การตรวจจับโหนดที่มีพฤติกรรมละทิ้งข้อมูลอย่างผิดปกติด้วยโมไบล์เอเจนต์ในเครือข่ายไร้สายแอดฮอกแบบ DSR

DETECTION OF PACKET DROPPING MISBEHAVIOR NODE BY MOBILE AGENTS IN DSR AD HOC WIRELESS NETWORKS

ชาวดี บารมี

CHAWDEE BARAMEE

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย

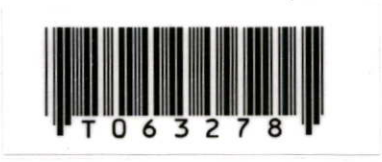
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2549

ISBN 974-15-2208-8

การตรวจจับโหนดที่มีพฤติกรรมละทิ้งข้อมูลอย่างผิดปกติด้วยโมไบล์เอเจนต์ในเครือข่ายไร้สายแอดฮอคแบบ DSR

DETECTION OF PACKET DROPPING MISBEHAVIOR NODE BY MOBILE AGENTS IN DSR AD HOC WIRELESS NETWORKS



ชาวดี บารมี

CHAWDEE BARAMEE

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2549

ISBN 974-15-2208-8

DETECTION OF PACKET DROPPING MISBEHAVIOR NODE BY MOBILE AGENTS IN DSR AD HOC WIRELESS NETWORKS

CHAWDEE BARAMEE

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN COMPUTER ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2006

ISBN 974-15-2208-8

หัวข้อวิทยานิพนธ์	การตรวจจับโหนดที่มีพฤติกรรมละทิ้งข้อมูลอย่างผิดปกติด้วยโมไบล์เอเจนต์ในเครือข่ายไร้สายแอดฮอคแบบ DSR
ชื่อนักศึกษา	นาย ชาวดี บารมี
รหัสประจำตัว	45061043
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
พ.ศ.	2549
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ.ดร ศักดิ์ชัย ทิพย์จักษุรัตน์

บทคัดย่อ

งานวิจัยฉบับนี้ได้เสนอวิธีการตรวจจับโหนดที่มีพฤติกรรมผิดปกติ (Misbehaving node) ในขณะที่มีรับส่งข้อมูลในเครือข่ายไร้สายแบบแอดฮอค ที่ใช้โปรโตคอลการค้นหาเส้นทางแบบดีเอสอาร์ โดยการใช้โหนดสื่อสารที่อยู่ในเครือข่ายทำหน้าที่เป็นโมไบล์เอเจนต์ เพื่อทำการตรวจสอบพฤติกรรมการรับและส่งข้อมูลของโหนดที่เป็นตัวกลางทำหน้าที่นำส่งข้อมูล โดยกำหนดสมมติฐานว่าโหนดที่ถูกระบุอยู่ในแพ็กเก็ตตอบกลับเส้นทาง จะต้องมีพฤติกรรมการรับและส่งต่อข้อมูลเพื่อให้บริการสื่อสารระหว่างต้นทางและปลายทาง หากไม่มีการส่งข้อมูลใดออกมาจากโหนดังกล่าวภายในเวลาที่กำหนด ก็จะตัดสินได้ว่าโหนดมีพฤติกรรมการนำส่งข้อมูลผิดปกติสำหรับการสื่อสารครั้งนั้น โมไบล์เอเจนต์จะทำการแจ้งความผิดปกตินี้ของโหนดดังกล่าวให้แก่เครือข่ายเพื่อให้กระบวนการค้นหาเส้นทางการสื่อสารครั้งต่อไป สามารถหลีกเลี่ยงการใช้งานโหนดที่มีพฤติกรรมผิดปกติดังกล่าว ผลที่ได้คือทำให้การสื่อสารในเครือข่ายไร้สายแบบแอดฮอคมีประสิทธิภาพดีขึ้น

Thesis Title	Detection of Packet Dropping Misbehavior Node by Mobile Agents in DSR Ad Hoc Wireless Networks
Student	Chawdee Baramee
Student ID.	45061043
Degree	Master of engineering
Programme	Computer engineering
Year	2006
Thesis Advisor	Asst. Prof. Sakchai Thipchaksurat

