟอร์ม จะทำให้มีบางกรณีที่บางตะกร้าที่ไม่มีลูกบอลอยู่ ซึ่งหมายความว่าโหนดเข้ารหัสโหนดนั้นไม่มีข้อมูลจากโหนดข้อมูลใดมาเอ็กซ์คลูซีฟออร์ เท่ากับว่าเป็นการส่งข้อมูลว่างเปล่าผ่านช่องสัญญาณ ซึ่งในขั้นตอนการสร้างรหัสเครือข่ายต่อไปนี้เป็นจะช่วยลดข้อผิดพลาดดังกล่าวโดยใช้ขั้นตอนดังต่อไปนี้

โดยกำหนดให้

V คือ เวกเตอร์ดีกรีที่เชื่อมโยงกับโหนดข้อมูลแบบหนึ่งต่อหนึ่ง

B คือ เซตของโหนดเข้ารหัสซึ่งแทนด้วยตะกร้าที่ยังไม่ได้ถูกเลือก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เริ่มจาก

3.1 ให้โหนดข้อมูล v_i ที่มีจำนวนลูกบอลเท่ากับ 1 สุ่มเลือกตระกร้า b_j แบบสุ่มและไม่ซ้ำกันก่อน โดยที่ $b \in B$ และ $j \in \{1, N\}$ หลังเรียบร้อยแล้วให้นำตระกร้า b_j ที่ถูกเลือกออกจากเซต B

3.2 ทำข้อ 1. ซ้ำจนกว่าโหนดข้อมูล v_i ที่มีจำนวนลูกบอลเพียง 1 ลูกจะถูกพิจารณาจนหมด

3.3 พิจารณาเซต B โดยแยกเป็น 2 กรณี ว่าเป็นเซตว่างหรือไม่

3.3.1 ถ้าไม่เป็นเซตว่าง เริ่มจากสุ่มโหนดข้อมูล v_i ที่มีจำนวนลูกบอล > 1 ขึ้นมา และให้สุ่มโยนลูกบอลลงตระกร้าที่ลูก โดยระหว่างนั้นตรวจสอบเซต B ไปด้วยว่าเป็นเซตว่างหรือไม่

3.3.2 ถ้าเป็นเซตว่างให้สุ่มโยนลูกบอลอย่างอิสระ

ผลลัพธ์ที่ได้สามารถแสดงได้ในรูปแบบของกราฟไบนารีไทม์ในลักษณะเช่นเดียวกับรูปที่ 2.16 ซึ่งความแตกต่างของกราฟไบนารีไทม์ที่ได้ระหว่างรหัสเครือข่ายเชิงระบบนั้นมีระดับความสุ่มที่น้อยกว่ารหัสแอลที และสามารถนำมาเขียนในรูปแบบเมทริกซ์ต้นกำเนิดได้ดังรูปที่ 4.3

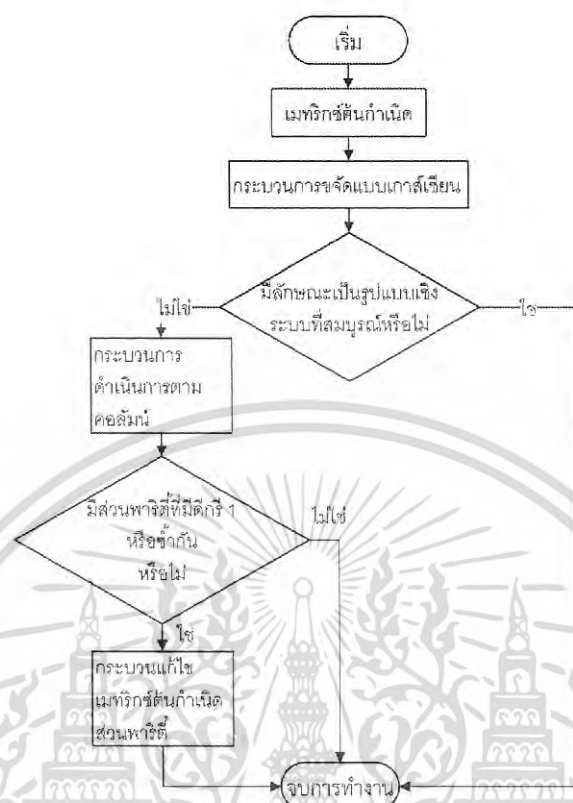
$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

รูปที่ 4.3 เมทริกซ์ต้นกำเนิดทั่วไปที่ผ่านกระบวนการสุ่มโยน (Random throw)

4. ขั้นตอนสุดท้ายเป็นการนำเมทริกซ์ต้นกำเนิดในรูปแบบทั่วไปจากรูปที่ 4.3 มาสร้างเป็นเมทริกซ์ต้นกำเนิดที่อยู่ในรูปแบบเชิงระบบ ซึ่งประกอบด้วยส่วนข้อมูล I และส่วนพาริตี P ในรูปของสมการที่ (12) โดยอาศัยกระบวนการสร้างเมทริกซ์ต้นกำเนิดเชิงระบบของรหัสเครือข่ายเชิงระบบในรูปที่ 4.4

$$G = [I | P] \quad (12)$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

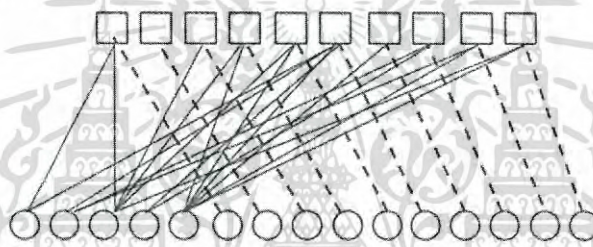


รูปที่ 4.4 กระบวนการสร้างเมทริกซ์ต้นกำเนิดเชิงระบบของรหัสเครือข่ายเชิงระบบ

การสร้างรูปแบบเชิงระบบที่ใช้กระบวนการจัดแบบเกาส์เซียน (Gaussian elimination) ที่ประกอบด้วยการดำเนินการตามแถว (Row Operation) เพียงอย่างเดียวนั้นไม่เพียงพอที่จะสร้างรูปแบบเชิงระบบที่สมบูรณ์ได้ดังสมการที่ (12) สำหรับการสร้างเมทริกซ์ต้นกำเนิดเชิงระบบในรหัสเครือข่ายเชิงระบบนั้น จะเพิ่มกระบวนการดำเนินการตามคอลัมน์ (Column Operation) และกระบวนการแก้ไขเมทริกซ์ต้นกำเนิดส่วนพหุคูณ โดยจะนำคอลัมน์ส่วนพหุคูณที่ซ้ำกันไม่ว่าจะเป็นส่วนข้อมูล I หรือส่วนพหุคูณ P กลับมาพิจารณาในมุมมองของกราฟไบนารีเททอีกครั้ง ซึ่งจะเป็นการลบเส้นเชื่อมทั้งหมดของโหนดเข้ารหัสที่พิจารณาอยู่และเริ่มต้นกระบวนการสุ่มโยน (Random throw) เฉพาะโหนดเข้ารหัสที่นำมาพิจารณา และสามารถแสดงผลลัพธ์สุดท้ายได้ดังรูปที่ 4.5 และ 4.6 ซึ่งปราศจากคอลัมน์ที่ซ้ำกัน และสามารถนำไปเข้ารหัสกับข้อมูลที่โหนดผู้ส่งได้จริงต่อไป

$$\left[\begin{array}{cccccccccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right]$$

รูปที่ 4.5 เมทริกซ์ต้นกำเนิดในรูปแบบเชิงระบบสำหรับรหัสเครือข่ายเชิงระบบ



รูปที่ 4.6 ความสัมพันธ์กราฟไบพาร์ไทท์เชิงระบบสำหรับรหัสเครือข่ายเชิงระบบ

4.1.2 กระบวนการตรวจสอบเมทริกซ์กำเนิด

อย่างไรก็ตามเพื่อยืนยันได้ว่าเมทริกซ์กำเนิดที่สร้างจากหัวข้อที่ผ่านมาสามารถนำไปใช้ได้จริงสำหรับการพิสูจน์ทราบหลังจากที่ได้ความสัมพันธ์ในรูปแบบเมทริกซ์กำเนิด G นั้น โหนดผู้ส่งจะต้องทดสอบการเข้ารหัสและถอดรหัสภายในหน่วยความจำภายในโดยไม่ต้องผ่านช่องสัญญาณใดๆ ก่อน เพื่อยืนยันว่าเมทริกซ์กำเนิด G ที่ได้มานั้นไม่มีข้อบกพร่องอันเกิดจากกระบวนการสร้างดังกล่าวมาแล้ว มีวิธีการที่เรียกว่ากระบวนการตรวจสอบเมทริกซ์กำเนิดซึ่งเริ่มจาก กำหนดเซตที่พิจารณาแต่ละโหนด รวมถึงเส้นเชื่อมในความสัมพันธ์แบบไบพาร์ไทท์กราฟซึ่งในหัวข้อนี้จะแสดงตัวอย่างการพิจารณาอย่างละเอียดโดยเริ่มจากตัวอย่างอย่างง่ายในรูปแบบกราฟไบพาร์ไทท์ในรูปที่ 4.6 เริ่มจากกำหนดให้

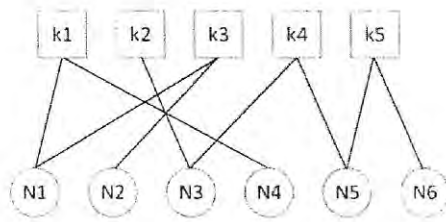
R = เซตของโหนดที่ได้รับการพิจารณาแล้ว (released encoding node set)

C_s = เซตครอบคลุม (covered set)

P = เซตของโหนดข้อมูลที่ได้รับการพิจารณาแล้ว (processed data node set)

R_p = เซตกระเพื่อม (ripple set)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.7 กราฟไบบิพาร์ไทท์ตัวอย่างในการพิจารณากระบวนการตรวจสอบเมทริกซ์กำเนิด

จากรูปที่ 4.7 สามารถพิจารณาใช้กราฟเพื่อสร้างรหัสเครือข่ายเชิงระบบได้ดังกระบวนการต่อไปนี้

1. พิจารณาโหนดเข้ารหัส N2, N4, N6 ซึ่งมีดีกรีเท่ากับ 1 และให้เซตของโหนดที่ได้รับการพิจารณาแล้ว มีสมาชิกเท่ากับโหนดเข้ารหัสดังกล่าว โดยโหนดเข้ารหัสทั้งสามนี้โยงไปยังโหนดข้อมูลคือ k1, k3, k5 และจากนั้นให้สมาชิกของเซตครอบคลุมและเซตกระเพื่อมเท่ากับโหนดข้อมูลดังกล่าว พร้อมทั้งให้เซตของโหนดข้อมูลที่ได้รับการพิจารณาแล้วเท่ากับเซตว่าง ซึ่งเซตต่างๆจะมีสมาชิกดังนี้

$$R = \{N2, N4, N6\}$$

$$C_s = \{k1, k3, k5\}$$

$$P = \{\}$$

$$R_p = \{k1, k3, k5\}$$

1.1 จากนั้นให้เริ่มพิจารณาทีละโหนดเข้ารหัสที่อยู่ในเซตกระเพื่อม พิจารณาโหนดข้อมูล k1 ซึ่งมีเส้นเชื่อมไปยังโหนดเข้ารหัส N1, N4 จากนั้นให้เพิ่มโหนดเข้ารหัสดังกล่าวลงในเซตของโหนดเข้ารหัสที่ได้รับการพิจารณาแล้ว พร้อมทั้งปรับเซตของโหนดข้อมูลที่ได้รับการพิจารณาแล้วให้เป็นปัจจุบันและลบเส้นเชื่อมระหว่างโหนดข้อมูล k1 และโหนดเข้ารหัส N1, N4 ซึ่งเซตต่างๆ จะมีสมาชิกดังนี้

$$R = \{N2, N4, N6, N1\}$$

$$C_s = \{k1, k3, k5\}$$

$$P = \{k1\}$$

$$R_p = \{k3, k5\}$$

1.2 พิจารณาโหนดข้อมูล k3 แบบเดียวกันกับข้อ 1.1

ซึ่งเซตต่างๆ จะมีสมาชิกดังนี้

$$R = \{N2, N4, N6, N1\}$$

$$C_s = \{k1, k3, k5\}$$

$$P = \{k1, k3\}$$

$$R_p = \{k5\}$$

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.3 พิจารณาโหนดข้อมูล k5 ซึ่งในขั้นตอนนี้หลังจากที่ลบเส้นเชื่อมระหว่างโหนดข้อมูล k5 กับโหนดเข้ารหัส N5, N6 ออกไปทำให้เส้นเชื่อมที่เชื่อมมายังโหนดเข้ารหัส N5 เหลือเพียงเส้นเดียวซึ่งก็คือดีกรีเท่ากับ 1 ให้เพิ่มโหนดเข้ารหัส N5 เข้าไปในเซตของโหนดเข้ารหัสที่ได้รับการพิจารณาแล้ว และเพิ่มโหนดข้อมูล k4 เข้าไปในเซตครอบคลุมและเซตกระเพื่อม ซึ่งเซตต่างๆ จะมีสมาชิกดังนี้

$$R = \{N2, N4, N6, N1, N5\}$$

$$C_s = \{k1, k3, k5, k4\}$$

$$P = \{k1, k3, k5\}$$

$$R_p = \{k4\}$$

1.4 พิจารณาโหนดข้อมูล k4 ซึ่งเซตต่างๆ จะมีสมาชิกดังนี้

$$R = \{N2, N4, N6, N1, N5, N3\}$$

$$C_s = \{k1, k3, k5, k4, k2\}$$

$$P = \{k1, k3, k5, k4\}$$

$$R_p = \{k2\}$$

1.5 พิจารณาโหนดข้อมูล k2 ซึ่งเซตต่างๆ จะมีสมาชิกดังนี้

$$R = \{N2, N4, N6, N1, N5, N3\}$$

$$C_s = \{k1, k3, k5, k4, k2\}$$

$$P = \{k1, k3, k5, k4, k2\}$$

$$R_p = \{\}$$

เมื่อไม่มีโหนดในเซตกระเพื่อมให้พิจารณาแล้ว ให้ตรวจสอบเซตต่างๆ ได้แก่ เซตของโหนดเข้ารหัสที่ได้รับการพิจารณาแล้วว่ามีโหนดเข้ารหัสที่ได้รับการพิจารณาครบทุกโหนดหรือไม่ และเซตครอบคลุมกับเซตของโหนดข้อมูลที่ได้รับการพิจารณาแล้วมีครบทุกโหนดแล้วหรือไม่ ในทำนองเดียวกัน หากทั้ง 3 เซตมีสมาชิกครบถ้วนถือว่าความสัมพันธ์กราฟไบบารีโตนนั้นสามารถนำไปใช้ส่งข้อมูลในลำดับชั้นตามแบบจำลอง OSI (OSI model) ได้ต่อไป

ซึ่งกระบวนการตรวจสอบเมทริกซ์กำเนิดที่แสดงไปนั้นสามารถเขียนให้อยู่ในรูปขั้นตอนได้ดังนี้

1. พิจารณาโหนดเข้ารหัสที่มีดีกรีเท่ากับ 1 เพิ่มเข้าไปในเซตของโหนดเข้ารหัสที่ได้รับการพิจารณาแล้วทันที และเพิ่มโหนดข้อมูลซึ่งสัมพันธ์กับโหนดดังกล่าวเข้าไปในทั้งเซตครอบคลุมและเซตกระเพื่อมทันที

- 1.1 พิจารณาทีละโหนดข้อมูลที่อยู่ในเซตกระเพื่อมว่าเชื่อมโยงไปยังโหนดเข้ารหัสโหนดใดบ้าง และนำโหนดเข้ารหัสเหล่านั้นเพิ่มเข้าไปในเซตของโหนดเข้ารหัสที่ได้รับการพิจารณาแล้ว

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.2 ลบเส้นเชื่อมระหว่างโหนดข้อมูลและโหนดเข้ารหัสซึ่งได้รับการพิจารณาแล้วในข้อ 1. พร้อมทั้งนำโหนดข้อมูลที่พิจารณาแล้วออกจากเซตกระเพื่อมด้วย และเพิ่มเข้าไปยังเซตเซตครอบคลุม

1.3 วนซ้ำข้อ 1. จนกว่าโหนดข้อมูลเซตกระเพื่อมจะหมด

2. ทำซ้ำข้อ 1. จากความสัมพันธ์ใหม่ที่ได้รับการปรับปรุงในข้อ 1.2 และทำซ้ำจนกว่าจะหาสมาชิกในเซตกระเพื่อมไม่ได้

ผลลัพธ์ที่ได้ในเซตกระเพื่อมควรจะเป็นเซตว่าง ในขณะที่สมาชิกของเซตของโหนดที่ได้รับการพิจารณาแล้ว และเซตครอบคลุมจะต้องมีทุกโหนดเข้ารหัสและทุกโหนดข้อมูลตามลำดับ

4.1.3 การถอดรหัสเครือข่ายเชิงระบบ

ขั้นตอนการถอดรหัสเครือข่ายเชิงระบบ (Decoding) ได้เพิ่มกรรมวิธีในการพิจารณารูปแบบของกระบวนการถอดรหัสแวลที่ซึ่งได้กล่าวไปแล้วในบทที่ 2 ซึ่งมี 2 ลักษณะดังนี้

1. การถอดรหัสโดยอ้อม ในการถอดรหัสแบบนี้จำเป็นต้องทราบโหนดข้อมูลที่ถอดรหัสแล้วมากเท่าการถอดรหัสโดยตรงในรหัสแวลที่ แต่ผู้รับจำเป็นต้องทราบว่าโหนดเข้ารหัสที่ได้รับมานั้นเกิดจากการเอ็กซ์คลูซีฟออร์ระหว่างโหนดใดบ้าง ซึ่งการถอดรหัสวิธีนี้โหนดผู้รับจะเปรียบเทียบกับโดยอาศัยเซตของโหนดเข้ารหัสที่เพิ่งได้รับมานำมาเปรียบเทียบกับเซตของโหนดเข้ารหัสที่รอการถอดรหัสในหน่วยความจำสำรอง ด้วยการนำสองเซตนั้นมาอินเตอร์เซกชัน (Intersection) กัน ถ้าผลที่ได้มีจำนวนสมาชิกเท่ากับหนึ่ง นั้นหมายความว่าสามารถถอดรหัสได้โดยการนำโหนดเข้ารหัสสองโหนดนั้นมาเอ็กซ์คลูซีฟออร์กันโดยตรง ซึ่งการถอดรหัสวิธีนี้นั้นส่งผลให้มีความเร็วในการถอดรหัสมากกว่าเมื่อเทียบกับการถอดรหัสในรหัสแวลที่

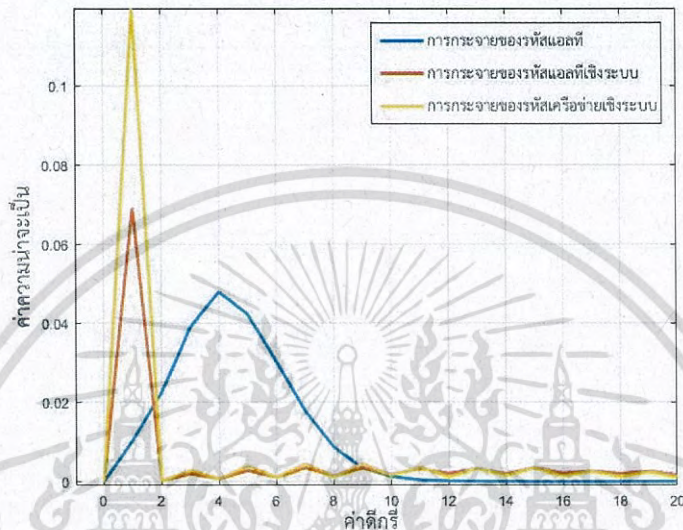
2. การผสมผสานระหว่างวิธีการถอดรหัสโดยตรงและการถอดรหัสโดยอ้อม โดยในบางครั้งไม่มีแพ็กเก็ตที่เพียงพอจำนวน $l - 1$ แพ็กเก็ต และมีโอกาสน้อยที่ผลลัพธ์จากการอินเตอร์เซกชันนั้นจะมีจำนวนสมาชิกเท่ากับ 1 ในวิธีนี้นั้นช่วยให้การถอดรหัสโหนดเข้ารหัสที่มีขนาดของดีกรีขนาดใหญ่มากได้รวดเร็วยิ่งขึ้น

4.1.4 ประสิทธิภาพระหว่างรหัสเครือข่ายเชิงระบบ รหัสแวลที่ และรหัสแวลที่เชิงระบบ

รหัสเครือข่ายเชิงระบบนั้นสามารถเพิ่มประสิทธิภาพของกระบวนการถอดรหัส ไม่เพียงแต่กระบวนการในการพิจารณาการถอดรหัสเพิ่มเติมในหัวข้อ 4.1.3 แต่ยังมีความสัมพันธ์เชิงระบบที่ปรากฏในลักษณะของกราฟไบบารีโตนหรือเมทริกซ์กำเนิดทำให้จำนวนของโหนดเข้ารหัสที่มีค่าดีกรีเท่ากับ 1 เป็นจำนวนคงที่และมากกว่าความสัมพันธ์ในรหัสแวลที่ เมื่อเปรียบเทียบกันให้เห็นได้อย่างชัดเจนในรูปที่ 2.16 และ 4.6 สำหรับการเปรียบเทียบกันในเชิงการกระจายตัวของดีกรีที่โหนดเข้ารหัส ซึ่งในรูปที่ 4.8 แสดงให้เห็นถึงการกระจายตัวของดีกรีในเมทริกซ์ต้นกำเนิดขนาด $[100 \times 150]$ ระหว่างรหัสเครือข่ายเชิงระบบ เปรียบเทียบกับรหัสแวลที่และรหัสแวลที่เชิงระบบสำหรับ ผลลัพธ์ที่ได้นั้นแสดงให้เห็นอย่างชัดเจน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

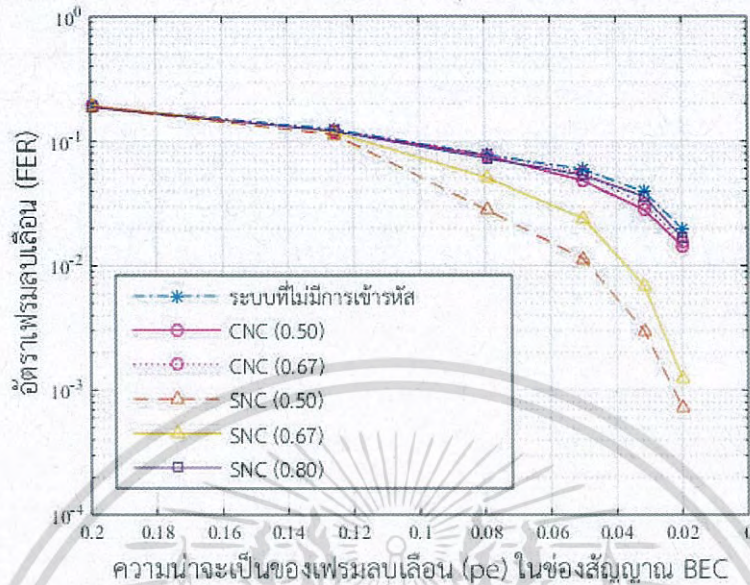
ว่ารหัสเครือข่ายเชิงระบบจะให้ค่าความน่าจะเป็นที่จะเกิดดีกรีเท่ากับ 1 สูงที่สุด ซึ่งส่งผลให้กระบวนการถอดรหัสมีประสิทธิภาพดีขึ้น และยังทำให้กระบวนการแพร่กระจายความเชื่อสามารถ (belief propagation) ทำงานได้รวดเร็วยิ่งขึ้นอีกด้วย



รูปที่ 4.8 การกระจายตัวของดีกรีในโพรพาร์ไทท์กราฟระหว่างรหัสเครือข่ายเชิงระบบ รหัสแอลที และรหัสแอลทีเชิงระบบ

อย่างไรก็ตามในบทนี้ได้ประยุกต์รหัสเครือข่ายเชิงระบบในฝั่งส่งและใช้การถอดรหัสด้วยการตัดสินใจแบบหยาบ (hard decision) เพื่อลดความซับซ้อนในถอดรหัสให้มากที่สุด ในฝั่งโหนดผู้รับ และโดยเฉพาะอย่างยิ่งปริมาณงานในโหนดข้างเคียง

รูปที่ 4.9 แสดงถึงประสิทธิภาพของรหัสเครือข่ายเชิงระบบในฝั่งส่งเปรียบเทียบกับรหัสเครือข่ายทั่วไป (Conventional Network Code : CNC) ซึ่งในการทดสอบคือรหัสแอลทีเชิงระบบ และเครือข่ายที่ปราศจากการเข้ารหัสทั้งสอง โดยในแกนนอนคือความน่าจะเป็นที่แพ็กเก็ตหรือเฟรมข้อมูลนั้นผิดพลาดซึ่งนิยามโดยช่องสัญญาณแบบลบเลือนได้ ในส่วนแกนตั้งคืออัตราการลบเลือนของเฟรมข้อมูล โดยถ้าหากมีบิตใดบิตหนึ่งเกิดการลบเลือนถือว่าทั้งเฟรมนั้นเป็นเฟรมลบเลือน (Erased Frame) ผลที่ได้นั้นแสดงให้เห็นว่ารหัสเครือข่ายเชิงระบบที่อัตรารหัสเท่ากับ 0.5 และ 0.67 ให้อัตราการลบเลือนน้อยกว่ารหัสเครือข่ายทั่วไปอย่างชัดเจน



รูปที่ 4.9 ประสิทธิภาพของรหัสเครือข่ายเชิงระบบเปรียบเทียบกับรหัสเครือข่ายทั่วไป และเครือข่ายที่ไม่มีการเข้ารหัสในช่องสัญญาณแบบลบเลือนได้ ซึ่งพิจารณาจากอัตราเฟรมลบเลือนที่เกิดขึ้น

4.2 การสร้างแผนการในการส่งข้อมูลซ้ำ

หลังจากที่ได้ประยุกต์รหัสเครือข่ายเชิงระบบในฝั่งส่งซึ่งช่วยลดอัตราการลบเลือนได้ระดับหนึ่ง ในหัวข้อนี้จึงได้พัฒนาระบบการส่งข้อมูลซ้ำเพื่อชดเชยประสิทธิภาพของรหัสเครือข่ายเชิงระบบที่ใช้การถอดรหัสด้วยการตัดสินใจแบบหยาบ โดยการใช้ข้อได้เปรียบของธรรมชาติการส่งข้อมูลผ่านเครือข่ายไร้สายที่แพร่กระจายในทุกทิศทางและโหมดเฝ้าสังเกต ที่มีอยู่แทบทุกอุปกรณ์เครือข่ายไร้สาย ซึ่งจะกล่าวในหัวข้อที่ 4.2.1 พร้อมกันนี้ ในหัวข้อ 4.2.2 ได้วิเคราะห์ถึงอัตราเฟรมลบเลือนร่วม (Mutual Erased Frame : MEF) เพื่อแสดงให้เห็นว่าโหนดผู้รับนั้นสามารถรับเฟรมหรือแพ็กเก็ตที่สูญหายไปจากโหนดที่อยู่ข้างเคียงได้

4.2.1 โหมดเฝ้าสังเกต

โหมดเฝ้าสังเกต หมายถึงโหมดพิเศษที่อยู่ในอุปกรณ์เครือข่าย เช่น ส่วนต่อประสานเครือข่าย (network interface cards : NICs) และส่วนต่อประสานเครือข่ายไร้สาย (wireless network interface cards : WNICs) ซึ่งอนุญาตให้อุปกรณ์ดังกล่าวสามารถรับข้อมูลการจราจรทั้งหมดในเครือข่าย โดยปกติแล้วอุปกรณ์ดังกล่าวจะไม่สนใจแพ็กเก็ตที่ไม่ได้ส่งถึงอุปกรณ์เหล่านั้นโดยตรง ซึ่งมีโปรแกรมประยุกต์ที่

ใช้งานได้แก่ โปรแกรมไวร์ชาร์ก (Wireshark) และโหมดฝ้าสังเกตในระบบปฏิบัติการคาลิลินุกซ์ (Kali - Linux) ซึ่งรูปที่ 4.10 ได้ทดสอบคุณสมบัติดังกล่าวโดยให้มีการส่งข้อมูลระหว่างเราเตอร์ที่มีหมายเลขไอพีแอดเดรส (IP address) 192.168.31.1 และคอมพิวเตอร์แล็ปท็อปหมายเลข 2 (Laptop 2) ที่มีหมายเลขไอพีแอดเดรส 192.168.31.104 และให้คอมพิวเตอร์แล็ปท็อปหมายเลข 1 (Laptop 1) ที่มีหมายเลขไอพีแอดเดรส 192.168.31.117 ทำการดักฟังข้อมูลที่สื่อสารกันระหว่างอุปกรณ์ดังกล่าวผ่านโปรแกรมไวร์ชาร์กซึ่งแสดงผลให้เห็นในรูปที่ 4.9



รูปที่ 4.11 แพ็กเก็ตที่แอบได้ยิน (Overheard) ด้วยคอมพิวเตอร์แล็ปท็อปหมายเลข 1

จากรูปที่ 4.11 แสดงถึงการได้ยินแพ็กเก็ตที่ส่งจากคอมพิวเตอร์แล็ปท็อปหมายเลข 2 ไปยังเราเตอร์ดังที่ปรากฏในฝั่งคอมพิวเตอร์แล็ปท็อปหมายเลข 1 ซึ่งจะสังเกตได้จากหมายเลขไอพีแอดเดรส 192.168.31.104

นอกจากนี้โหมดดังกล่าวยังมีส่วนสำคัญในการพัฒนาระบบการสื่อสารโดยใน [4] ได้นำเสนอขั้นตอนวิธีโคป ซึ่งใช้ธรรมชาติของการแพร่กระจายสัญญาณไร้สาย เพื่อหาโอกาสที่จะนำแพ็กเก็ตมาเข้ารหัสด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การเอ็กซ์คลูซีฟออร์ นอกจากนี้ยังมีอัลกอริธึม ANCR ที่ใช้งานโหนดดังกล่าวในลักษณะเดียวกัน สำหรับรหัสเครือข่ายเชิงระบบนี้ได้ใช้โหนดดังกล่าวเพื่อสร้างแผนการในการส่งข้อมูลซ้ำและได้ปรับปรุงแก้ไขจาก [30] ซึ่งช่วยลดเวลาแฝงที่เกิดขึ้นจากการส่งข้อมูลซ้ำโดยใช้ข้อมูลที่มีอยู่จากโหนดข้างเคียงที่รับแพ็กเก็ตจากโหนดดังกล่าว อย่างไรก็ตามในรหัสเครือข่ายเชิงระบบได้ปรับปรุงกลวิธีในการส่งข้อมูลซ้ำ ซึ่งลดความซับซ้อนในการเลือกโหนดข้างเคียงที่เหมาะสมในการส่งแพ็กเก็ตที่สูญหายไปยังโหนดผู้รับ โดยใช้ขั้นตอนวิธีในรูปที่ 4.12 โดยเมื่อมีโหนดผู้รับได้รับแพ็กเก็ตหรือเฟรมลบเลือนจึงจำเป็นที่จะต้องส่งแพ็กเก็ตร้องขอการส่งข้อมูลซ้ำ (Request retransmission packet) ไปยังโหนดผู้ส่งโหนดข้างเคียงซึ่งสามารถรับรู้การร้องขอนี้ได้จึงนำมาเปรียบเทียบกับแพ็กเก็ตที่มีในหน่วยความจำสำรองซึ่งได้มาจากโหนดสังเกตการว่าสามารถส่งแพ็กเก็ตเหล่านั้นแทนได้หรือไม่

```

INPUT: encoding frames  $N$ , Generator matrix  $G_{snc}$ .
OUTPUT: retransmission message  $retx\_msg$ .
 $err\_frames = \text{decoding}(N, G_{snc});$ 
 $retx\_msg = \text{broadcasting\_req\_retx}(\text{neighbors}, err\_frames);$ 
while received_acks(neighbors); do
  if  $mef == 0$  then
    retransmission (neighbors);
  else
    request_retransmission (source);
  end if
end while

```

รูปที่ 4.12 ขั้นตอนวิธีการส่งข้อมูลซ้ำด้วยโหนดข้างเคียงในรหัสเครือข่ายเชิงระบบ

ในระบบที่ไม่ได้ประยุกต์รหัสเครือข่ายเชิงระบบ เมื่อโหนดผู้รับได้รับแพ็กเก็ตลบเลือน เวลาที่ใช้ในการส่งข้อมูลทั้งหมด (total time of transmission : t_x) สามารถหาค่าได้จากสมการที่ (13) โดยที่ t คือระยะเวลาที่ส่งหนึ่งแพ็กเก็ต, h คือจำนวนฮอป ระหว่างโหนดผู้ส่งและโหนดผู้รับ, N คือจำนวนแพ็กเก็ตที่ต้องการส่ง และ E_i จำนวนแพ็กเก็ตลบเลือนของโหนด i^{th} และกรณีนี้ยังเป็นกรณีที่แย่ที่สุดของการส่งข้อมูลผ่านเครือข่ายมัลติคาสต์ที่ทำการทดสอบในงานวิจัยนี้ด้วย

$$t_x = th \times (N + E_i) \quad (13)$$

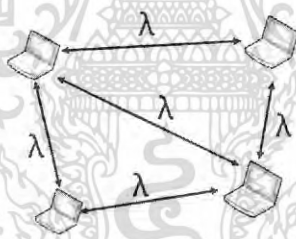
เมื่อเปรียบเทียบกับระบบที่มีการประยุกต์ใช้รหัสเครือข่าย ทันทีที่มีการสูญหายของข้อมูลเกิดขึ้นที่ฝั่งผู้รับ โหนดผู้รับนั้นจะแพร่กระจายข้อความไปยังโหนดผู้ส่งที่อยู่ห่างไกลออกไป ซึ่งแพ็กเก็ตร้องขอนี้จะประกอบไปด้วยหมายเลขแพ็กเก็ตที่สูญหายและต้องการให้โหนดผู้ส่งส่งกลับมาอีกครั้ง และด้วยธรรมชาติของการส่งข้อมูลผ่านสื่อสัญญาณไร้สาย ทำให้โหนดข้างเคียงสามารถรับรู้ได้ถึงการส่งข้อความดังกล่าว ซึ่ง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โหนดข้างเคียงจะทำการตรวจสอบกับแพ็กเก็ตที่ต้นมืออยู่ซึ่งได้มาจากการแอบได้ยิน ว่าหมายเลขแพ็กเก็ตที่สูญหายเหมือนกับโหนดผู้รับหรือไม่ ซึ่งถ้าหากไม่มีหมายเลขแพ็กเก็ตที่สูญหายเหมือนกันก็จะสามารถทำให้โหนดข้างเคียงสามารถส่งข้อมูลที่สูญหายแทนโหนดผู้ส่งที่อยู่ห่างไกลออกไป ซึ่งข้อได้เปรียบนี้เองทำให้ระบบที่มีรหัสเครือข่ายเชิงระบบสามารถลดเวลาในการร้องขอข้อมูลซ้ำ ซึ่งเวลาที่ใช้นั้นสามารถหาได้จากสมการที่ (14)

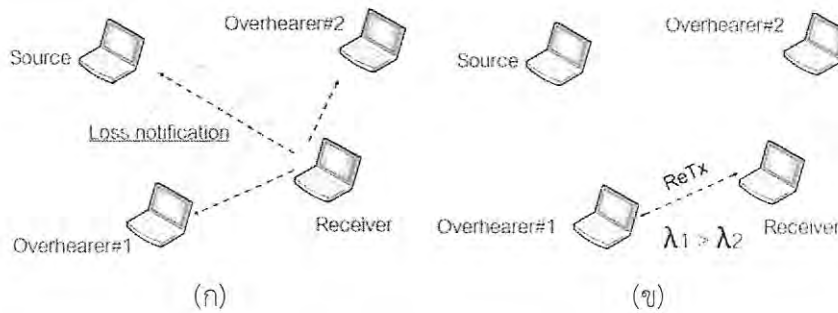
$$t_x = t \times (hN + E_i) \quad (14)$$

ในการประยุกต์ใช้จริงนั้น ทุกโหนดในเครือข่ายไร้สายจำเป็นจะต้องส่งแพ็กเก็ตขนาดเล็กทุกช่วงเวลาเพื่อรักษาสถานะการเชื่อมต่อกับโหนดอื่นๆ โดยรหัสเครือข่ายเชิงระบบได้ใช้ข้อได้เปรียบนี้ในการพัฒนาและให้แต่ละโหนดส่งค่าทางสถิติของอัตราการรับข้อมูลสำเร็จ (success receiving rate : λ) ซึ่งหมายถึงอัตราการแอบได้ยินด้วยเพื่อช่วยในการตัดสินใจ เช่นในรูปที่ 4.13 เมื่อโหนดผู้รับแพร่กระจายข้อความร้องขอการส่งข้อมูลซ้ำ โหนดข้างเคียงจะสามารถรับข้อความนี้ได้เช่นเดียวกัน และในรูปที่ 4.14 โหนดผู้รับทราบอยู่แล้วว่าโหนดใดที่อยู่ใกล้และมีค่า λ สูงที่สุดซึ่งหมายความว่าโหนดข้างเคียงนั้นให้โอกาสที่จะมีเฟรมลบเลือนร่วมน้อยมาก ทำให้สามารถสร้างการเชื่อมต่อเพื่อที่จะส่งข้อมูลที่สูญหายในโหนดผู้รับทันที



รูปที่ 4.13 การส่งแพ็กเก็ตเพื่อรักษาสถานะของการเชื่อมต่อและค่าอัตราการรับส่งข้อมูลสำเร็จ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.14 การสร้างการเชื่อมต่อระหว่างโหนดผู้รับและโหนดข้างเคียง

(ก) การส่งข้อความแจ้งเตือนไปยังโหนดผู้ส่ง

(ข) การสร้างการเชื่อมต่อเพื่อส่งข้อมูลซ้ำระหว่างโหนดผู้รับและโหนดข้างเคียง

จากรูปที่ 4.14 ทันทีที่โหนดผู้รับได้รับข้อมูลที่เสียหายหรือเฟรมลบเลือน หลังจากการที่ทำการถอดข้อมูลที่ถูกรหัส (Decapsulation) จึงได้ทำการส่งแพ็กเก็ตร้องขอไปยังโหนดแหล่งกำเนิดเพื่อส่งข้อมูลเหล่านั้นซ้ำอีกครั้งแสดงในรูป (ก) ซึ่งในหลักการแพร่กระจายสัญญาณนี้เองทำให้โหนดข้างเคียงทั้งสองในรูป (ข) นั้นสามารถรับรู้ถึงการร้องขอนี้ ซึ่งทำให้โหนดผู้รับนั้นสามารถที่จะสร้างการเชื่อมต่อกับโหนดข้างเคียงที่มีค่าอัตราการรับส่งข้อมูลสำเร็จที่สูงที่สุดเพื่อส่งข้อมูลที่เสียหายได้ โดยในหัวข้อที่ 4.2.2 จะแสดงให้เห็นถึงความน่าเชื่อถือจากการที่โหนดผู้รับเลือกที่จะรับข้อมูลที่เสียหายจากโหนดข้างเคียง

4.2.2 การวิเคราะห์อัตราเฟรมลบเลือนร่วม

เฟรมลบเลือนร่วม หมายถึง จำนวนหมายเลขแพ็กเก็ตหรือหมายเลขเฟรมที่ลบเลือนซึ่งปรากฏอยู่ในโหนดผู้รับที่มีมากกว่าหรือเท่ากับ 2 โหนดขึ้นไป โดยมีส่วนสำคัญในการพัฒนาการส่งข้อมูลซ้ำด้วยการแอบได้ยินในโหนดข้างเคียง ซึ่งในส่วนการวิเคราะห์นี้เป็นหนึ่งในการวัดประสิทธิภาพของรหัสเครือข่ายเชิงระบบในรูปแบบของความน่าจะเป็นที่จะเกิดเฟรมลบเลือนร่วม (probability of mutual erasure frame frame : P_{mef}) ซึ่งสามารถอธิบายในสมการที่ (15)

$$P_{mef} = \frac{\prod_{i=1}^q E_i}{\prod_{i=1}^q U_i} \quad (15)$$

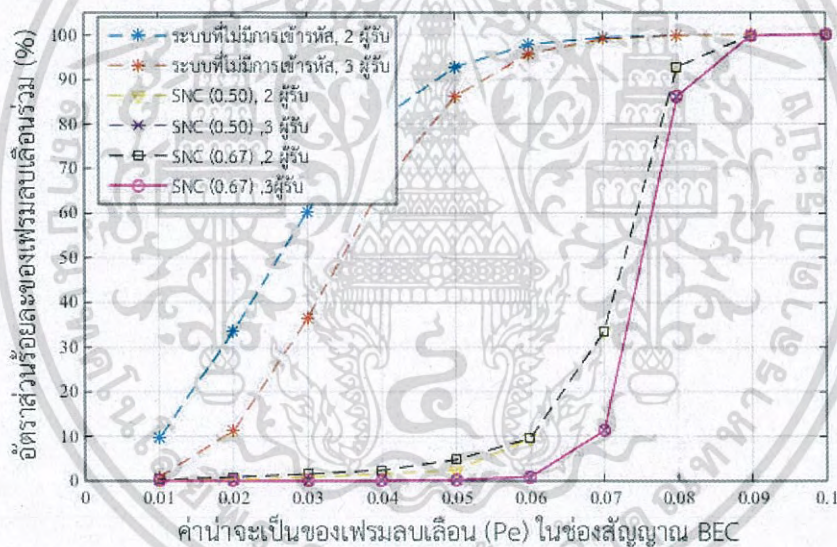
กำหนดให้ E_i เป็นเซตหมายเลขเฟรมลบเลือนของโหนด i^{th} ในกลุ่มที่มีโหนดผู้รับจำนวน q ซึ่งรวมถึงโหนดข้างเคียงที่ทำหน้าที่แอบได้ยินด้วย นอกจากนี้ยังได้วัดค่าข่าวสารร่วม (mutual information) ระหว่าง 2 โหนดผู้รับในสมการที่ (16) และ q โหนดผู้รับในสมการที่ (17) เมื่อ $p(e_1, e_2)$ คือความน่าจะเป็นที่จะเกิดเฟรมลบเลือนร่วมดังในสมการที่ (15) ของโหนด 1 และ 2 เป็นต้น และ $p(e)$ คือความน่าจะเป็นที่เฟรมจะลบเลือนซึ่งนิยามโดยช่องสัญญาณแบบลบเลือนได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$I(E_1; E_2) = \sum_{e_1 \in E_1} \sum_{e_2 \in E_2} p(e_1, e_2) \log_2 \frac{p(e_1, e_2)}{p(e_1) p(e_2)} \quad (16)$$

$$I(E_1; E_2 \dots; E_q) = I(E_1; E_2) - I(E_1; E_2 | E_3) - I(E_1; E_2; E_3 | E_4) \dots - I(E_1; E_2; \dots; E_{q-1} | E_q) \quad (17)$$