ABSTRACT

This research proposes a methodology to detect misbehaving nodes in ad-hoc wireless networks that uses Dynamic Source Routing (DSR) for discovering a transmission path. The mobile agents are employed in the networks for monitoring the data communication at each intermediate node on the transmission path. The misbehaving nodes, detected by the mobile agents, are to be verified by the destination node in order to reduce the monitoring error. For final data analysis, destination nodes will exchange the misbehaving nodes information with other nodes in the networks. This information is later compared with the highest acceptable failure of networks to whether the intermediate nodes misbehave or not.

กิตติกรรมประกาศ

คุณความดีอันใดที่บังเกิดจากวิทยานิพนธ์ฉบับนี้ ขอมอบแด่บิดาและมารดาของผู้วิจัย ผู้ที่คอยห่วงใย เอาใจใส่ เป็นแรงใจในการทำวิทยานิพนธ์ฉบับนี้และให้การสนับสนุนการศึกษามาโดยตลอด

วิทยานิพนธ์ฉบับนี้ประสบความสำเร็จลุล่วงได้เป็นอย่างดี โดยได้รับความกรุณาจาก ผศ.ดร. ศักดิ์ชัย ทิพย์จักษุรัตน์ ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ที่ได้ให้ความเอาใจใส่แนะนำความรู้และทฤษฎีต่างๆที่ใช้ ชี้แนะแนวทางการแก้ปัญหา ให้คำปรึกษาและให้ความช่วยเหลือเสมอมา ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์จากท่านและขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณกรรมการสอบวิทยานิพนธ์ทุกท่านที่ได้กรุณาให้คำแนะนำในทุกๆ เรื่อง ทั้งวิธีการแก้ปัญหาที่เกิดขึ้นในวิทยานิพนธ์และมุมมองในเชิงวิศวกรรมอื่นๆ ซึ่งช่วยให้ผู้วิจัยมีวิสัยทัศน์ที่กว้างไกลขึ้น

ขอขอบคุณอาจารย์ทุกๆท่านที่ประสิทธิ์ประสาทวิชาความรู้ คำแนะนำต่างๆในการศึกษาและการทำวิจัยจนสำเร็จได้ด้วยดี รวมทั้งคำสั่งสอนและอบรมให้ข้าพเจ้าเป็นคนดี ข้าพเจ้าขอกราบขอบพระคุณเป็นอย่างสูง

ข้าพเจ้าขอขอบคุณสำหรับกำลังใจ คำแนะนำ และประสบการณ์ที่ดีจาก พี่ ๆ เพื่อน ๆ และน้อง ๆ นักศึกษาป.โททุกท่าน ที่ทำให้บรรยากาศในห้องวิจัยเป็นไปด้วยความสนุกสนาน โดยเฉพาะอย่างยิ่ง น.ส. ปองเกษม พลสันติกุล ที่ได้คอยช่วยเหลือในส่วนเอกสารและบทความวิชาการที่เป็นภาษาอังกฤษ ทำให้การจัดทำบทความสามารถสำเร็จลงได้ด้วยดี

ขอขอบคุณ บัณฑิตวิทยาลัยและบัณฑิตศึกษา สถาบันเทคโนโลยีประจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ให้การสนับสนุนการทำวิทยานิพนธ์นี้

สุดท้ายนี้ หากวิทยานิพนธ์ฉบับนี้มีข้อผิดพลาดประการใดข้าพเจ้าขอน้อมรับไว้เพียงผู้เดียว

ชาวดี บารมี

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันระบบเครือข่ายคอมพิวเตอร์แบบไร้สาย (Wireless LAN) เป็นสิ่งที่ได้รับความนิยมเป็นอย่างสูง เพราะมีค่าใช้จ่ายในการติดตั้งไม่มากนักเหมือนในอดีต และมีความสะดวกในการใช้งานและเคลื่อนย้ายสูงกว่าเครือข่ายแบบมีสายมาก รวมถึงอุปกรณ์คอมพิวเตอร์แบบเคลื่อนที่ได้ทั้งคอมพิวเตอร์กระเป๋าหิ้วหรือพีดีเอรุ่นใหม่ๆ ได้มีการติดตั้งอุปกรณ์การสื่อสารแบบไร้สายไว้เป็นอุปกรณ์มาตรฐานแล้วทั้งสิ้น