ในรูปที่ 4.15 แสดงให้เห็นถึงอัตราส่วนร้อยละของอัตราเฟรมลบเลื่อนร่วมที่เกิดขึ้นระหว่าง 2 ถึง 3 โหนดผู้รับ โดยมีค่าความน่าจะเป็นที่เฟรมจะลบเลื่อนระหว่าง 0.01 ถึง 0.1 ในแกน x ผลที่ได้เปรียบเทียบกับระหว่างเครือข่ายที่ไม่มีการเข้ารหัสและเครือข่ายที่มีรหัสเครือข่ายเชิงระบบในอัตรารหัสเท่ากับ 0.5 และ 0.67 ในช่วงความน่าจะเป็นของเฟรมลบเลื่อนระหว่าง 0.01 ถึง 0.07 ในเครือข่ายที่ไม่มีการเข้ารหัสมีอัตราส่วนร้อยละของอัตราเฟรมลบเลื่อนร่วมใกล้เคียง 100% ในขณะที่เครือข่ายที่มีรหัสเครือข่ายเชิงระบบมีอัตราส่วนร้อยละของอัตราเฟรมลบเลื่อนร่วมอยู่ระหว่าง 0% ถึง 10% ซึ่งแสดงให้เห็นอย่างชัดเจนว่าโหนดผู้รับสามารถรับเฟรมลบเลื่อนจากโหนดข้างเคียงได้อย่างมีประสิทธิภาพ



รูปที่ 4.15 อัตราส่วนร้อยละของความน่าจะเป็นที่จะเกิดเฟรมลบเลื่อนร่วมในจำนวน 2-3 โหนดผู้รับ

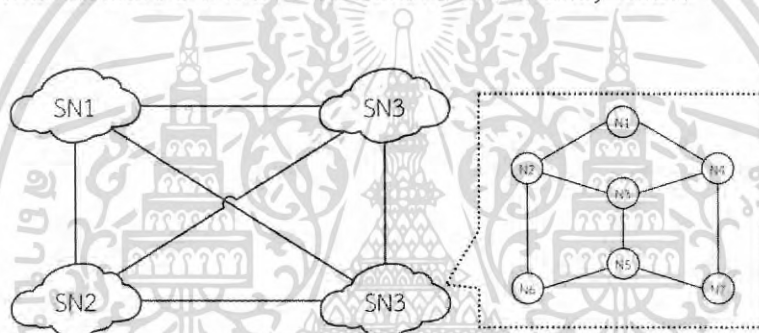
4.3 การวัดผลและผลลัพธ์

ในมุมมองของระบบทั้งหมด รหัสเครือข่ายเชิงระบบได้ย้ายภาระการคำนวณมาไว้ที่โหนดผู้ส่งในขั้นตอนการแปลงเมทริกซ์กำเนิดให้มาอยู่ในรูปแบบเชิงระบบด้วยการสร้างเมทริกซ์ต้นกำเนิดเชิงระบบดังรูปที่ 4.4 โดยใช้ความซับซ้อนที่ใกล้เคียงกับกระบวนการจัดแบบเกาส์เซียนที่ $O(Nk^2)$ ซึ่งประสิทธิภาพที่เพิ่มขึ้นจะตกอยู่ที่ฝั่งโหนดผู้รับและโหนดข้างเคียง โดยจะใช้ความซับซ้อนในการถอดรหัสของรหัส

เครือข่ายเชิงระบบนั้นจะอยู่ในระดับคงที่เท่ากับ $O(N - k)$ เมื่อเปรียบเทียบกับรหัสแอลทีที่ใช้ความซับซ้อนในการถอดรหัสเท่ากับ $O(N)$ ซึ่งในหัวข้อที่ 4.3.1 จะกล่าวถึงทอพอโลยีที่ใช้ในการทดสอบรหัสเครือข่ายเชิงระบบพร้อมทั้งวัดผลในแง่ของค่าทรูพุดและเวลาแฝงในการส่งข้อมูลในหัวข้อที่ 4.3.2

4.3.1 ทอพอโลยีที่ใช้ทดสอบ

ทอพอโลยีเครือข่ายที่ใช้ในการวัดประสิทธิภาพนั้นคือเครือข่ายขนาดใหญ่ดังรูปที่ 4.16 ซึ่งประกอบไปด้วย 4 เครือข่ายย่อยเชื่อมต่อถึงกันโดยตรง ภายแต่ละในเครือข่ายย่อยนั้นมีเครือข่ายรูปผีเสื้อซึ่งประกอบด้วย 7 โหนด ในการทดสอบให้โหนดหมายเลข N1 เป็นโหนดผู้ส่งและโหนดหมายเลข N6 และ N7 เป็นโหนดผู้รับ ในการวัดประสิทธิภาพนั้นจะเน้นไปที่การส่งข้อมูลระหว่างเครือข่ายย่อยซึ่งขั้นตอนวิธีการเข้ารหัสเครือข่ายทั้งใน [4] และในบทที่ 3 เองนั้นไม่สามารถทำงานได้อย่างมีประสิทธิภาพ โดยงานวิจัยนี้อาศัยโหนดหมายเลข 3 ทำหน้าที่เป็นโหนดเกตเวย์ (Gateway Node)



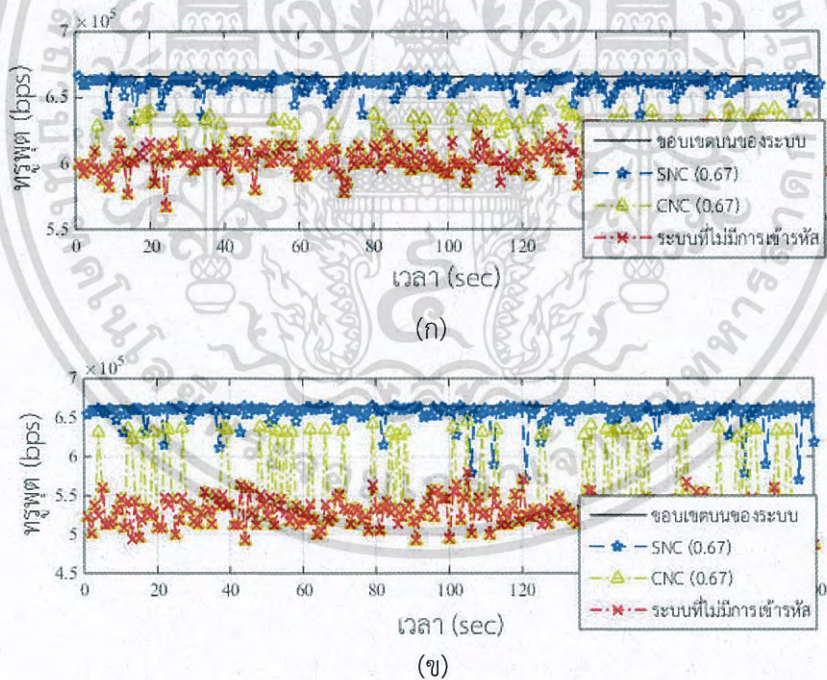
รูปที่ 4.16 เครือข่ายขนาดใหญ่และเครือข่ายรูปผีเสื้อ

ในเครือข่ายขนาดใหญ่ในรูปที่ 4.16 การสร้างการเชื่อมต่อระหว่างโหนดผู้ส่งและกลุ่มโหนดผู้รับที่อยู่ต่างเครือข่ายย่อยทำให้เกิดความยุ่งยากและล่าช้าในกระบวนการส่งข้อมูลเข้าไปยังกลุ่มโหนดผู้รับต่างๆ สำหรับการส่งข้อมูลระหว่างโหนดนั้น เครือข่ายที่มีรหัสเครือข่ายเชิงระบบจะช่วยลดจำนวนการส่งข้อมูลซ้ำและยังช่วยให้ค่าทรูพุดของเครือข่ายเพิ่มขึ้นอีกด้วย ในการจำลองได้ตั้งสมมติฐานว่าช่องสัญญาณรบกวนเกาส์เซียนขาวบวก แทพไม่มีผลกับเครือข่ายเนื่องจากได้พิจารณาไปแล้วด้วยกลไกของลำดับชั้นในแบบจำลองการเชื่อมต่อระหว่างระบบเปิดที่อยู่ระดับต่ำลงไป ในการส่งข้อมูลของรหัสเครือข่ายเชิงระบบด้วยอัตรารหัส $\frac{k}{N}$ นั้นจะเป็นการส่งข้อความเข้ารหัสจำนวน N เฟรมซึ่งสร้างจากข้อมูลที่ต้องการจะส่งจำนวน k เฟรม ซึ่งแต่ละเฟรมมี f บิตและคุณภาพของการส่งสัญญาณอยู่ที่ L เมกะบิตต่อวินาที (Megabit per sec : Mbps) ผ่านช่องสัญญาณแบบลบเลื่อนได้

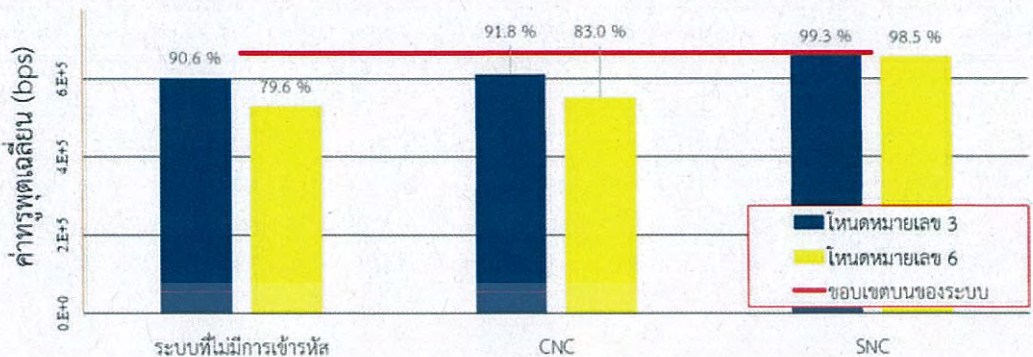
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.2 ผลลัพธ์

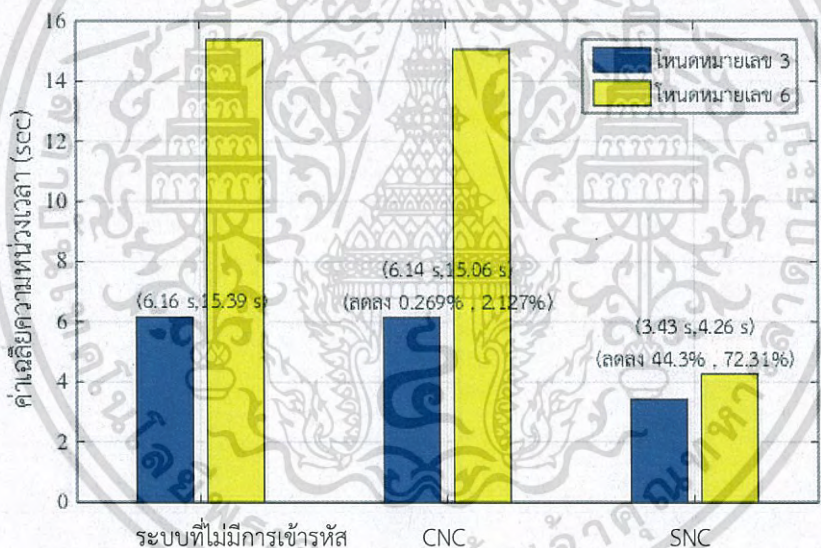
เพื่อแสดงให้เห็นถึงประสิทธิภาพของรหัสเครือข่ายเชิงระบบ ได้กำหนดให้ $f = 1,000$ บิต จำนวนเฟรมข้อมูลคงที่ $k = 1,000$ และให้เฟรมเข้ารหัส $N = 1,500$ ซึ่งข้อมูลที่จะต้องส่งทั้งหมดมีค่าเท่ากับ $f \times N$ ผลลัพธ์ที่ได้แสดงให้เห็นว่าเครือข่ายที่มีรหัสเครือข่ายเชิงระบบที่มีอัตรารหัสเท่ากับ 0.5 และ 0.67 ให้ประสิทธิภาพที่ดีกว่าเครือข่ายที่ใช้รหัสเครือข่ายทั่วไปซึ่งในที่นี้เปรียบเทียบกับรหัสแอลที่ซึ่งนำมาใช้ในฝั่งส่งซึ่งได้ทำการวัดทรูพุดในห้วงเวลา 200 วินาทีของโหนดหมายเลข 3 ซึ่งเป็นโหนดผู้รับที่อยู่ในเครือข่ายย่อยเดียวกันและโหนด 6 ซึ่งเป็นหนึ่งในโหนดผู้รับที่อยู่ต่างเครือข่ายย่อย ในรูปที่ 4.17 แสดงให้เห็นว่าเครือข่ายที่มีรหัสเครือข่ายเชิงระบบนั้นใกล้เคียงกับขอบเขตบนของระบบมากที่สุดในเส้นสีน้ำเงิน ในขณะที่เครือข่ายที่ใช้รหัสเครือข่ายทั่วไปและเครือข่ายที่ไม่มีมีการเข้ารหัสดังกล่าวให้ค่าทรูพุดน้อยกว่าอย่างเห็นได้ชัด นอกจากนี้ยังพิจารณาถึงค่าเฉลี่ยของทรูพุด ในรูปที่ 4.18 ซึ่งแสดงให้เห็นอย่างชัดเจนยิ่งขึ้นของการเพิ่มขึ้นของค่าทรูพุดในเครือข่ายที่ใช้รหัสเครือข่ายเชิงระบบโดยใกล้เคียงกับขอบเขตบนมากที่สุดที่ 99.3% และ 98.5% ซึ่งเพิ่มขึ้นจากเครือข่ายที่ใช้รหัสเครือข่ายทั่วไป 7.5% และ 15.5% และเพิ่มขึ้นจากเครือข่ายที่ไม่ใช้รหัสเครือข่ายใดๆ 8.7% และ 18.9% ของโหนดหมายเลข 3 และ 6 ตามลำดับ



รูปที่ 4.17 (ก) ค่าทรูพุดที่วัดได้จากโหนดหมายเลข 3 และ (ข) โหนดหมายเลข 6



รูปที่ 4.18 การเปรียบเทียบค่าเฉลี่ยทฤษฎีของโหนดหมายเลข 3 และหมายเลข 6 ระหว่างเครือข่ายที่มีรหัสเครือข่ายเชิงระบบ (SNC), เครือข่ายที่ใช้รหัสเครือข่ายทั่วไป (CNC) และเครือข่ายที่ปราศจากการใช้รหัสเครือข่าย (w/o encoding)



รูปที่ 4.19 การเปรียบเทียบค่าเฉลี่ยของเวลาแฝงในการส่งข้อมูลของโหนดหมายเลข 3 และหมายเลข 6 ระหว่างเครือข่ายที่มีรหัสเครือข่ายเชิงระบบ (SNC), เครือข่ายที่ใช้รหัสเครือข่ายทั่วไป (CNC) และเครือข่ายที่ปราศจากการใช้รหัสเครือข่าย (w/o encoding)

นอกจากนี้ในงานวิจัยนี้ยังได้วัดประสิทธิภาพในแง่ของเวลาที่ใช้ในการส่งข้อมูลทั้งหมด โดยรูปที่ 4.19 แสดงให้เห็นถึงค่าเวลาแฝงเฉลี่ยของทั้งระบบของการส่งข้อมูลจากโหนดผู้ส่งไปยังโหนดผู้รับ โดยผลจากกราฟแสดงให้เห็นถึงค่าเวลาแฝงของโหนดหมายเลข 6 มีค่าสูงกว่าโหนดหมายเลข 3 ในทั้งสามระบบ แต่อย่างไรก็ตามเครือข่ายที่ใช้รหัสเครือข่ายเชิงระบบนั้นรวดเร็วกว่าทั้งสองระบบที่เหลือและลดเวลาแฝง

เฉลี่ยลงเกือบ 70% เมื่อเทียบกับเครือข่ายที่ไม่ใช่การเข้ารหัสเครือข่ายใดๆ สำหรับค่าเวลาแฝงเฉลี่ยของ โหนดหมายเลข 3 ในเครือข่ายที่มีระบบเครือข่ายเชิงระบบน้อยกว่าในระบบที่ไม่มีการเข้ารหัสเครือข่าย ใดๆ ประมาณ 40%

4.4 การวิเคราะห์ผลการทดลองและอัลกอริธึม

ในหัวข้อนี้ได้วิเคราะห์ถึงความต้องการของระบบเครือข่าย เพื่อให้ทำให้อัลกอริธึมรหัสเครือข่ายเชิงระบบนั้นมีประสิทธิภาพสูงที่สุด โดยเริ่มจากการกำหนดตัวแปรต่างๆ เพิ่มเติม โดยเริ่มจากการหาเวลาในการส่งข้อมูล 1 เฟรม, t , โดยสามารถหาได้จากสมการที่ (18)

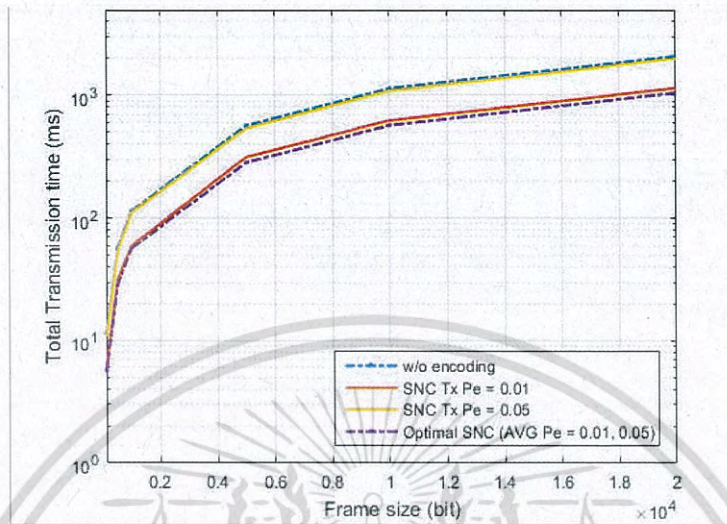
$$t = \frac{f}{b_w} \text{ วินาที (second)} \quad (18)$$

โดยที่ b_w คือ ค่าแบนด์วิธของระบบซึ่งในการวัดผลนั้นกำหนดให้มีค่าเท่ากับ 54 Mbps ในการวัดประสิทธิภาพนั้นได้ทดสอบกับเครือข่ายที่มีทอพอโลยีลักษณะเช่นเดียวกับรูปที่ 4.16 ซึ่งวัดเวลาในการส่งข้อมูลจำนวน 1,500 เฟรม เปรียบเทียบกับระบบที่ไม่มีการเข้ารหัสใดๆ กับระบบที่มีรหัสเชิงระบบทั้งแบบสุ่มความผิดพลาดและเงื่อนไขที่ดีที่สุด พร้อมทั้งกำหนดค่าความน่าจะเป็นที่เฟรมเหล่านั้นจะเกิดการลบ-เลือน p_e และขนาดของเฟรม f ที่มีค่าที่แตกต่างกัน

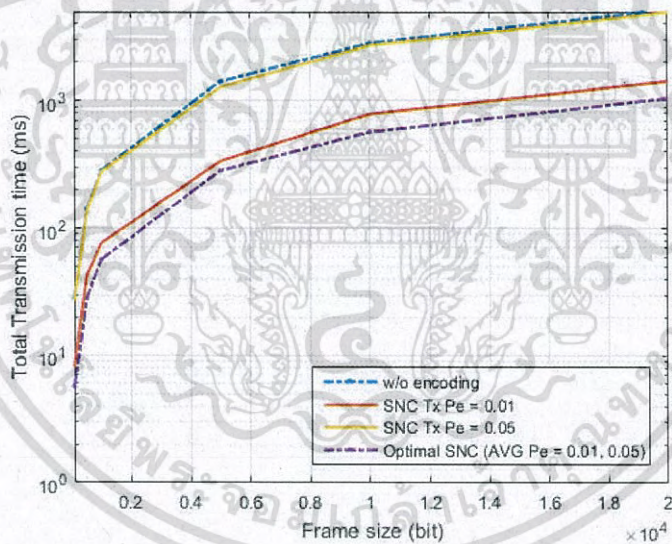
ในรูปที่ 4.20 (ก) เป็นผลลัพธ์ที่ได้จากการวัดค่าที่โหนดหมายเลข 3 ซึ่งเป็นโหนดเกตเวย์ และรูปที่ 4.20 (ข) เป็นผลลัพธ์ที่ได้จากการวัดค่าที่โหนดหมายเลข 6 ซึ่งเป็นโหนดผู้รับ โดยได้เปรียบเทียบระหว่างขนาดของเฟรมที่ใช้ส่งที่แตกต่างกันด้วยขนาด 100, 500 1,000, 5,000, 10,000 และ 25,000 บิต กับเวลาในการส่งข้อมูลทั้งหมดซึ่งรวมถึงการส่งข้อมูลซ้ำด้วย ในระบบที่แตกต่างกัน เช่น ระบบที่ส่งข้อมูลตามเร้าตั้งโพรโตคอลมาตรฐาน, ระบบที่มีรหัสเครือข่ายเชิงระบบ และระบบที่มีรหัสเครือข่ายเชิงระบบด้วยเงื่อนไขที่เหมาะสมที่สุด สำหรับระบบที่มีรหัสเครือข่ายเชิงระบบ โดยระหว่างการทดสอบประสิทธิภาพนั้น ได้กำหนดให้มีโอกาสที่จะเกิดเฟรมสูญหายร่วมกับโหนดแอบไต่กิน ด้วยเงื่อนไข $m_{i,j} \neq \emptyset$ ซึ่งทำให้โหนดข้างเคียงไม่สามารถส่งข้อมูลที่สูญหายไปยังโหนดผู้รับได้ และระบบที่มีรหัสเครือข่ายเชิงระบบด้วยเงื่อนไขที่เหมาะสมที่สุดที่กำหนดให้ $m_{i,j} = \emptyset$ ซึ่งจะทำให้โหนดข้างเคียงสามารถส่งข้อมูลที่สูญหายได้ทุกครั้ง

ผลที่วัดได้นั้น จากการทดลองส่งแพ็กเก็ตขนาด 10,000 บิต จากโหนดผู้ส่ง (โหนดหมายเลข 1) ไปยังโหนดผู้รับ (โหนดหมายเลข 6) ที่อยู่ต่างเครือข่ายย่อย ผ่านช่องสัญญาณที่มีค่า p_e เท่ากับ 0.01 ในระบบที่มีรหัสเครือข่ายเชิงระบบด้วยเงื่อนไขที่เหมาะสมที่สุดนั้นเป็นการเฉลี่ยค่าที่ได้จากค่า p_e เท่ากับ 0.01 และ 0.05 ซึ่งผลลัพธ์ที่ได้นั้นมีค่าใกล้เคียงกันอย่างมาก ซึ่งจะใช้เวลาในการส่งโดยเฉลี่ย 550 ms ในขณะที่ระบบที่มีรหัสเครือข่ายเชิงระบบนั้นใช้เวลาในการส่งอยู่ที่ 750 – 780 ms และในระบบที่ส่งข้อมูลตามเร้าตั้งโพรโตคอลมาตรฐานอยู่ที่ 2,800 – 3,000 ms

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ก)



(ข)

รูปที่ 4.20 ความสามารถในการลดเวลาการส่งโดยรวมเมื่อเปรียบเทียบระหว่างระบบที่ส่งข้อมูลตามเร้าตั้งโพรโตคอลมาตรฐาน, ระบบที่มีรหัสเครือข่ายเชิงระบบ และระบบที่มีรหัสเครือข่ายเชิงระบบด้วยเงื่อนไขที่เหมาะสมที่สุด

(ก) ในโหมดหมายเลข 3 (ข) ในโหมดหมายเลข 6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

ในการสื่อสารข้อมูลในเครือข่ายมัลติคาสต์แบบ 2-minimal ในกรณีที่เส้นทางการส่งข้อมูลผ่านเส้นทางที่สั้นที่สุด (Shortest path) และในกรณีที่บางเส้นทางไม่สามารถให้บริการได้ ทำให้เส้นทางของการส่งผ่านแพ็กเก็ตมีตัวเลือกน้อยลงและมีโอกาสที่จะเกิดเส้นทางคอคอดขึ้นในระบบ ซึ่งผลที่ตามมาคือปริมาณงานที่โหนดคอคอด ซึ่งมีหน้าที่เก็บและส่งผ่านข้อมูล (Store and forward) ไม่สามารถทำงานได้อย่างมีประสิทธิภาพและอาจมีการดรอปแพ็กเก็ตนั้นทิ้งไปเนื่องจากมีทรัพยากรที่จำกัด ทำให้การส่งแพ็กเก็ตใช้เวลามากขึ้นในการส่งแพ็กเก็ตจากโหนดผู้ส่งไปยังโหนดผู้รับ และการทำให้การใช้งานช่องสัญญาณมีประสิทธิภาพลดลง

งานวิจัยนี้ได้ศึกษาการทำงานของระบบเครือข่ายไร้สายมัลติคาสต์แบบ 2-minimal ซึ่งการแก้ปัญหาคอคอดที่เกิดขึ้นนั้น ได้นำเสนอวิธีเครือข่ายแบบปรับตัวได้ (ANCR) โดยเป็นการนำทฤษฎีกราฟไม่เนอร์เข้ามาช่วยพิจารณาแพ็กเก็ตของโหนดผู้ส่ง โดยใช้ทิศทางไหลของข้อมูล ประกอบกับ ทอพอโลยีที่โหนดดังกล่าวนั้นได้เรียนรู้มา เพื่อหาโอกาสที่จะนำแพ็กเก็ตนั้นมาเข้ารหัสด้วยการเอ็ชต์คลูซีฟออร์ที่โหนดคอคอด ผลที่ได้ช่วยให้ทำให้ทรูพุดโดยรวมของทั้งระบบเพิ่มขึ้น 35% และใกล้เคียง 50% โดยเปรียบเทียบกับการจัดเส้นทางด้วยโพรโตคอลตามมาตรฐานและยังลดระยะเวลาการส่งข้อมูลได้ถึง 30%

เมื่อทดสอบกับเครือข่ายที่มีลักษณะใหญ่ขึ้นพบว่า ในขั้นตอนการหาค่าของกราฟในรหัสเครือข่ายแบบปรับตัวได้นั้นไม่สามารถทำงานได้อย่างมีประสิทธิภาพและการสื่อสารผ่านช่องสัญญาณแบบโบนารีลบเลื่อนได้ในเครือข่ายขนาดใหญ่จะทำให้เกิดความล่าช้าของการส่งข้อมูลจากโหนดผู้ส่งที่อยู่ห่างไกลออกไป งานวิจัยนี้จึงได้นำเสนอวิธีเครือข่ายเชิงระบบมาช่วยเพิ่มความน่าเชื่อถือในการส่งข้อมูลผ่านช่องสัญญาณแบบโบนารีลบเลื่อนได้ ซึ่งรหัสเครือข่ายเชิงระบบดังกล่าวนี้ได้ปรับปรุงและพัฒนามาจากรหัสแอลที่ตั้งแต่การสร้างความสัมพันธ์ในรูปแบบกราฟโบนารีโทพีในขั้นตอนสุ่มโยน ตลอดจนกระบวนการถอดรหัส โดยเน้นไปที่ความรวดเร็วในการสร้างและลดความซับซ้อนในการถอดรหัส พร้อมทั้งยังปรับปรุงขั้นตอนวิธีการส่งข้อมูลซ้ำซึ่งช่วยให้ประหยัดเวลาในการส่งข้อมูลจากโหนดผู้ส่งที่อยู่ห่างไกลออกไปโดยรับข้อมูลที่ต้องการจากโหนดที่อยู่ข้างเคียงที่มีอัตราการรับข้อมูลสำเร็จสูงที่สุด ผลที่ได้คือในเครือข่ายที่มีรหัสเครือข่ายเชิงระบบช่วยเพิ่มทรูพุดได้ถึง 8% และเพิ่มขึ้นถึง 19% เมื่อส่งข้อมูลที่สูญหายในเครือข่ายย่อยเดียวกัน และยังช่วยลดเวลาที่ใช้ในการส่งข้อมูลทั้งหมดได้ถึง 40 - 70% เมื่อเปรียบเทียบกับการใช้รหัสเครือข่ายแบบดั้งเดิม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

5.1 ข้อเสนอแนะ

ในงานวิจัยยังพบว่ามีปัญหาเกิดขึ้นในรหัสเครือข่ายแบบปรับตัวได้ ซึ่งในการทดลองนั้นได้ทดสอบการเข้ารหัสได้เพียงครั้งละ 2 ถึง 3 แพ็กเก็ต ซึ่งถ้าพิจารณาแพ็กเก็ตจำนวนมากกว่านี้จะทำให้เพิ่มเวลาแฝงให้กับระบบ เมื่อโหนดผู้รับจะต้องรอแพ็กเก็ตที่จะเข้ามาผ่านช่องทางการแอบได้ยิน และนอกจากนี้ในขั้นตอนการคำนวณหาคุณสมบัติกราฟไมเนอร์ โหนดผู้ส่งจำเป็นต้องอาศัยการเรียนรู้ทอพอโลยีให้มากที่สุด โดยอาศัยความหลากหลายของเส้นทางที่โหนดผู้ส่งนั้นเคยส่งข้อมูลไป เพื่อที่จะสร้างทอพอโลยีที่ใกล้เคียงความสมบูรณ์ที่สุดที่จะสามารถนำมาใช้ให้เกิดประโยชน์และเพียงพอต่อการหากราฟไมเนอร์ ซึ่งในงานวิจัยนี้ผู้วิจัยได้ตั้งสมมติฐานว่าโหนดผู้ส่งนั้นทราบเส้นทางในการส่งข้อมูล รวมถึงทราบทอพอโลยีทั้งหมดที่ได้สร้างไว้แล้ว

ในส่วนรหัสเครือข่ายเชิงระบบนั้นยังคงมีปัญหาปลายเปิดสำหรับการหาค่า c ที่เหมาะสมในการสร้างรหัสเพื่อใช้ในการส่ง และความเป็นอิสระเชิงเส้นในเมทริกซ์ต้นกำเนิด ซึ่งในมุมมองของรหัสแอลที่คือการสร้างรหัสที่เกิดจากการสุ่มโดยสมบูรณ์ อย่างไรก็ตามในมุมมองของผู้วิจัยคือการส่งข้อมูลที่มีความซ้ำซ้อน ถึงแม้ว่าการสร้างความสัมพันธ์เชิงระบบด้วยกรรมวิธีการกำจัดแบบเกาส์เซียนจะช่วยขจัดปัญหาเหล่านี้ออกไปแต่ก็ยังไม่สมบูรณ์ โดยการแก้ไขเบื้องต้นคือ การนำกระบวนการตรวจสอบความเป็นอิสระเชิงเส้นมาตรวจสอบเมทริกซ์ต้นกำเนิดที่อยู่ในรูปเชิงระบบก่อนที่จะนำไปเข้ารหัส แต่ผลที่ตามมาคือเวลาแฝงที่เพิ่มขึ้นอย่างมากในการสร้างรหัสโดยรวม

เอกสารอ้างอิง

- [1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," **IEEE Transactions on Information Theory**, vol.46, no. 4, 2000, pp. 1204–1216.
- [2] Y. Wu, P.A. Chou, and S.-Y. Kung, "Information exchange in wireless networks with network coding and physical-layer broadcast," in **Proc. of 39th Ann. Conf. Inform. Sci. Syst.**, Baltimore, MD, USA, Mar. 2005.
- [3] D. D. Couto, D. Aguayo, J. Bicket and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," in **Proc. of ACM MOBICOM '03**, New York, USA, Sept. 2003, pp. 134-146.
- [4] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard and J. Crowcroft, "XORs in the air: Practical wireless network coding," **IEEE/ACM Transactions on Networking**, vol. 16, no. 3, 2008, pp. 497–510.
- [5] M. Médard and A. Sprintson, **Network Coding Fundamentals and Applications**, Academic Press., 2012.
- [6] G. S. Paschos, C. Fragiadakis, L. Georgiadis and L. Tassiulas, "Wireless network coding with partial overhearing information," in **Proc. of IEEE INFOCOM**, Turin, Italy, Apr. 2013, pp. 2337–2345.
- [7] R. Koetter and M. Médard, "An algebraic approach to network coding," **IEEE/ACM Transactions on Networking**, vol. 11, no. 5, 2003, pp. 782–795.
- [8] S. Y. R. Li, R. W. Yeung and N. Cai, "Linear network coding" **IEEE Transactions on Information Theory**, vol. 49, no. 2, 2003, pp. 371–381.
- [9] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and Lmga Tolhuizen, "Polynomial time algorithms for multicast network code construction," in **IEEE Transactions on Information Theory**, vol. 51, no. 6, 2005, pp. 1973–1982.
- [10] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi and B. Leong, "A random linear network coding approach to multicast," in **IEEE Transactions on Information Theory**, vol. 52, no. 10, 2006, pp. 4413–4430.
- [11] M. Luby, "LT codes," in **Proceeding of the 43rd Annual IEEE Symposium on Foundations of Computer Science**, Nov. 2002, pp. 271–282.
- [12] W. Dargie and Christian Poellabauer, **Fundamentals of Wireless Sensor Networks Theory and Practice**, WILEY. 2010.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารอ้างอิง (ต่อ)

- [13] I. D. Chakeres and E. M. Belding-Royer, "AODV routing protocol implementation Design," in *Proc. of 24th IEEE Inter. Conference.*, Mar. 2004, pp. 698-703.
- [14] S. J. Lee and M. Gerla, "AODV-BR: Backup routing in ad hoc networks," in *Proc. of Wireless Communications and Networking Conference (WCNC).*, vol. 3, Sep. 2000, pp. 1311-1316.
- [15] R. Diestel, *Graph Theory.*, Springer-Verlag., 1997.
- [16] T. Ho, M. Médard, J. Shi, M. Effros and D. R. Karger, "On randomized network coding," in *Proc. of the Annual Allerton Conference on Communication Control and Computing.*, Vol. 41, No. 1, 2003.
- [17] J. Barat and G. Joret, "Disproof of the list hadwiger conjecture," *The Electronic Journal of Combinatorics.*, vol. 18, Dec. 2011, pp. 232-238.
- [18] B. Bollob as, P. A. Catlin and P. Erdos, "Hadwiger's conjecture is true for almost every graph," *European Journal of Combinatorics.*, vol. 1, 1980, pp. 195-199.
- [19] N. Robertson, P. Seymour and R. Thomas, "Hadwiger's conjecture for k_6 -free graphs," *Combinatorica.*, vol. 14, 1993, pp. 279-361.
- [20] A. Kostochka, "Lower bound of the hadwiger number of graphs by their average degree," *Combinatorica.*, vol. 4, 1984, pp. 307-316.
- [21] N. Robertson and P. Seymour, "Graph minors .xiii. the disjoint paths problem," *Journal of Combinatorial Theory. Series B.*, vol. 63, no. 1, 1995, pp. 65-110.
- [22] X. Yin, Y. Wang, X. Wang, X. Xue, and Z. Li, "A graph minor perspective to network coding: Connecting algebraic coding with network topologies," in *Proc. of INFOCOM.*, Apr. 2013, pp. 2364-2372.
- [23] S. Maheshwar, Z. Li and B. Li, "Bounding the coding advantage of combination network coding in undirected networks," in *IEEE Transactions on Information Theory.*, vol. 58, no. 02, Feb. 2012, pp. 570-584.
- [24] C. Chekuri, C. Fragouli and E. Soljanin, "On average throughput and alphabet size in network coding," in *IEEE Transactions on Information Theory.*, vol. 52, no. 6, Jun. 2006, pp. 2410-2424.
- [25] C. Fragouli and E. Soljanin, "Information flow decomposition for network coding," in *IEEE Transactions on Information Theory.*, vol. 52, no. 3, Mar. 2006, pp. 829-848.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เอกสารอ้างอิง (ต่อ)

- [26] D.J.C Mackay, "Fountain Codes," **Capacity Approaching Codes Design and Implementation Special Section IEEE Proceeding.**, no. 20050237. May. 2005.
[Online]. Available : <https://www.ma.utexas.edu/users/voloch/Homework/MacKay05.pdf>
- [27] T. D. Nguyen, L. L. Yang and L. Hanzo, "Systematic Luby transform codes and their soft decoding," **IEEE Signal Processing Systems '07.**, Shanghai, China, Oct. 2007, pp. 67-72.
- [28] V. H. Tran, K.-T. Lay and L.-C. Peng, "Modified LT Coding with Systematic Connections," in **Anti-Counterfeiting, Security and Identification (ASID).**, Taipei, 2012, pp. 1-4.
- [29] N. Muangboonma, N. Puttarak and P. Kaewprapha, "The Adaptive Network Coding-Routing (ANCR) Based on Graph for Multicast Networks," **Applied Mechanics and Materials.**, vol. 781, no. 70, 2015, pp. 36-40.
- [30] M. Lu, P. Steenkiste and T. Chen, "Design, Implementation and Evaluation of an Efficient Opportunistic Retransmission Protocol," in **Proc. of ACM MOBICOM '09.**, Beijing, China, 2009, pp 73-84.
- [31] R. Draves, J. Padhye, and B. Zill., "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks," in **Proc. of ACM MOBICOM '04.** New York, USA, Sept. 2004, pp. 114-128.
- [32] N. Muangboonma, N. Puttarak and P. Kaewprapha, "Latency-reduced Retransmission in Multicast Network using Systematic Network code," in **Proc. of International Conference on Electronics, Information and Communication (ICEIC).**, Da Nang, Vietnam, Feb. 2016, pp. 56-59.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ก.1 MATLAB Source code ของอัลกอริธึม ANCR

ก.1.1 MATLAB Source code ในการประกาศตัวแปรและค่าเริ่มต้น

```

%Main Setup -----
clc;clear;
%Main console and Global varriable
pk_per_turn=2;
pk_size =2000000;
loops =10000 ;
%Channel characterize
snr =4.5 ;%fixed SNR
    No =1/(10^(snr/10));
    var =No/2;
    sigma =sqrt(var);
%Topology Setup -----
con_tab =[0 1 0 1 0 0 0 ;
          1 0 1 0 0 1 0 ;
          0 1 0 1 1 0 0 ;
          1 0 1 0 0 0 1 ;
          0 0 1 0 0 1 1 ;
          0 1 0 0 1 0 1 ;
          0 0 0 1 1 1 0];
%Node Setup -----
n1 =myRouter_v2('n1',1,'Source',[2 4]); %rID,rStatus,neighborSet)
n2 =myRouter_v2('n2',2,'R',[1 3 6]);
n3 =myRouter_v2('n3',3,'R',[2 4 5]);
n4 =myRouter_v2('n4',4,'R',[1 3 7]);
n5 =myRouter_v2('n5',5,'R',[3 6 7]);
n6 =myRouter_v2('n6',6,'Sink',[2 5]);
n7 =myRouter_v2('n7',7,'Sink',[4 5]);
routersLinkList(1)=n1;
routersLinkList(2)=n2;
routersLinkList(3)=n3;
routersLinkList(4)=n4;
routersLinkList(5)=n5;
routersLinkList(6)=n6;
routersLinkList(7)=n7;

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ก.1.2 MATLAB Source code ในการสร้างเหตุการณ์แบบสุ่มรวมถึงหาเส้นทาง

```

fprintf ('\n ##1.Create sending event ----- \n')
[sending_pair]=create_event_by_classRouterSet_v001b (routersLinkList,
pk_per_turn,'on');
fprintf ('\n ##2.Calculate all possible Fwd Paths ----- \n')
path_per_turn =get_dataFlow_v001b(sending_pair,routersLinkList , 0);
fprintf ('\n ##3.Initialize Packet ----- \n')
for i =1 :pk_per_turn
    temp_pair =sending_pair(i,:);
    packet(i)pk_ID =i;
    packet(i)pk_Type = 'Norm';
    packet(i).source =temp_pair(1);
    packet(i).sink =temp_pair(2);
    packet(i).fwd_path =[];
    packet(i).data =randi([0 1],1,pk_size);
    packet(i).x_pid =[];
    packet(i).x_src =[];
    packet(i).x_dst =[];
    packet(i).x_data =[];
    packet(i);
end

```

ก.1.2.1 MATLAB Source code ฟังก์ชันที่ใช้ในการสร้างเหตุการณ์แบบสุ่ม

```

function [sending_pair]=create_event_by_classRouterSet_v001b(
routerClassSet , numPacket , report_on_off)
%Get "Source" Type form routerClassSet
source_IdSet =[];
for i =1 :length(routerClassSet)
    if strcmp(routerClassSet(i).rStatus , 'Source')==1
        source_IdSet =[source_IdSet routerClassSet(i).rID];
    end
end
%Get "Sink" Type form routerClassSet
sink_IdSet =[];
for i =1 :length(routerClassSet)
    if strcmp(routerClassSet(i).rStatus , 'Sink')==1
        sink_IdSet =[sink_IdSet routerClassSet(i).rID];
    end
end
sending_pair =[];
%pick source type
for i =1 :numPacket
    source_ranID =source_IdSet(randi(numel(source_IdSet)));

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

sink_ranID =sink_IdSet(randi(numel(sink_IdSet)));
sending_pair =[sending_pair ; source_ranID sink_ranID];
end
%show_report
rep = '';
[m,n]=size(sending_pair);

if report_on_off == 'on'
    rep = '\n Event Report : \n';
    for i = 1 :m
        e =sending_pair(i,:);
        strbuff =['\t N ',num2str(e(1)), ' ---> N ',num2str(e(2)), '\n'];
        rep =[rep strbuff ];
    end
    fprintf('\n' , rep , '\n');
elseif report_on_off == 'off'
    rep = '';
end
end

```

ก.1.2.2 MATLAB Source code ของฟังก์ชันที่ใช้ในการหาทิศทางการไหลของข้อมูลที่เป็นไปได้ทั้งหมดจากโหนดผู้ส่งจนถึงโหนดผู้รับ

```

function [All_path_per_turn]=get_dataFlow_v001b(sending_pair,routerClassSet, show_path)
All_path_per_turn = [];
[pair_row , ~]=size(sending_pair);
for p = 1 :pair_row %ดูทีละคู่ ไม่ต้องสนใจ
    pair =sending_pair(p,:); %ย้ายมาเก็บไว้ในตัวแปร pair
    source_ID =pair(1); %ตัวแรกของ pair
    sink_ID =pair(2); %ตัวที่สองของ pair
%-----
for r = 1 :length(routerClassSet)%ทุก myRouter
    rID =routerClassSet(r).rID; %ตัวที่จะนำมาเทียบกับ source_ID
    if rID == source_ID
        %พอมาถึงตรงนี้จะเป็นการเจอ myRouter ตัวที่เป็น Source
        %กรณี 1 สามารถเชื่อมต่อได้โดยตรง (ไม่ต้องหา path สำรอง)
        if ismember(sink_ID,routerClassSet(r).neighborSet)
            path =[source_ID sink_ID];
            All_path_per_turn =[All_path_per_turn ;{path}];
        %กรณี 2 ไม่เชื่อมต่อได้โดยตรง
        else
            %root_level
            root_Obj =search_myrouter_byRID(source_ID ,routerClassSet);
            %intermediate node level
            %กรณีที่ 2.1 ถ้าหากNeighbor ของ root มีมากกว่า 1 ตัว
            if length(root_Obj.neighborSet)> 1
                [~, N]=size(root_Obj.neighborSet);
                %Scan ทีละ Neighbor
            end
        end
    end
end
end

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

for i =1 :n
%intermediate node object (ตัวที่ i)
    fwd_node_obj = search_myrouter_byRID
(root_Obj.neighborSet(i),routerClassSet);
%ถ้าหากNeighbor ของ intermediate node เจอ
%Sink พอดี(2 Hops Arrived)
    if sum(ismember(fwd_node_obj.neighborSet , sink_ID))==1
        path =[source_ID fwd_node_obj.rID sink_ID];
        All_path_per_turn =[All_path_per_turn ;{path}];

%และหาPath สำรอง
%หาfwd_source
%scan loop
        nb_temp = fwd_node_obj.neighborSet;
        for i =1 :length(nb_temp)
            nb_temp_obj =
search_myrouter_byRID(nb_temp(i), routerClassSet);
            if (nb_temp_obj.rStatus == 'R')
                fwd_source =nb_temp_obj
            end
        end
%Recursion Call
        fwd_sending pair =[fwd_source.rID sink_ID];
        fwd_path =get_dataFlow_v001b_recursion
(fwd_sending_pair,routerClassSet ,show_path );
%เอาเส้นทางย้อนออก
        temp_fwd_path =[];
        for i =1 :length(fwd_path)
            if ~ismember(fwd_node_obj.rID ,fwd_path{i}(2:end))
                temp_fwd_path =[temp_fwd_path ;
{fwd_path{i}}];
            end
        end
        fwd_path =temp_fwd_path;
%union new path
        temp_path =[source_ID fwd_node_obj.rID];
        for i =1 :length(fwd_path)
            add_path=
non_ordering_union(temp_path,fwd_path{i});
            All_path_per_turn =[All_path_per_turn
;{add_path}];
        end
    else %ไม่ถึงSinkพอดี(non 2 Hops Arrived)
        temp_path =[source_ID fwd_node_obj.rID];
%หาfwd_source
        nb_temp = fwd_node_obj.neighborSet;
        for i =1 :length(nb_temp)
            nb_temp_obj =search_myrouter_byRID
(nb_temp(i),routerClassSet);
            if (nb_temp_obj.rStatus == 'R')

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้


```

                                fwd_path = temp_fwd_path
%union new path
                                temp_path =[source_ID fwd_node_obj.rID];
                                for i =1 :length(fwd_path)
                                    add_path =
non_ordering_union(temp_path,fwd_path{i});
                                All_path_per_turn =[All_path_per_turn;{add_path}];
                                end
                                else
                                    temp_path =[source_ID fwd_node_obj.rID];
                                    nb_temp = fwd_node_obj.neighborSet;
                                    for i =1 :length(nb_temp)
                                        nb_temp_obj = search_myrouter_byRID
(nb_temp(i),routerClassSet);
                                        if (nb_temp_obj.rStatus == 'R')
                                            fwd_source = nb_temp_obj;
                                        end
                                        end
                                        fwd_sending_pair =[fwd_source.rID sink_ID]
                                        fwd_path = get_dataFlow_v001b_recursion
(fwd_sending_pair,routerClassSet , show_path);
                                %union new path
                                    for i =1 :length(fwd_path)
                                        path =
non_ordering_union(temp_path,fwd_path{i});
                                        All_path_per_turn =[All_path_per_turn
;{path}];
                                    end
                                end
                                end
                                end
                                end
                                end
                                %-----
                                All_path_per_turn =[All_path_per_turn ;{[0 0 0 0]}];
                                end
                                end%end function

```

ก.1.3 MATLAB Source code ที่ใช้ในการจัดการเส้นทางให้กับแต่ละแพ็กเก็ตเกิดเป็นค่าเริ่มต้น ก่อนที่จะนำไปตัดสินใจว่าเพียงพอที่จะนำมาทำการเข้ารหัสเครือข่ายหรือไม่

```

%+++++
fprintf('\n ##4.Pair to the Paths ----- \n')
%Packet ID pair with path_per_turn
All_pkID_n_Paths = [];
pk_iD_index = 1 ;
for i =1 :length(path_per_turn)
    if sum(path_per_turn{i})~=0

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

        temp_path =path_per_turn{i};
        All_pkID_n_Paths =[All_pkID_n_Paths ; {pk_iD_index} {temp_path}];
    else
        pk_iD_index =pk_iD_index +1;
    end
end
end
%Matrix var
%to Table Var
    raw_pkID_n_Paths_table =pkID2Paths_to_Table_v003rt(All_pkID_n_Paths);
%Choose 1 form 2 paths (1.Main 2.Alternate)
    sorted_Paths_table =selectpath_form_tab_v003rt_nc(packet,
raw_pkID_n_Paths_table );
%group by Pid
    table =collapse_by_pID_v003rt_nc(sorted_Paths_table );
%+++++
    fprintf('\n ##5.Assign path (Rand)to packet ----- \n')
%By Random all possible path
    for p =1 :length(packet)
        pID =packet(p).pk_ID;
    [sm,sn]=size(table);
        for sp =1 :sm
            T_pID =table.T_pID{sp};
            if pID ~=T_pID
                assign_path =table.T_travelPath{sp};
                rand_path_index =randi(numel(assign_path));
                assign_path =assign_path(rand_path_index);
                fprintf('\n \t Packet ID : ' num2str(pID) ' path = '
mat2str(assign_path) '\n');
                packet(p).fwd_path = assign_path;
            end
        end
    end
end
end

```

ก.1.4 MATLAB Source code ที่ใช้ในการควมรวมทิศทางการหดตัวของกราฟ พร้อมทั้งตรวจสอบคุณสมบัติของกราฟไมเนอรัที่ได้ และกำหนดลักษณะของเพ็คเกจถ้าหากมีความเพียงพอในการเข้ารหัส

```

%+++++
fprintf('\n ##6.Network coding Opportunity ----- \n')
%%check_NC_Oppportunity
[NC_flag ]=check_NC_Oppportunity_v003nc(packet , pk_per_turn );
k4_flag =0;
routing =0;
if NC_flag ==1
    fprintf('\n #####6.Awith NC Opportunity ----- \n')
    %Prepare
    raw_pkID_n_Paths_table;

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

sorted_Paths_table =
selectpath_form_tab_v003rt_nc(packet,raw_pkID_n_Paths_table);
table =collapse_by_pID_v003rt_nc(sorted_Paths_table );
%Decomposition and Combine minor from 2 flows
graphs =decomposition_per_pID_v001c(table , routersLinkList);
joint_graph_minors =xor_graphs_v003nc(graphs );

%K4_checker
k4_flag =k4minors_checker_v003nc(joint_graph_minors ,
routersLinkList);
if k4_flag ==0
break
end
if k4_flag ==1 %add joint_graph_minors' properties
x_graph_minors =add_minors_properties(joint_graph_minors ,
routersLinkList)
%assign XOR properties to packet
for i =1 :length(x_graph_minors.minors)
C =x_graph_minors.minors(i).clique;
P =x_graph_minors.minors(i).property;
if strcmp(P , 'COOP')
for pk =1 :length(packet)
packet(pk).pk_Type = 'Xor'
packet(pk).x_node ={C};
end
end
end
end
end
end
%.Network Coding ..
else
routing =-1;
%Sending by normal routing
fprintf('\n #####6-B.No Opportunity , Doing Routing-----\n')end
if k4_flag ==0 && routing ==0
fprintf('\n #####6-C.Not K4 , Doing Routing-----\n')
end
end

```

ก.1.5 MATLAB Source code ที่ใช้ในการส่งแพ็กเก็ต

```

fprintf('\n ##7.Forward packets by the Path -----\n')
while 1
for sender =1 :length(routersLinkList)
if ~isempty(routersLinkList(sender).sendingQueue)
routersLinkList(sender).rName;
routersLinkList(sender).sendingQueue;
for sender_packet =1 :length(routersLinkList(sender).sendingQueue)
%ส่ง
routersLinkList(sender).sendingQueue(sender_packet);

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

        message = routersLinkList(sender)
        .sendingQueue(sender_packet);
        fwd_path = routersLinkList(sender)
        .sendingQueue(sender_packet).fwd_path;
        routersLinkList(sender).numberPKsent =
            routersLinkList(sender).numberPKsent + 1;
        if length(fwd_path) > 1 %แสดงว่ายังไม่จบผู้รับ
            reveiver_ID = fwd_path(1); %Head of fwd_path
            fprintf('\n \t \t Packet ID : ' num2str(message.pk_ID) ' Passed @Node : '
            num2str(reveiver_ID) '\n')
            new_fwd_path = fwd_path(fwd_path ~= reveiver_ID);
            %Dequeue
            %sending to message to receiver
            message.fwd_path = new_fwd_path;
            %AWGN CH
            [new_data , tp]=to_AWGNch_v001rt(message.data, sigma);
            message.data = new_data;
            routersLinkList(reveiver_ID).sendingQueue =
[routersLinkList(reveiver_ID).sendingQueue message];
            %รับ
            %Add TP record
            for nonR = 1 : length(routersLinkList)
                if reveiver_ID == routersLinkList(nonR).rID
                    routersLinkList(nonR).throughputRec =
[routersLinkList(nonR).throughputRec 0];
                else
                    routersLinkList(reveiver_ID).throughputRec =
= [routersLinkList(reveiver_ID).throughputRec tp];
                    routersLinkList(reveiver_ID).numberPKreceived =
routersLinkList(reveiver_ID).numberPKreceived + 1;
                end
            end
        end
    end
end

```

ก.1.6 MATLAB Source code ฟังก์ชันที่ใช้ในการหัดตัวของกราฟ

```

function [graphs]=decomposition_per_pID_v001c(tab , routerClassSet )
[tm,tn]=size (tab);
for i_tab =1 :tm
    pID =tab(i_tab, :).T_pID{1};
    %Add pID
    graphs (pID).pID =pID;
    ind_flows =tab (i_tab, :).T_fullPath {1};
    %Add flows
    graphs (pID).flows =ind_flows;
    ind_graph_properties =adding_graph_properties_v001d(ind_flows,
routerClassSet);
    %Minor process
    c =1;

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

for f = 1:length(ind_flows)
    flow = ind_flows{f};
    pair = get_pairSet_from_flow_v001c(flow );
%check every pair
    for p = 1:length(pair)
        the_pair = pair(p);
        pair_A = the_pair(1);
        pair_B = the_pair(2);
        graph_pair_B = search_graph_bygID(pair_B,
ind_graph_properties);
        Outdeg_B = graph_pair_B.OutDeg_set;

        if length(Outdeg_B) == 1
            pair_C = Outdeg_B;
            if flowend == pair_C
                %fprintf(' \n Sink found!!! \n')
                minors(c).clique = [pair_A pair_B pair_C];
                c = c + 1;
            else
                decomposition_Lv0 = the_pair;
                decomposition_Lv1 = [pair_A pair_B pair_C];
                Critical_node = search_graph_bygID
(pair_C, ind_graph_properties);
                if Critical_node.OutDeg == 1
                    minors(c).clique = decomposition_Lv0;
                    c = c + 1;
                else
                    minors(c).clique = decomposition_Lv1;
                end
            end
        end
    end
end
end
graphs (pID).minors = minors;
end
end

```

ก.1.7 MATLAB Source code ฟังก์ชันที่ใช้ในการตรวจสอบคุณสมบัติไมเนอร์ K_4 ภายในทอพอโลยี

```

function [flag ] = k4minors_checker_v003nc(x_paths_graph_minors,
routersLinkList)
    flag = 0 ;
    if length(x_paths_graph_minors.minors) == 4
        main_check_flag = [];

        for i = 1 : 4

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

for j = 1 : 4
    if i < j
        A = x_paths_graph_minors.minors(i).clique;
        B = x_paths_graph_minors.minors(j).clique;
%LV_1 checking
        if sum(ismember(A,B))>=1 || sum(ismember(B,A))>=1
            main_check_flag = (main_check_flag 1);
        else
%LV_2 checking
            LV2_check_flag = [];
            for k = 1 : length(A)
                R_Obj = search_myrouter_byRID(A(k), routersLinkList);
                C = R_Obj.neighborSet;

                if sum(ismember(C,B))>=1 || sum(ismember(B,C))>=1
                    LV2_check_flag = (LV2_check_flag 1);
                else
                    LV2_check_flag = (LV2_check_flag 0);
                end
            end
            if sum(LV2_check_flag)>=1
                main_check_flag = (main_check_flag 1);
            else
                main_check_flag = (main_check_flag 0);
            end
        end
    end
end
else
    flag = 0 ; %จำนวนไมเนอร์ ~ 4
end
[k i]=find(main_check_flag == 0);
if isempty(k)
    flag = 1 ;
end
end
end

```

ก.1.8 MATLAB Source codeในส่วนของการแสดงผลและประเมินประสิทธิภาพด้วยกราฟ

```

load('rt_data.mat')%Routing only
rt_ts_cumsum = cumsum(rt_timeslot_usage);
load('ancr_data.mat')%Routing only
nc_avg_tp_rec
nc_avg_ts_rec
nc_max_ts_rec
nc_timeslot_usage
nc_ts_cumsum = cumsum(nc_timeslot_usage);
%Time slots comparision
x_max = [rt_max_ts_rec nc_max_ts_rec];

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

x_avg =[rt_avg_ts_rec nc_avg_ts_rec];
y =[1 2];
combine_x =[x_max ; x_avg];
figure;
bar(y , combine_x , 'grouped')
set(gca, 'Xtick', 1:4, 'XTickLabel', {'Routing', 'ANCR', ''})
legend('Max Timeslots usage', 'AVG timeslots usage')
ylabel('Timeslot usage (times)');
title('Timeslot usage of ANCR and Routing Transmission');
grid on;

%-----
%Actual Throughput
print_node_set =[3 7];
for i =1 :length(print_node_set)
    subplot(length(print_node_set),1,i)
    target =print_node_set(i);
    x1_axis =1:length(rt_routersLinkList(target).throughputRec);
    y1_axis =(1/10e6).*rt_routersLinkList(target).throughputRec(1:end);
    x2_axis =1:length(nc_routersLinkList(target).throughputRec);
    y2_axis =nc_routersLinkList(target).throughputRec(1:end);
    L_rt =length(rt_routersLinkList(target).throughputRec(1:end));
    L_nc =length(nc_routersLinkList(target).throughputRec(1:end));
    diffL =abs(L_rt -L_nc);
    append_data =zeros(1,diffL);
    new_y2_axis =(1/10e6).*y2_axis +append_data;
    plot(x1_axis , new_y2_axis , x1_axis , y1_axis , 'r' , 'LineWidth', 2 )
    if routersLinkList(target).rID == 3
        legend('ANCR throughput', 'AODV Throughput')%add legend
        title('Actual Throughput at bottleneck node :
',int2str(routersLinkList(target).rID))
        ylabel('Throughput(Mbps)');
        xlabel('Timeslot (t)');
    elseif routersLinkList(target).rID == 7
        legend('ANCR throughput', 'AODV Throughput')%add legend
        title('Actual Throughput at sink node such as:
',int2str(routersLinkList(target).rID))
        ylabel('Throughput(Mbps)');
        xlabel('Timeslot (t)');
    end
    grid on;
end
%throughput compare
x_rt =[rt_avg_tp_rec{1,2} rt_avg_tp_rec{2,2} rt_avg_tp_rec{3,2}];
x_nc =[nc_avg_tp_rec{1,2} nc_avg_tp_rec{2,2} nc_avg_tp_rec{3,2}];
y =[1 2 3];
figure;
tp_x =(1/10e6).*[x_rt' x_nc']

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

bar(y , tp_x , 'grouped')
legend('Max Throughput (Mbps)', 'AVG Throughput (Mbps)' , 'Location',
'NorthWest' )
set(gca, 'Xtick', 1:5, 'XTickLabel', {'Node 3', 'Node 6', 'Node 7' , ''})
ylabel('Throughput (Mbps)');
grid on;

```



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ก.2 MATLAB Source code ของรหัสเครือข่ายเชิงระบบ

ก.2.1 MATLAB Source code เพื่อใช้ในการแสดงการกระจายตัวแบบโซลิตอน และโรบัสต์โซลิตอน

```

%Character -----
%k =number of Input symbols
%K =number of Encoding symbols
%delta =failure probability of the decoder to recover data for a given a
% number of K of encoding symbols.
%mu[]=Robust soliton distribution
%R =c*sqrt(k)*log(kdelta)
%Initialize -----
delta = 1; %100 percent
c = 1;
k = 100;
plot = 1;
R = c*sqrt(k)*log(kdelta);
tau = zeros(1,k);
    l1 = ceil((k/R)-1);
    l2 = ceil(k/R);
    l3 = ceil((k/R)+1);
for i = 1 :k
    if i<=l1
        tau(i)=R*(k-i);
    elseif i ==l2
        tau(i)=(R/k)*log(Rdelta);
    else
        tau(i)=0;
    end
end
end
%Rho -----
%from Ideal soliton distribution
rho = zeros(1,k);
for i = 1 :length(rho)
    if i ==1
        rho(i)= 1/k;
    else
        rho(i)= 1/(i*(i-1));
    end
end
end
%Rho -----
beta = sum(tau + rho);
mu = (tau + rho)/beta;
sum(mu)
%-----
if plot = 1
    figure;
    stem(1:k,mu , 'r' , 'LineWidth' , 3)
    hold on
    stem(1:k,rho , 'g' , 'LineWidth' , 2)

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

hold off
grid on
legend('Robust soliton distribution with c = ' , num2str(c), ...
      ', delta = ' num2str(delta)], 'Ideal Soliton distribution', ...
      'Location', 'Northeast')
end

```

ก.2.2 MATLAB Source code เพื่อใช้ในการวิเคราะห์ค่าตัวแปรที่เหมาะสมของการกระจายแบบโรบัสต์โซลิตอน

```

%Character -----
%k =number of Inbut symbols
%K =number of Encoding symbols
%delta =failure probability of the decoder to recover data for a given a
% number of K of encoding symbols.
%mu[]=Robust soliton distribution
%R =c*sqrt(k)*log(kdelta)
%Initialize -----
delta =0.1 ;
k =1000; %input symbols
K =1500;
%-----
end_c =1;
c =0.1; %start c
step_size =0.1;
avgloop =50;
K_collector =[];
sumDeg_collector =[];
c_collector =[];
percent_collector =[];
for ii =c :step_size :end_c
    c_collector =[c_collector c];
    avg_sum_collector =[];
    avg_K_collector =[];
    for avg =1 :avgloop
        [mu , rho , ~ , ~]=robust_Soliton_Dist_Fn_03(delta , c , k);
        avg_K_collector =[avg_K_collector K];
        ideal_degVector =randsample(k,k,true,rho);
        robust_degVector =randsample(k,k,true,mu);
        avg_sum_collector =[avg_sum_collector sum(robust_degVector)];
    end
    sumDeg_collector =[sumDeg_collector sum(avg_sum_collector)/avgloop];
    K_collector =[K_collector sum(avg_K_collector)/avgloop];
end
figure;
stem(c_collector,K_collector , 'r' , 'LineWidth' , 3)
hold on
stem(c_collector,sumDeg_collector , 'b' , 'LineWidth' , 2)
hold off
legend('Encoding symbols', 'Sum of Deg', 'Location', 'Northeast')
grid on
xlabel('c value')

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
ylabel('Number of Degree and Encoding Symbols')
```

ก.2.3 MATLAB Source code ฟังก์ชันที่ใช้ในการเข้ารหัสแวลทีและรหัสแวลทีเชิงระบบ

```
function [LTgenMx_Input_Location , lim_exceed_flag]=fn_robustLTencoder_v03(k ,
robust_degVector , K , linLimit , textOn)
count_linLimit =0;
lim_exceed_flag =0;
while(1)
    cov_encSymb = [];
    uncov_encSymb =[1:K];
    protected_covEncSyms = [];
    LTgenMx_Input_Location = zeros(k,K);
    deg_1 =find(robust_degVector ==1);
    for i =1 :length(deg_1)
        random_encPositon =uncov_encSymb(randi(numel(uncov_encSymb)));
        cov_encSymb =sort((cov_encSymb random_encPositon));
        uncov_encSymb =setdiff(uncov_encSymb , cov_encSymb);
        LTgenMx_Input_Location(deg_1(i) , random_encPositon)=1;
    end
    cov_encSymb;
    protected_covEncSyms =cov_encSymb;
    uncov_encSymb;
    LTgenMx_Input_Location;
    protected_covEncSyms;
    unprotected_covEncSyms =setdiff(1:K) , protected_covEncSyms;
    deg_n =find(robust_degVector ~=1);
    for i =1 :length(deg_n)
        deg_n(i);
        deg_val =robust_degVector(deg_n(i));
        for j =1 :deg_val
            if ~isempty(uncov_encSymb)
                random_encPositon =uncov_encSymb(randi(numel(uncov_encSymb)));
                if ismember(random_encPositon , protected_covEncSyms)
                    while(~ismember(random_encPositon ,
protected_covEncSyms))
                        random_encPositon =
uncov_encSymb(randi(numel(uncov_encSymb)));
                    end
                end
                cov_encSymb =sort((cov_encSymb random_encPositon));
                uncov_encSymb =setdiff(uncov_encSymb , cov_encSymb);
            else
                random_encPositon =
unprotected_covEncSyms(randi(numel(unprotected_covEncSyms)));
            end
            LTgenMx_Input_Location(deg_n(i) , random_encPositon)=deg_n(i);
        end
    end
    end
    %Verify process
    Mx =LTgenMx_Input_Location > 0;
    A =~isempty(find(sum(Mx)=1));
    if A
        %S =linearity_Indy_Check(Mx , textOn);
    end
end
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้


```

        decode_flag = 0;
        if recover_erasure_flg == 1
%recovery process
            recov_syms = intersect(erasure_eq , erasure_knw_syms);

            recov_data = 0;
            for rrr = 1 :length(recov_syms)
                recov_data =xor(recov_data , Dec_syms(recov_syms(rrr)));
            end
            erasure_enc_syms(rx_enc)=recov_data;
%*****
            decode_flag = 1 ;
        end
    end
%+-----+
    if decode_flag == 1
        pending_Dec_syms_mkr =Dec_syms_mkr;
        pending_Dec_syms      =Dec_syms;
        enc_eq =find(LT_Gen_Mat(:,rx_enc)==1)';
        enc_deg =sum(enc_eq );
        Enc_syms_mkr(rx_enc)=(rx_enc); %Update Marker
        if enc_deg == 1
            if t == 1
                fprintf('\n\t==>S.Decodable Obtain dec symb : ' , num2str(enc_eq))
            end
            pending_Dec_syms_mkr(enc_eq)=enc_eq;
            pending_Dec_syms(enc_eq) = erasure_enc_syms(rx_enc);
%+-----+
        else
%By Knowing
            knw_syms =find(pending_Dec_syms_mkr >= 0);
            knw_chk =setdiff(enc_eq,knw_syms); %equation ที่ประกอบด้วย symb ใดก็ได้ที่รู้มาก่อนแล้ว
            if t == 1
                fprintf('\n\tEncoding Syms combination : ' , mat2str(enc_eq) , ...
                    ' +by Knowing dec symb : ' , mat2str(knw_syms))
            end

            if numel(knw_chk)== 1
%Decode
                if t == 1
                    fprintf('\n\t==>KS.Decodable Obtain dec symb : ' , num2str(knw_chk) )
                end
                pending_Dec_syms_mkr(knw_chk)=knw_chk;
                tempX =k_xor_v1(enc_eq , knw_syms , pending_Dec_syms);
                pending_Dec_syms(knw_chk)=xor(erasure_enc_syms(rx_enc),tempX);
            end
            Lookback_eq_col =find(Enc_syms_mkr > 0);
            for lb = 1 :length(Lookback_eq_col)
                lb;
                enc_eq;
                ext_eq =find(LT_Gen_Mat(:,Lookback_eq_col(lb))==1)';

                ext_chk =k_setdiff_v01(enc_eq , ext_eq);
                if t == 1
                    fprintf('\n\tEncoding Syms combination : ' , mat2str(enc_eq) , ...
                        ' +Encoding Syms combination : ' , mat2str(ext_eq))
                end
                if numel(ext_chk)== 1

                    if t == 1
                        fprintf('\n\t==>ES.Decodable Obtain dec symb : ' , num2str(ext_chk));

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

end

    pending_Dec_syms_mkr(ext_chk)=ext_chk;
    pending_Dec_syms(ext_chk)=xor(erasure_enc_syms(irx_enc),
erasure_enc_syms(Lookback_eq_col(lb)));
end
end
end
Dec_syms_mkr;
pending_Dec_syms_mkr;
Dec_syms;
pending_Dec_syms;
update_Num =sum(Dec_syms_mkr ~=pending_Dec_syms_mkr);
update_syms =find(Dec_syms_mkr ~=pending_Dec_syms_mkr > 0);
if t ==1
fprintf('\nUpdate : ' , num2str(update_Num), ...
        ' syms , : ' , mat2str(update_syms), '\n')
end
%Update For Next Process
Dec_syms_mkr =pending_Dec_syms_mkr;
Dec_syms      =pending_Dec_syms;
if update_Num > 0
sb_loop =0;
while(update_Num ~=0)
sb_loop =sb_loop +1;
if t ==1
fprintf('\n ScanBack process ' , num2str(sb_loop))
end
%ScanBack Process
pending_Dec_syms_mkr =Dec_syms_mkr;
pending_Dec_syms      =Dec_syms;
%Just refresh Knw syms
knw_syms =find(pending_Dec_syms_mkr >=0);
%-----
Scanback_eq_col =find(Enc_syms_mkr > 0);
for sb =1 :length(Scanback_eq_col)
index_sb =Scanback_eq_col(sb);
sb_enc_eq =find(LT_Gen_Mat(:,index_sb)==1);
sb_chk =setdiff(sb_enc_eq , union(update_syms, knw_syms));
if t ==1
fprintf('\n\tEncoding Syms combination : ' , mat2str(sb_enc_eq), ' *Known
syms*Recently Update : ' , mat2str(union(update_syms, knw_syms)), '\n')
end
if numel(sb_chk)==1
if t ==1
fprintf('\n\t==>S.B.Decodable Obtain dec symb : ' , num2str(sb_chk));
end
pending_Dec_syms_mkr(sb_chk)=sb_chk;
tempX =k_xor_v1(sb_enc_eq , knw_syms , pending_Dec_syms);
pending_Dec_syms(sb_chk)=xor(erasure_enc_syms(index_sb), tempX);
end
end
update_Num =sum(Dec_syms_mkr ~=pending_Dec_syms_mkr);
update_syms =find(Dec_syms_mkr ~=pending_Dec_syms_mkr > 0);
if t ==1
fprintf('\nUpdate : ' , num2str(update_Num), ...
        ' syms , : ' , mat2str(update_syms), '\n')
end
%Update For Next Process
Dec_syms_mkr =pending_Dec_syms_mkr;
Dec_syms      =pending_Dec_syms;
end

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

end
end
%+++++
Decoded =sum(Dec_syms_mkr > 0);
if t =2
    disp(sprintf('\nReceived :(' num2str(rx_enc), '/' ,
num2str(length(erasure_enc_syms)), ')R-Decoded :(' , num2str(Decoded), ' of ' ,
num2str(length(input_syms))));
end
if Decoded ==length(input_syms)
    break;
end
end
dec_syms =Dec_syms;
bit_err =sum(input_syms ~= dec_syms);
end

```

ก.2.5 MATLAB Source code ของการบวนการตรวจสอบเมทริกซ์กำเนิดรหัสแอลทีว่าสามารถถอดรหัสได้หรือไม่

```

function [flag] =LT_process_v01(LT_Gen_Mat , LTgenMx_inpLoc)
%initialize process
covered =[];
processed =[];
ripple =[];
released =[];
LT_Gen_Mat_2 =LT_Gen_Mat;
LTgenMx_inpLoc_2 =LTgenMx_inpLoc;
%.....
%Initialize phase
degl =sum(LT_Gen_Mat_2);
[~,indx]=find(degl == 1);
if ~isempty(indx)
    Init_released_enc =indx;
    Init_covered_inp =[];
    for i =1 numel(Init_released_enc)
        inp =find(LTgenMx_inpLoc_2(:,Init_released_enc(i))~=0);
        Init_covered_inp =[Init_covered_inp inp];
        LTgenMx_inpLoc_2(:,Init_released_enc(i))=0;
        LT_Gen_Mat_2(:,Init_released_enc(i)) =0;
    end
    Init_ripple =Init_covered_inp;
end
released =Init_released_enc;
covered =Init_covered_inp;
processed;
ripple =sort(Init_ripple);
%-----
trigger =0;
while (trigger =0)
    action =ripple(1);
    %....
    processed =[processed action];
    ripple =ripple(ripple ~= action);
    LTgenMx_inpLoc_2(action ,:)=0;
    LT_Gen_Mat_2(action ,:)=0;
    [~,new_released_indx]=find(sum(LT_Gen_Mat_2)=1);
    new_released_indx =setdiff(new_released_indx , released);
    new_covered_indx =[];
    if ~isempty(new_released_indx)

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

    for i = 1 : numel(new_released_indx)
        temp = find(LTgenMx_inpLoc_2(:,new_released_indx(i)) ~= 0);
        new_covered_indx = [new_covered_indx temp];
    end
else
end
%Update released //covered
released = k_unique_unsorted([released new_released_indx]);
covered = k_unique_unsorted([covered new_covered_indx]);
processed = k_unique_unsorted(processed);
ripple = k_unique_unsorted([ripple new_covered_indx]);
if action == ripple
    ripple = [];
    trigger = 1;
elseif isempty(ripple)
    trigger = 1;
end
ripple;
%-----
end
[k,K]=size(LT_Gen_Mat);
released = sort(released);
covered = sort(covered);
processed = sort(processed);
ripple;
flag = 0;
if numel(released)==K
    flag = flag + 1;
end
if numel(covered)==k
    flag = flag + 1;
end
if processed == covered
    flag = flag + 1;
end
flag = (flag==3);
end

```

ก.2.6 MATLAB Source code วัดประสิทธิภาพของรหัสเครือข่ายเชิงระบบกับรหัสแอลที

```

yysavepath =
'D:\Dropbox\Master.KMITL\Matlab_Code\Works02.01\LTEncode_Decode_RobustIdealSoliton\20_CodeR
ate_n2000k1000\';
load(yysavepath, 'LTmatrix_n2000k1000.mat');
%Global setting
LTGenMat_M01R;
LTGenMat_M01S;
[k,K]=size(LTGenMat_M01R{1});
[numCode , ~]=size(LTGenMat_M01R);
f = 1000;
delta = 0.9;
c = 1;
LTGenMatx01 = LTGenMat_M01R;
LTGenMatx01S = LTGenMat_M01S;
Pe = 0:0.01:0.1;
avg = 50;
option = 'reg'; %'reg', 'sys';
fname = ['S00_L', num2str(avg), '_FER_', option, '.mat'];
fprintf(option, '%s', fname);
tt_frame_nrm_err = zeros(1, length(Pe));
tt_frame_xLT_err = zeros(1, length(Pe));

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ก.2.7 MATLAB Source code แยกเพื่อใช้สร้างเมทริกซ์กำเนิดรหัสแอลที

```

k = 1000;
K = 1500;
c = 1; %Use Robust_derec v04a to find c value
delta = 0.1;
%-----
fileIndex = 1;
numfiles = 5;
while(1)
    fileIndex;
%+++++
    exceed_flg = 1;
    while(exceed_flg == 1)
%prevent no degree form RBD
        OneChk = 0; %Just Initialize
        loop = 0;
        while(OneChk == 0)
%-----
            [mu , rho , ~ , ~]=robust_Soliton_Dist_Fn_03_not_Stable(delta , c , k );
            robust_degVector =randsample(k,k,true,mu)';
%-----
            OneChk = numel(find(robust_degVector==1));
            loop = loop +1;
        end
        sumDeg = sum(robust_degVector);
[LTgenMx_inpLoc , exceed_flg]=fn_robustLTencoder_v03(k , robust_degVector ,...
                                                    K , 5 , 0);
    end
    input_syms =randi(0 1,1,k);
    LTGenMat01R =mod(LTgenMx_inpLoc > 0,2);
    Enc_syms =mod(input_syms*LTGenMat01R,2);
    LTGenMat01S =to_systematicForm_v01(LTGenMat01R );
    if fileIndex > numfiles
        break
    end
    if isSystemetricForm(LTGenMat01S)==1
        find(sum(LTGenMat01R)=0)
        find(sum(LTGenMat01S)=0)
        fileIndex =fileIndex +1;
    end
end
end

```

ก.2.8 MATLAB Source code ฟังก์ชันที่ใช้ในการคำนวณค่าเฟรมผิดพลาดร่วม

```

function []=MutualFrameErased_Calculator(pe_nm , pe05 ,pe067 )

pm2 =[];
pm3 =[]
pm_CR050_R2 =[];
pm_CR050_R3 =[];
pm_CR067_R2 =[];
pm_CR067_R3 =[];

for i =1 :length(pe_nm)
    buff =fn_mutualErasure_calc_v02(n , pe_nm(i));
    pm2 =[pm2 buff];

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

    buff =fn_mutualErasure_calc_v02(n , pe05(i));
    pm_CR050_R2 =(pm_CR050_R2 buff);
    buff =fn_mutualErasure_calc_v02(n , pe067(i));
    pm_CR067_R2 =(pm_CR067_R2 buff);
end
pm3 =pm2.^2;
pm_CR050_R2;
pm_CR050_R3 =pm_CR050_R2.^2;
pm_CR067_R2;
pm_CR067_R3 =pm_CR067_R2.^2;
pm2 =pm2*100
pm3 =pm3*100
pm_CR050_R2 =pm_CR050_R2*100
pm_CR050_R3 =pm_CR050_R3*100
pm_CR067_R2 =pm_CR067_R2*100
pm_CR067_R3 =pm_CR067_R3*100
plot(pe_nm ,pm2 , 'b-' , ...
    pe_nm ,pm3 , 'r-' , ...
    pe_nm ,pm_CR050_R2 , 'b-' , ...
    pe_nm ,pm_CR050_R3 , 'r-' , ...
    pe_nm ,pm_CR067_R2 , 'b-' , ...
    pe_nm ,pm_CR067_R3 , 'r-' , ...
axis([0 max(pe_nm)0 105])
ylabel('Mutual Frame Error (%)')
xlabel('Erasure Probaility (Pe)')
legend('wo Encoding, 2 recievers', ...
    'wo Encoding, 3 recievers', ...
    'SNC(0.50), 2-receivers', ...
    'SNC(0.50),3-receivers', ...
    'SNC(0.67),2-receivers', ...
    'SNC(0.67),3-receivers')
title('MFE value of of n receivers and different coderates')
grid on;
end
function [pm]=fn_mutualErasure_calc_v01(n , pe , d)
e =(pe^n);
n1 =(n);
exp =1;
if e < 1
    while(e<=1)
        e =e*10;
        exp =exp*10;
    end
    e =ceil(e);
    n1 =n1*exp;
end
if mod(e,1)~=0
    while(mod(e,1))
        e =e*10;
        exp =exp*10;
    end
    n1 =n1*exp;
end
A =(fn_chz_nchoosek(n1,e)^(d-1);
B =[];
for i =1 :d-1
    buff =fn_chz_nchoosek(n1-(i*e) , e);

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

    B =[B buff];
end
B =prod(B); pm =1-(B/A);
if isnan(pm)
    pm =1;
end
end
end

```

ก.2.9 MATLAB Source codeในการวัดค่าทรูพุดและเวลาที่ใช้ในการส่ง

```

addpath('D:\Dropbox\Master.KMITL\Matlab_Code\Works02.01\Inter_Network\LTcode');

%LT code
%Code rate (N,K)=(1000,500)
Pe =0.04;
f =1000;
Link_Quality =1e6;
%Node Setup -----
%มีประเภท myRouter_v3('ชื่อ',หมายเลขID,'สถานะ',[หนวดข้างฝั่ง]);
%(rID,rStatus,neighborSet)
%Initialize Variable Lvl :1
aln1 =myRouter_v3(1,101,'Source',[],[]);
aln2 =myRouter_v3(1,102,'Relay',[],[]);
aln3 =myRouter_v3(1,103,'Router',[],[]);
aln4 =myRouter_v3(1,104,'Relay',[],[]);
aln5 =myRouter_v3(1,105,'Relay',[],[]);
aln6 =myRouter_v3(1,106,'Sink',[],[]);
aln7 =myRouter_v3(1,107,'Sink',[],[]);
local_connection_table =|0 1 0 1 0 0 0 ;
    1 0 1 0 0 1 0 ;
    0 1 0 1 1 0 0 ;
    1 0 1 0 0 0 1 ;
    0 0 1 0 0 1 1 ;
    0 1 0 0 1 0 1 ;
    0 0 0 1 1 1 0|;
inter_connection_table =|0 1 1 1 ;
    1 0 1 1 ;
    1 1 0 1 ;
    1 1 1 0 |;

%Autonomous System
as1_rt_LinkList =|aln1 aln2 aln3 aln4 aln5 aln6 aln7|;
clearvars aln1 aln2 aln3 aln4 aln5 aln6 aln7
%Assign Local Neighbor จาก Connection Table
for r =1 :length(as1_rt_LinkList)
    as1_rt_LinkList(r).neighborSet =find(local_connection_table(r,:)=1);
end
%Copied
as2_rt_LinkList =as1_rt_LinkList;
as3_rt_LinkList =as1_rt_LinkList;
as4_rt_LinkList =as1_rt_LinkList;
%Change ASID
for r =1 :length(as1_rt_LinkList)
    as2_rt_LinkList(r).ASID =2;
    as3_rt_LinkList(r).ASID =3;
    as4_rt_LinkList(r).ASID =4;
    as2_rt_LinkList(r).rID =200+r;
    as3_rt_LinkList(r).rID =300+r;
    as4_rt_LinkList(r).rID =400+r;

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

end
%Connect AS up
as1_rt_LinkList(3).gatewaySet = find(inter_connection_table(1,:)=1);
as2_rt_LinkList(3).gatewaySet = find(inter_connection_table(2,:)=1);
as3_rt_LinkList(3).gatewaySet = find(inter_connection_table(3,:)=1);
as4_rt_LinkList(3).gatewaySet = find(inter_connection_table(4,:)=1);
%Now We have
as1_rt_LinkList;
as2_rt_LinkList;
as3_rt_LinkList;
as4_rt_LinkList;
entire_Network =[as1_rt_LinkList ;
                  as2_rt_LinkList ;
                  as3_rt_LinkList ;
                  as4_rt_LinkList];
clearvars as1_rt_LinkList as2_rt_LinkList as3_rt_LinkList as4_rt_LinkList r
%ทำการสุ่ม Source node จาก AS 1อันก็ได้ จาก entire_Network
reloop = 300;
sink_TPrec3 = zeros(reloop,3);
sink_TPrec6 = zeros(reloop,3);
sink_DLrec3 = zeros(reloop,2);
sink_DLrec6 = zeros(reloop,2);
for ui = 1 :reloop

[numAS , ~]=size(entire_Network);
AS =[1:numAS];
SourceAS = randi([1 numAS],1,1);
AS =AS(AS~=SourceAS);
SinksAS =AS(randi([1 length(AS)],1,1));
fprintf('\n AS: ', num2str(SourceAS), ' ---> AS: ', num2str(SinksAS))
%Packet creation .....
option = 'sys';
load('D:\Dropbox\Master.KMITL\Matlab_Code\Works02.01\Inter_Network\LTMat\LT_n4_n1500k1000.mat')
        %xLT_n5_n750k500.mat
        %xLT_n4_n1500k1000.mat
[numCode , ~]=size(LTGenMat_M01R);
[K , N] =size(LTGenMat_M01R{1});
input_Frames = frameCells_creator_v01(K,f);
code_index =randi([1 numCode], 1 , 1);

if strcmp(option , 'sys')
    LTGenMat01 =LTGenMat_M01S{code_index};
elseif strcmp(option , 'reg')
    LTGenMat01 =LTGenMat_M01R{code_index};
end
enc_tx_Frames =frameCell_encoder_v01(input_Frames , LTGenMat01 ,f );
input_rx_Frames =erasureFrame_ch_v01(input_Frames , Pe );

clearvars LTGenMat_M01R LTGenMat_M01S

packet =myPacket_v1(1,SinksAS, [entire_Network(SinksAS,6).rID entire_Network(SinksAS,7).rID], ...
    [],input_Frames ,enc_tx_Frames , LTGenMat01 ,[], [], []);
%.....
%node-2-node
%Source
A1S1 =entire_Network(SourceAS,1);
A1S3 =entire_Network(SourceAS,3);
A1S4_OH =entire_Network(SourceAS,4);
A2S6 =entire_Network(SourceAS,6);
A2S2_OH =entire_Network(SourceAS,2);

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

AlS1.sendingQueue = packet;
clearvars packet
%ส่งผ่าน BEC CH
packet_ch13 = AlS1.sendingQueue;
packet_ch13.enc_data = erasureFrame_ch_v01(AlS1.sendingQueue.enc_data , Pe);
packet_ch14_oh = AlS1.sendingQueue;
packet_ch14_oh.enc_data = erasureFrame_ch_v01(AlS1.sendingQueue.enc_data , Pe);
packet_ch16 = AlS1.sendingQueue;
packet_ch16.enc_data = erasureFrame_ch_v01(AlS1.sendingQueue.enc_data , Pe);
packet_ch12_oh = AlS1.sendingQueue;
packet_ch12_oh.enc_data = erasureFrame_ch_v01(AlS1.sendingQueue.enc_data , Pe);
%Receiver AS1
AlS3.receivedPool = packet_ch13;
clearvars packet_ch
%Decoding
%AlS3.receivedPool
input_Frames = AlS3.receivedPool.inp_data;
enc_rx_Frames = AlS3.receivedPool.enc_data;
LTGenMat01 = AlS3.receivedPool.LT_tab;
[decode_Framecells3 , ...
lt_num_frameErr3 , ...
lt_FrameErr3 ] = fn_robustLTdecoder_frame_v07s(input_Frames ...
, enc_rx_Frames ...
, LTGenMat01 , f , 2 );
%OverHeard AS1
AlS4_OHreceivedPool = packet_ch14_oh;
input_Frames = AlS4_OHreceivedPool.inp_data;
enc_rx_Frames = AlS4_OHreceivedPool.enc_data;
LTGenMat01 = AlS4_OHreceivedPool.LT_tab;
[decode_Framecells4oh , ...
lt_num_frameErr4oh , ...
lt_FrameErr4oh ] = fn_robustLTdecoder_frame_v07s(input_Frames ...
, enc_rx_Frames ...
, LTGenMat01 , f , 2 );
%Throughput Calc -----
w = f/Link_Quality;
DataSize = K*f;
h13 = 2 ; %Node 2 ret by Node 3
NoRet_Time3 = (h13+N)*w;
%Throughput Without retransmission
TP_wo_ret3 = DataSizeNoRet_Time3;
NumFramesSend3 = N-lt_num_frameErr3;
%Throughput With Norm retransmission
Norm_ret_time3 = NoRet_Time3 + (2*h13*NumFramesSend3*w);
TP_nm_ret3 = DataSizeNorm_ret_time3;
DL_nm_ret3 = (2*h13*NumFramesSend3*w);
if isempty(intersect(lt_FrameErr3,lt_FrameErr4oh))
%Throughput With OverHeard retransmission
Oh_ret_time3 = NoRet_Time3 + (2*NumFramesSend3*w);
TP_oh_ret3 = DataSizeOh_ret_time3;

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```

    DL_oh_ret3 =(2*1*NumFramesSend3*w);
else
    TP_oh_ret3 =TP_nm_ret3;
    DL_oh_ret3 =DL_nm_ret3;
end
%-----
%Receiver Next AS
A2S6.receivedPool =packet_ch16;
clearvars packet_ch
%Decoding
    A2S6.receivedPool;
    input_Frames =A2S6.receivedPool.inp_data;
    enc_rx_Frames =A2S6.receivedPool.enc_data;
    LTGenMat01 =A2S6.receivedPool.LT_tab;
[decode_Framecells6 , ...
    lt_num_frameErr6 , ...
    lt_FrameErr6 ]=fn_robustLTdecoder_frame_v07s(input_Frames ...
                                                ,enc_rx_Frames ...
                                                ,LTGenMat01 , f , 2 );
%OverHeard Next AS
A2S2_OH.receivedPool =packet_ch12_oh;
    input_Frames =A2S2_OH.receivedPool.inp_data;
    enc_rx_Frames =A2S2_OH.receivedPool.enc_data;
    LTGenMat01 =A2S2_OH.receivedPool.LT_tab;
[decode_Framecells2oh , ...
    lt_num_frameErr2oh , ...
    lt_FrameErr2oh ]=fn_robustLTdecoder_frame_v07s(input_Frames ...
                                                ,enc_rx_Frames ...
                                                ,LTGenMat01 , f , 2 );
%Throughput Calc -----
h16 = 5 ;%Node 6 ret by Node 2
NoRet_Time6 =(h16*N)*w;
%Throughput Without retransmission
TP_wo_ret6 =DataSizeNoRet_Time6;
NumFramesSend6 =N*lt_num_frameErr6;
%Throughput With Norm retransmission
Norm_ret_time6 =NoRet_Time6 +(2*h16*NumFramesSend6*w);
TP_nm_ret6 =DataSizeNorm_ret_time6;
DL_nm_ret6 =(2*h16*NumFramesSend6*w);
if isempty(intersect(lt_FrameErr6,lt_FrameErr2oh))
    %Throughput With OverHeard retransmission
    Oh_ret_time6 =NoRet_Time6 +(2*NumFramesSend6*w);
    TP_oh_ret6 =DataSizeOh_ret_time6;
    DL_oh_ret6 =(2*NumFramesSend6*w);
else
    TP_oh_ret6 =TP_nm_ret6;
    DL_oh_ret6 =DL_nm_ret6;
end
sink_TPrec3(ui,1)=TP_wo_ret3;
sink_TPrec3(ui,2)=TP_nm_ret3;
sink_TPrec3(ui,3)=TP_oh_ret3;
sink_DLrec3(ui,1)=DL_nm_ret3;
sink_DLrec3(ui,2)=DL_oh_ret3;
sink_TPrec6(ui,1)=TP_wo_ret6;
sink_TPrec6(ui,2)=TP_nm_ret6;
sink_TPrec6(ui,3)=TP_oh_ret6;
sink_DLrec6(ui,1)=DL_nm_ret6;
sink_DLrec6(ui,2)=DL_oh_ret6;
sink_TPrec3(ui,);
sink_DLrec3(ui,);

```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
sink_TPrec6(ui,3)
sink_DLrec6(ui,3)
end
save('D:\Dropbox\Master.KMITL\Matlab_Code\Works02.01\Inter_Network\LTMat\sinkLTTx_x100_pe004
_file1.mat','sink_TPrec3','sink_TPrec6','sink_DLrec3','sink_DLrec6')
```



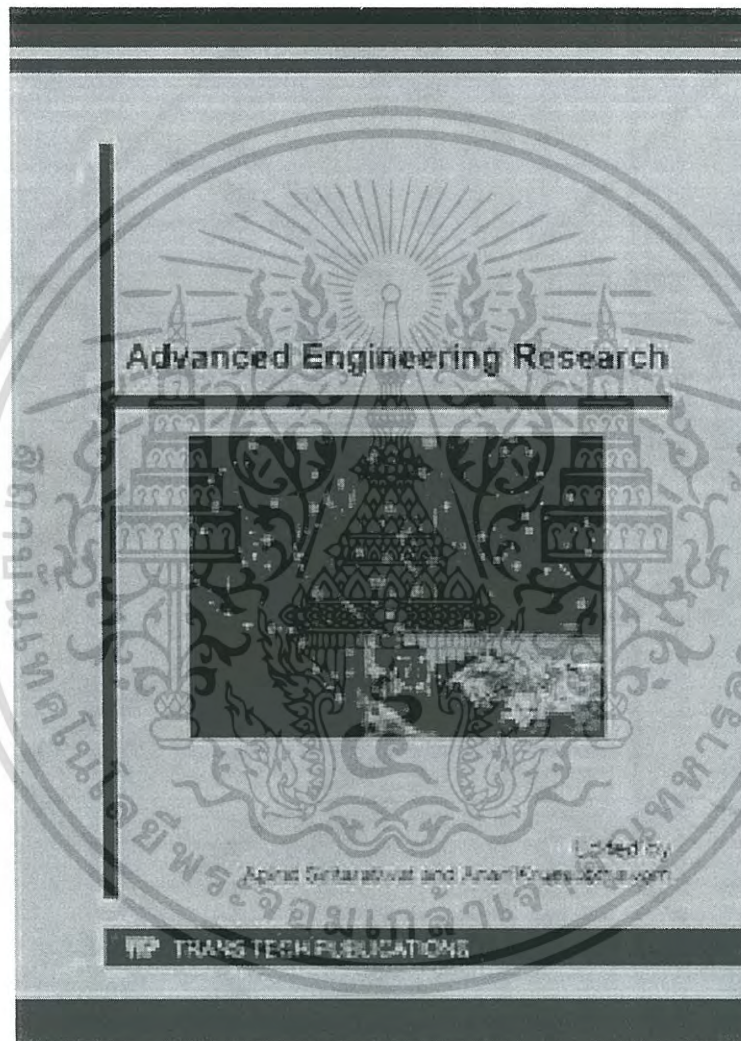
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



ภาคผนวก ค.

ผลงานที่ได้รับการตีพิมพ์ในวารสารและการประชุมวิชาการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

The Adaptive Network Coding-Routing (ANCR) Based on Graph for Multicast Networks*

Nakhon Muangboonma^{1, a}, Nattakan Puttarak^{1, b} and Phisan Kaewprapha^{2, c}

¹Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand

²Faculty of Engineering, Thammasat University, Pathumthani, Thailand

^as6601257@kmitl.ac.th, ^bkpnattak@kmitl.ac.th, ^ckaewprapha@gmail.com

Keywords: multicast wireless network, network coding, routing protocol

Abstract. The multicast wireless network, where a source needs to deliver packets of data to a set of destination through a group of relays over a network topology, is degraded by a limited bandwidth and capacity regime. Network throughput can be improved using network coding. However, the network coding might or might not be helpful to increase throughput due to an unpredictable network topology. In this paper, we propose an adaptive network coding-routing (ANCR) algorithm to automatically select whether a packet can construct a network code at a relay node before forwarding to destination or not based on the minor of network graphs. If there is no an appropriate packet, the relay will be forwarded a data packet using routing protocol. The results show that this technique can significantly improve both throughput and timeslot usage. The throughput gain at a bottleneck relay node is increased by 35%, while the timeslot usage is decreased for more than 30%.

Introduction

Recently a multicast wireless communications network has become more important and necessary for data transmission. People usually surf the Internet in daily lives, use wireless sensor network, and transfer a huge amount of data such as video stream or pictures across the wireless network. However, the multicast network with relay nodes always get affected from the bottleneck problem which leads to a delay of sending data packets or losing them from packet drop in routers. Likewise, the capacity or throughput of the network is limited by relay capability to forward a received packet at a time from multiple sources [1]. Routing protocol plays an important role to determine an appropriate route for delivering data packets to destination. Generally, routes are mainly multihops since wireless communication is limited by a radio propagation range and network topology is always unpredictably changed [2]. The Ad-hoc On-Demand Distance Vector (AODV) [2] protocol is an on-demand routing protocol which each node does not need to periodic update route table, since network hosts only keep route table entries with the destination nodes they communicate with. Later, an AODV-Backup Routing (AODV-BR) is introduced to improve the performance of AODV in order to utilize multiple paths. It provides robustness to mobility and enhances protocol performance [3]. However, routing protocol still cannot overcome a bottleneck problem that has a high probability to occur because in wireless network, all nodes can randomly and unpredictably move. They need more timeslots to deliver all data packets through a bottleneck route and yield more transmission delay and decrease throughput.

Network coding is a well-known technique to efficient increase a network throughput by allowing relays to algebraically compute a new packet by XORing any two incoming packets, and forward it to a bottleneck route [4]. The capacity can be achieved by using a network code in which

outgoing packets from a node are computed by linear combinations of two incoming packets over a certain field [5]. There are more techniques to improve the performance of network coding such as [6] developed an algebraic framework, and [1] presented an efficient construction of network coding by applying a randomized algorithm. However, to construct a network coding for wireless network is not easy, since all nodes are movable and randomly changed. The timeslot may be wasted for waiting a helpful packet to construct a new packet and forward it through a bottleneck route which causes more delay.

In this work, we consider a butterfly network for 2-minimal multicast communications and propose the algorithm called "*adaptive network coding-routing (ANCR)*," where all relays are capable to either forward data to the best route using AODV and AODV-BR routing protocol or algebraic compute packets before routing. Our scheme is inspired by [7] introduced and proved that a K_4 graph minor of any graph topology can reduce computation time of network coding. They introduced the relation between algebraic coding and network topologies and claimed that network coding can be applied and make a difference from routing only if the network topology contains a K_4 minor. Therefore, the ANCR algorithm is motivated by the requirement to improve a network capacity by increasing throughput, and yet reduce transmission time for individual relays.

Proposed Algorithm

Consider a graph $G(V, E)$ which refers to a butterfly network, where V and E are the set of vertices and edges respectively as shown in Fig. 1. This network topology includes one source (V_1), four relay (R_2, R_3, R_4, R_5), and two sink (D_6, D_7). To setup a transmission, we focus on the application of 2-minimal networking which is based on AODV wireless sensor network protocol [2] with capability to find routing path independently. This protocol will allow each path be depended on the specific path called as a condition path to verify how fast RREQ/RREP process flooding and queue management of each node. For our algorithm, to obtain more paths we have applied techniques and ideas from AODV-BR [3] by using an alternate path to construct network. This technique differs from COPE in [4] that the promiscuous mode is not required and it can wait for *reception report* from neighbor nodes where all packets are allowed to build a coding operation. When the shortest path's RREP packet was delayed, that path becomes to be an alternate path in a routing table. The source have already known the path information and used graph-based knowledge to make a decision which packets will be included for a network coding. The ANCR algorithm is shown in Fig. 2 can be considered in 2 phases: packet selection and decomposition. **Phase I: Packet selection:** This phase describes how and which packet could be selected to construct a network code before forwarding. After the source node finished sending and receiving RREQ and RREP, respectively, the primary and secondary paths will be setup at each intermediate relays connected to the source. Then, the source node needs to seek path that has at least two packets to be carried and put it on top of the forwarding queue. At least one of all packets must be a multicast packet (P_m) that can be retrieved at its destination. Let d_{P_u}, d_{P_m} be a destination set of unicast packet (P_u) and multicast packet (P_m). If the first two packets are P_m and P_u , the relationship between destination set d_{P_u} and d_{P_m} must be $d_{P_u} \in d_{P_m}$ and if the first two packets are both P_m , we set $d_{P_m}^1$ and $d_{P_m}^2$ be the first and the second of destination set of these two packets that also have different destinations. **Phase II: Decomposition process:** After two packets have been selected from phase I then the decomposition process will be operated by defining flow F_i , which is obtained from all paths of packet i^{th} , where $f_{pi}, f_{si} \in F_i$ are the primary flow and secondary flow, respectively. Moreover, the $f_{pi}, f_{si} \in F_i$ and $f_{pj}, f_{sj} \in F_j$ must relate to each other, if packets i^{th} and j^{th} are in the same minor. The

algorithm of this decomposition process is presented by Algorithm. 1. As soon as the decomposition process is finished, the source can build up a graph minor, which contains an appropriate group of nodes used for XORing, if a graph minor is K_i as claimed in [7]. The result shows packets generated only from nodes in the same minor that can be allowed to apply network coding before relaying or not shown in Fig. 3.

Channel Model and Network Coding: We have simulated the transmission system in physical layer through an additive white Gaussian noises (AWGN) channel. Let a received data be $y = x + n$, where x is a transmitted data and n is an AWGN noise $N(0, \sigma)$. If the XORed packet has arrived at the receiver node, it will be decoded by XORing this packet with another packet that might be sent from other relays.



Figure 1: Butterfly Network Figure 2: The ANCR algorithm. Algorithm 1: Decomposition process

However, if that packet is not found at the received queue, a longer wait time will be extended for t_d . After the construction of ANCR, source node S_i will add the additional field named as "coding node addr" automatically added into an original packet of S_i to indicate whether this packet is an XORed packet or not. Also, "decode PK ID set" is added to indicate which packet is used for decoding this XORed packet. Therefore, to decode data let $d_o = d_x \oplus (d_{n1} \oplus d_{n2} \oplus \dots)$, where d_o is an actual data needed at a receiver node, d_x is a XORed packet and d_n is a data packet sent by the source node guided by a graph minor.

Results

To study a behavior of data from network coding or routing and evaluate their performance improvements made by an ANCR algorithm, we apply the butterfly network as shown in Fig. 1. The ANCR algorithm is used to adaptive select whether data packet should be XORed before forwarding or not and if it is not, the routing protocols, which are AODV and AODV-BR in [2] and [3], will be applied. Our goal is to increase throughput at receiver nodes, and also reduce transmission times of network that might be degraded by a bottleneck issue. The K4 minor is embedded in the network referred to the composition process of this algorithm.

The simulation results is shown in Fig. 4 that present a throughput measurement of node 3 (bottleneck) and node 7 (receiver) with the changes of timeslot usage for both ANCR algorithm and conventional routing protocol. The result shows that a network with an ANCR algorithm achieves more throughputs compared with the same network solely operating by conventional routing protocol. Not only node 3 can increase its throughput, but also the throughputs of both sinks are significantly increased and simultaneously reduce timeslot usage. The throughput gains of all receiver nodes and relay node are represented in Table 1. Most of relay nodes can be benefited by

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

the ANCR algorithm since they all achieve throughput gain and outperform a conventional routing protocol. Node 3 gains more throughput than the one using routing protocol for approximately 36%. In addition, receivers also obtain this benefit with throughput gains for over 45%. The timeslot usage is considered since a delay of transmission is important for performance improvement. To measure the number of timeslots, we count a CTS/RTS process as one timeslot [8].

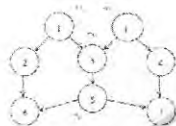


Figure 3. The K_4 minor of a butterfly network from the decomposition process.

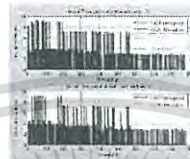


Figure 4. Actual throughput at a bottleneck node 3 and receiver node 7.

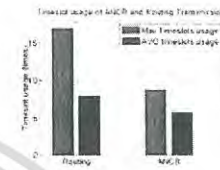


Figure 5. The maximum and average timeslots usage.

Table 1. Throughput measurement

Node	AODV or AODV-RR		ANCR	
	Average Throughput (Mbps)	Average Throughput (Mbps)	Average Throughput (Mbps)	Throughput Gain (%)
Source node 1	0.0000	0.0000	0.0000	0
Relay node 2	6.5920	6.9296	6.9296	31.03
Bottleneck node 3	7.4636	7.8458	7.8458	36.32
Relay node 4	6.2751	7.1668	7.1668	32.46
Relay node 5	5.4624	6.6034	6.6034	35.79
Sink node 6	6.6210	13.1222	13.1222	47.54
Sink node 7	6.8193	12.0437	12.0437	49.37

The result in Fig. 5 illustrates that an ANCR technique uses less timeslot than a routing protocol measured in average and in the maximum number of timeslots that both methods can use to finish their transmission. Fig.4 and Fig.5 show that the ANCR technique requires the number of transmissions for approximately 550 times to finish transmitting their packets, while the AODV routing method needs more than 850 times to finish them. Thus, our method can reduce the transmission time by 35%.

Conclusion

We have proposed a scheme called "adaptive network coding-routing (ANCR)" to reduce a transmission time and simultaneously increase throughput by using graph minor perspective to apply the network coding at a bottleneck route. The routing protocols are also applied in this technique to obtain more route information with 2-minimal property. Our results show this algorithm improves speed and efficient transmission in wireless communication network. Network throughput is increased and gained more than 35% at the bottleneck relay, and also gained approximately 50% at receiver nodes compared with the throughput of network with a routing protocol. In addition, our ANCR technique can reduce time to transmit the whole packets from source to destination for more than 30%.

*This work was supported by the NSTDA, Thailand under grant no. SCH-NR2014-223.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

References

- [1] T. Ho, M. Médard, J. Shi, M. Effros, and D. R. Karger, "On randomized network coding," *Proc. of the Annual Allerton Conference on Commu. Control and Computing*, Vol. 41, No. 1, 2003.
- [2] I. D. Chakeres, and E. M. Belding-Royer, "AODV routing protocol implementation design," *Proc. of 24th IEEE Inter. Conference*, 2004.
- [3] S. J. Lee, and M. Gerla, "AODV-BR: Backup routing in ad hoc networks," *Proc. of Wireless Communications and Networking Conference (WCNC)*, Vol. 3, pp. 1311-1316, 2000
- [4] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: practical wireless network coding," *ACM SIGCOMM Computer Communication Review*, Vol. 36, No. 4, pp. 243-254, 2006.
- [5] S. Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Info. Theory*, Vol 49, pp.371-381, 2003.
- [6] R. Koetter, and M. Médard, "An algebraic approach to network coding," *IEEE ACM Trans. Networking*, Vol 11, pp. 782-795, 2003
- [7] X. Yin, Y. Wang, X. Wang, X. Xue, and Z. Li, "A graph minor perspective to network coding: Connecting algebraic coding with network topologies," *Proc. of INFOCOM*, pp. 2364-2372, 2013.
- [8] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey," *IEEE Communications Magazine*, Vol 44, No. 4, pp. 115-121, Apr 2006.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Advanced Engineering Research

10.4028/www.scientific.net/AMM.781

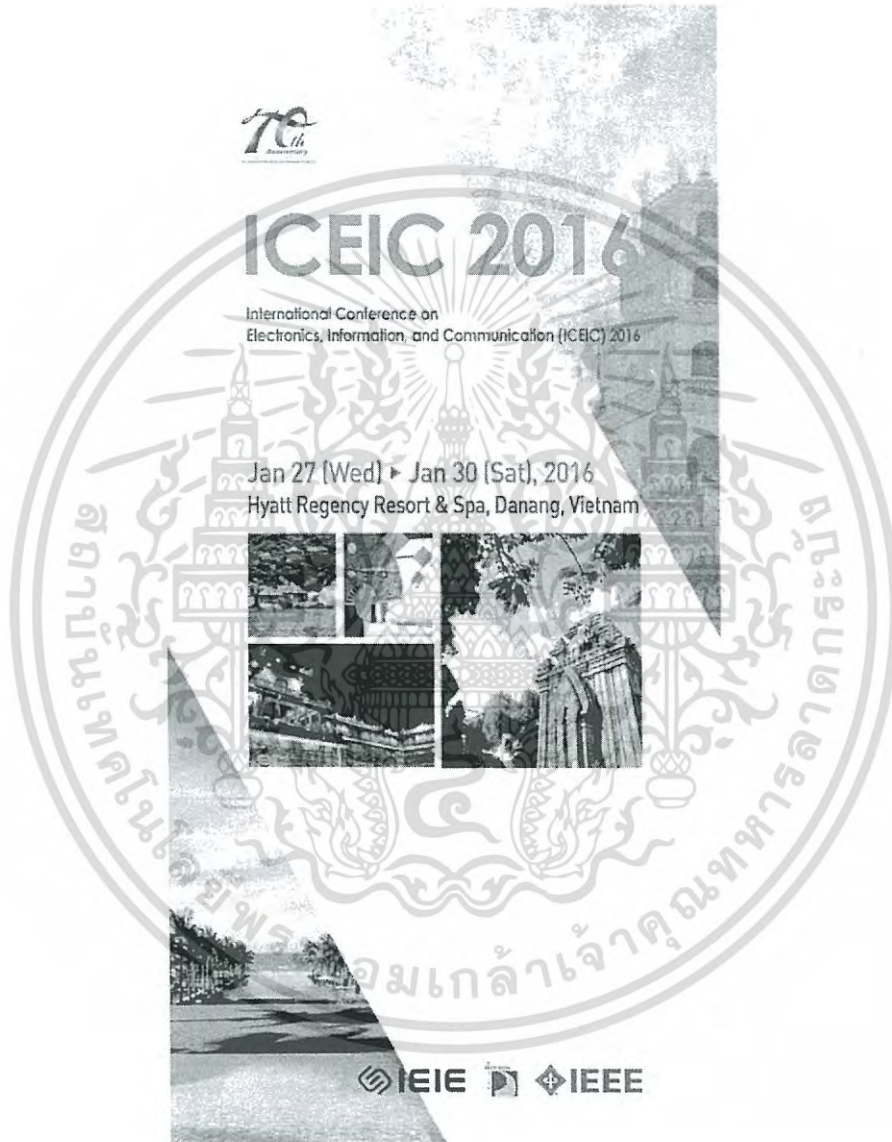
The Adaptive Network Coding-Routing (ANCR) Based on Graph Minors for Multicast Networks

10.4028/www.scientific.net/AMM.781.36

DOI References

- [2] I. D. Chakeres, and E. M. Belding-Royer. AODV routing protocol implementation design. Proc. of 24th IEEE Inter. Conference, (2004).
10.1109/icdesw.2004.1284108
- [3] S. J. Lee, and M. Gerla, AODV-BR: Backup routing in ad hoc networks. Proc. of Wireless Communications and Networking Conference (WCNC), Vol. 3, pp.1311-1316, (2000).
10.1109/wcnc.2000.904822
- [4] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft. XORs in the air: practical wireless network coding. ACM SIGCOMM Computer Communication Review, Vol. 36, No. 4, pp.243-254, (2006).
10.1145/1151659.1159942
- [5] S. Y. Li, R. W. Yeung, and N. Cai. Linear network coding. IEEE Trans. Info. Theory, Vol 49, pp.371-381, (2003).
10.1109/TIT.2002.807285
- [6] R. Koetter, and M. Médard. An algebraic approach to network coding. IEEE/ACM Trans. Networking, Vol 11, pp.782-795, (2003).
10.1109/TNET.2003.818197
- [7] X. Yin, Y. Wang, X. Wang, X. Xue, and Z. Li, A graph minor perspective to network coding: Connecting algebraic coding with network topologies. Proc. of INFOCOM, pp.2364-2372, (2013).
10.1109/infcom.2013.6567041

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Latency-reduced Retransmission in Multicast Network using Systematic Network code*

Nakhon Muangboonma
Faculty of Engineering
King Mongkut's Institute of
Technology Ladkrabang
Bangkok, Thailand
S6601257@kmitl.ac.th

Nattakan Puttarak
Faculty of Engineering
King Mongkut's Institute of
Technology Ladkrabang
Bangkok, Thailand
kpnattak@kmitl.ac.th

Phisan Kaewprapha
Faculty of Engineering
Thammasat University
Pathumthani, Thailand
kphisan@engr.tu.ac.th

Abstract—The reliability of multicast network where source delivers many frames of data to multiple receivers over a large scale network is degraded by delay of retransmissions after some data frame has been lost. This paper proposes a coding technique applying on network layer to combat this problem by using systematic network code with overheard retransmission technique. Latency of retransmission and throughput will be measured to represent the performance of this algorithm. The results show that this technique can improve reliability and performance of multicast network by decreasing a delay of retransmission for 40-70 % and yet increasing throughput for more than 8-19% compared with a conventional method.

Keywords—multicast network, network code, retransmission, throughput gain

I. INTRODUCTION

The rises of big data and a huge amount of data transfer allows the multicast network to consist of variety devices and services and the increasing of application such as internet of things (IoT) concept have become more significant in everyday life. People communicate across the world by accessing networks and transfer a huge data anytime, anywhere. However, a reliability/integrity of communication in a large scale network is always degraded by delay/latency of data retransmission which depends on a number of transmission hops.

In wireless multicast communication system and sensor network, a particular source sends data to multiple destinations. Bottleneck problem is still a major problem which causes either packets drop in transmission side or delay of arrival time. In [1], network code is introduced to increase system throughput by considering incoming packets and computing a new packet at bottleneck node. The construction of this network code depends on feedback reports from neighbors. Then, a 2-minimal multicast network is considered and ANCR (adaptive network coding-routing) technique is also introduced in [2] to overcome a bottleneck problem in a butterfly network and claims that it takes less feedback from neighbor. However, an ANCR algorithm and COPE [1] are not suitable for a larger network, where the transmission is more than 2 hops. In the appropriate condition, flooding of XOR packets to group of receivers through erasure channel is imperfect and reduces overall performance after erasure packet have been found in the higher layer and source node will suffer from negative acknowledgements (NACK). When any lost data frame is

required to retransmit from an original source, a latency on round-trip transmission is twice.

The opportunistic retransmission mechanism [3] is introduced for reducing a source workload and delay of retransmission time by exploiting behavior of promiscuous mode. The basic concept of opportunistic retransmission is that the destinations can automatically broadcasting request retransmission when they fail to receive data packets and wait for a period of time from intermediate node's acknowledgement. The link quality of overhearers who sense such request retransmission is estimated by received signal strength indicator (RSSI) with threshold and statistical of probe message named "the packet delivery rate (PDR)" [4], [5]. Then the best qualified relay is selected for retransmission instead of any predecessor node of requested receiver. The analytical and results shown in [3] achieve high throughput gain over IEEE802.11 standard implemented in mesh network for WLANs. This work [3] gives more fairness mechanism to apply at either physical or datalink layer and inspires us to deploy at network layer where the probability of erasure still effects on data frames.

Luby transform codes (LT code) [6] has been designed for binary erasure channel (BEC) by encoding between data frames using simple exclusive-or (XOR) operation. Since this code is a rateless near-optimal erasure correcting code, it is preferable for the system without a feedback channel where the retransmission is neglected. The systematic LT code [7] is after introduced to reduce complexity of decoding process. The reduction of system latency is studied in [8] in order to combat with limitation of feedback efficiency while traditional transmission at lossy link provides more feedback of errors. The ability to correct erasures of decoding process of systematic code outperforms the regular one is shown in [8]. However, the complexity at other receiver nodes still remains when the overheard nodes try to recalculate and produces a new code from shifted distribution for retransmission.

In this work, we propose a systematic network code (SNC) for a large scale communication network which is inspired by systematic LT code and opportunistic retransmission method to increases throughput, arrival time and also reduces transmission latency between nodes. Moreover, we also modify the mechanism for retransmission that give more throughput gain than that of a conventional method by analyzing and estimating

*This work was supported by the NSTDA, Thailand under grant no. SCH-NR2014-223.

III. EXPERIMENTAL SETUP

The network topology is designed based on the 7-nodes butterfly network as a subnetwork (SN) and subnetworks are directly connected through node number 3 to build a larger scale network with totally 28 nodes shown in Fig. 3. The intra-connection between nodes inside each subnetwork might be limited by a bottleneck problem in transmission process. The ANCR algorithm [2] is applied to increase throughput and also reduce traffic in bottleneck routes.

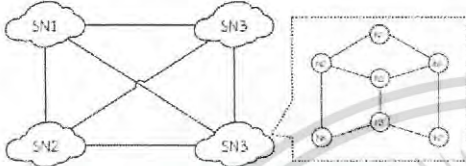


Figure 3. Large Scale Network and Butterfly Network.

A large scale network which establishes communication between sources and multiple sinks from many subnetworks will definitely suffer from a latency of retransmission. For the transmission between nodes either in the same or different subnetworks, the SNC is applied in order to reduce the number of retransmission, and also to observe an actual throughput gain. In this simulation setup, we assume that the AWGN can be neglected, since it is considered and eliminated by the lower layer mechanism. The encoded N frames are constructed from K data frame using the SNC scheme. So, the code rate is K/N . Each frame contains f bits and let a connection link quality be L Mbps through BEC with frame error probability p_e .

We design an additional mechanism which is adapted from an overheard retransmission originally used to reduce retransmission delay by sharing the heard data frame from their neighbor nodes. Any receiver node in our network has at least two neighbor nodes (one is a predecessor node and the other is an overheard node). The algorithm to make a decision which source will be responsible for an automatic repeat request (ARQ) is shown in Alg. 1. The best source node depicted by RSSI value or the receive succession rate is considered and finally chosen. We also consider about MEF value happened in both receiver and overheard node by the probability showing in Eq. (1).

Fig. 4 shows the percentage of MEF value between two and three receivers, while p_e value is varying from 0.01 to 0.1. The graph shows comparisons between the MEF value of non-coding scheme (w/o SNC) and that of our SNC in different code rates, where there are 1,000 bits in each frame. When p_e is in range of 0.01 to 0.07, the MEF is rapidly occurred almost 100% in the system without encoding. It means that with a little chance of erasures ($p_e=0.07$), all frames can be lost or erased and there are no "good" frames to retransmit from neighbor nodes. However, the systems with the SNC outperforms in reducing the MEF probability at all code rates. At the lower p_e ($p_e = 0.01-0.06$), a number of MEF is less than 10% of total frame transmitted since receivers help each other to retransmit and recover lost frames. After that, the percentage of MEF will increase when p_e is higher and finally reach 100% at $p_e = 0.1$.

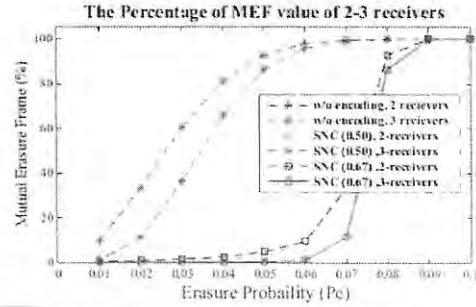


Figure 4. The Percentage of MEF Value of 2-3 receivers.

Algorithm 1. Overhead retransmission

```

Input : encoding frames  $N$ , systematic generator matrix  $G_{sys}$ 
output : retransmission message  $retx\_msg$ 
err_frames - decoding ( $N, G_{sys}$ );
retx_msg - broadcasting req_retx (neighbor_set, err_frames);
received_acks (neighbor_set);
If mef == 0
    retransmission (neighbor node);
else
    request_retransmission (source);
end

```

IV. RESULTS

To compare the performance of SNC with the conventional network code (CNC), the system with CNC, SNC, and without encoding will be considered. Fig. 5 shows the FER in different code rates of CNC and SNC, when p_e is varying from 0.2 to 0.02. For the simulation, we set $f = 1,000$ bits, so the totally transmitted data equals to $f \times N$ bits, where we transmit $N=1,500$ frames. The result shows that the system with SNC at code rate 0.50 and 0.67 achieve better performance than the one with CNC which has almost the same FER as the non-coding system has. However, the SNC system with code rate = 0.80 gives worse FER than CNC system, since at the same probability of MEF as others, this system has not enough parity to recover erasures.

The actual throughput during 200-seconds transmission of node number 3 (the receiver in the same subnetwork as source node) and 6 (the receiver from the different subnetwork from source node) are shown in Fig. 6. The system with SNC closely reaches the upperbound throughput which is the actual throughput of our link, while throughputs of the system with CNC and without encoding are significantly lower. Note that the throughput gain of the SNC multicast system is approximately 0.5-1 Mbps. We also measure and demonstrate the average throughput shown in Fig. 7. The average throughputs of SNC system in both kinds of node are higher than those of CNC system and without encoding system for 7.50% and 8.70%, respectively for node 3, and for 15.5% and 18.90%, respectively for node 6.

FER of SNC and CNC in different coderates vs non encoding

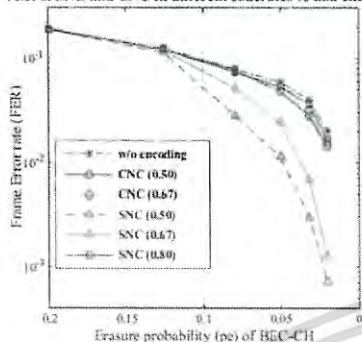


Figure 5. FER of SNC, CNC, and non-coding scheme

In addition, a total transmission time is measured to compare the system latency. Fig. 8 illustrates the average delay from source to destination when the retransmission is responsible by node 3 or node 6 in both SNC and without encoding systems. One can intuitively predict that retransmission from far-away relay node, which is located in different subnetwork, will definitely take more latency than retransmission from relay node located in the same subnetwork. So, the average delay of node 6 is higher than that of node 3 in both systems, but SNC system is still faster than system without encoding by decreasing approximately 70% of network latency. The average delay of node 3 in SNC system is less than that of node 3 in system without encoding approximately 40%.

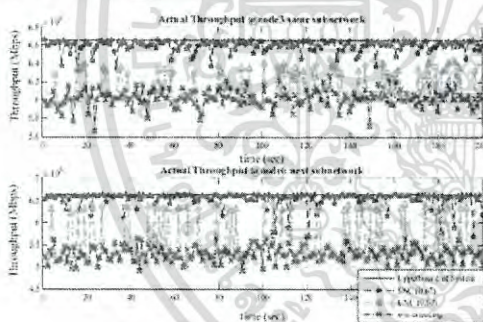


Figure 6. Actual throughput measurement of node number 3 and number 6.

V. CONCLUSION

In this paper, we have proposed a coding technique called "systematic network code (SNC)" to improve stability of transmission over binary erasure channel (BEC) by reducing delay of retransmission and simultaneously increasing throughput over a large scale network. The SNC is constructed based on CNC and LT codes. The results show that network

throughput is increased approximately 8% and also gained nearly 19%, when retransmitting from relay nodes in the same subnetwork and different subnetwork from source node, respectively. In addition, our technique can reduce delay time to retransmit all data approximately 40-70%.

Comparison of AVG Throughput of node number 3 and 6 Between SNC vs CNC and w/o encoding

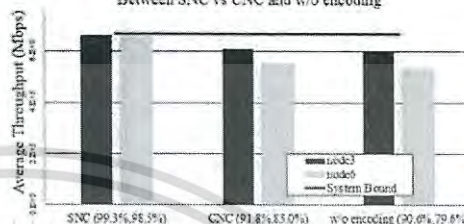


Figure 7. Comparison of AVG Throughput at node number 3 and 6 between SNC vs CNC and without encoding.

Comparison of AVG arrival delay of node number 3 and 6 Between SNC vs CNC and w/o encoding

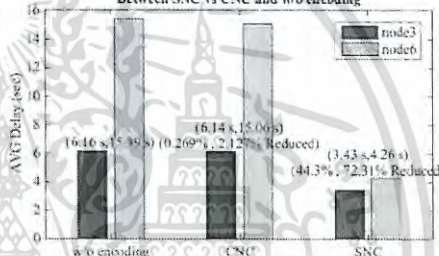


Figure 8. Comparison of AVG arrival delay reduction at node number 3 and 6 between SNC vs CNC and without encoding.

REFERENCES

- [1] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: practical wireless network coding," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 4, pp. 243-254, 2006.
- [2] N. Muengboonma, N. Puttarak, P. Kaewpraphin, "The Adaptive Network Coding-Rerouting (ANCR) Based on Graph for Multicast Networks," *Applied Mechanics and Materials*, pp. 36, 2015.
- [3] M. Lu, P. Steenkiste and T. Chen, "Design, Implementation and Evaluation of an Efficient Opportunistic Retransmission Protocol," *MOBICOM '09, 2009*.
- [4] D. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," *Proc. ACM MOBICOM*, Sept. 2003
- [5] R. Draves, J. Padhye, and B. Zill, Routing, "Multi-Radio, Multi-Hop Wireless Mesh Networks," *Proc. ACM MOBICOM*, Sept. 2004.
- [6] M. Luby, "LT codes," in *Proceeding of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, November 2002, pp. 271-282.
- [7] T. D. Nguyen, L. L. Yang and L. Hanzo, "Systematic Luby transform codes and their soft decoding," *IEEE SiPS '07*, pp. 67-72, Oct 2007.
- [8] M. T. Tang, B. Shradler, and T. C. Royster IV, "The Use and Performance of LT Codes for Multicast with Relaying," *The 2010 Military Communications Conference*, pp. 1262-1267, 2010.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ข้อมูลประวัติผู้วิจัย

นายนคร เมืองบุญมา

จบการศึกษาระดับปริญญาตรีในสาขาวิศวกรรมคอมพิวเตอร์ มหาวิทยาลัยขอนแก่น

งานวิจัยที่สนใจ : คอมพิวเตอร์เน็ตเวิร์ค, การสื่อสารไร้สาย.

อีเมล : nakhon.m1@gmail.com

ผลงานตีพิมพ์ในวารสารประชุมวิชาการ

1. N. Muangboonma, N. Puttarak, P. Kaewprapha, "The Adaptive Network Coding-Routing (ANCR) Based on Graph for Multicast Networks," Applied Mechanics and Materials. (AMM), vol. 781, no. 70, 2015, pp. 36-40.
2. N. Muangboonma, N. Puttarak, P. Kaewprapha, "Latency-reduced Retransmission in Multicast Network using Systematic Network code," in Proc. of International Conference on Electronics, Information and Communication (ICEIC), Da Nang, Vietnam, Feb. 2016, pp. 56-59.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้