เครือข่ายไร้สายแบบแอดฮอค (Ad Hoc Wireless Network) เป็นอีกรูปแบบการสื่อสารของการสื่อสารแบบไร้สายที่อุปกรณ์สามารถสื่อสารกันได้โดยตรง โดยไม่จำเป็นต้องใช้อุปกรณ์กระจายสัญญาณหรือแอคเซสพอยต์ ทำให้ระบบเครือข่ายไร้สายแบบแอดฮอคมีจุดเด่นคือการที่สามารถจัดตั้งและยกเลิกเครือข่ายได้อย่างรวดเร็ว จึงเหมาะสมอย่างยิ่งกับเครือข่ายที่จัดตั้งเพื่อการทำงานแบบเฉพาะกิจ เช่นเครือข่ายสำหรับสนามรบ หรืองานสัมมนาต่างๆ

ระบบความปลอดภัยของเครือข่าย ถือเป็นจุดอ่อนที่เปราะบางที่สุดอย่างหนึ่งในการใช้งานเครือข่ายไร้สาย เนื่องจากเครือข่ายไร้สายมีความเป็นระบบเปิดอย่างสมบูรณ์เพราะคลื่นสัญญาณที่รับส่งมีการกระจายในพื้นที่สื่อสาร ทำให้การสื่อสารถูกเฝ้าฟังและโจมตีจากผู้บุรุกที่อยู่ในบริเวณนั้นได้อย่างง่ายดาย ในปัจจุบันได้มีการพัฒนารูปแบบการโจมตีบนเครือข่ายไร้สายในหลายรูปแบบ โดยแต่ละแบบได้สร้างความเสียหายแก่เครือข่ายแตกต่างกันไป เช่นการปลอมแปลงข้อมูลที่ส่ง, การเฝ้าฟังข้อมูลเพื่อนำไปใช้, การเปลี่ยนแปลงเส้นทางการสื่อสาร หรือการโจมตีเครือข่ายโดยการส่งข้อมูลจำนวนมากเพื่อให้เครือข่ายไม่สามารให้บริการได้เป็นต้น ผลเสียที่เกิดขึ้นนอกจากจะทำให้เครือข่ายมีประสิทธิภาพการให้บริการและความน่าเชื่อถือลดลงแล้ว ยังอาจส่งผลให้ผู้ใช้งานขาดความมั่นใจในการใช้งานระบบเครือข่ายได้อีกด้วย

ระบบตรวจจับการบุกรุกบนเครือข่าย (Network Intrusion Detection System: NIDS) นับว่าเป็นเครื่องมือบริหารจัดการเครือข่ายที่ได้รับความนิยมสูงขึ้นในระยะหลัง เนื่องจากปัญหาการบุกรุกและโจมตีบนเครือข่ายคอมพิวเตอร์ได้ขยายขอบเขตและสร้างความเสียหายมากขึ้น เครือข่ายที่ได้รับการติดตั้งระบบตรวจจับการบุกรุกจะมีความสามารถในการตรวจสอบความผิดปกติที่เกิดขึ้นได้อย่างถูกต้องในเวลาอันรวดเร็ว ส่งผลให้การแก้ไขปัญหาสามารถทำได้ก่อนที่ความเสียหายจะลุกลามมากยิ่งขึ้น

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

- เพื่อศึกษารูปแบบการบุกรุกและโจมตีบนเครือข่ายไร้สายแบบแอดฮอค และการทำงานของระบบตรวจจับความผิดปกติบนเครือข่ายที่ได้มีการศึกษามาก่อนโดยนักวิจัยอื่นๆ
- พัฒนาโครงสร้างพื้นฐานสำหรับการเฝ้าฟัง ตรวจสอบ และรวบรวมข้อมูลพฤติกรรมการสื่อสารของโหนดในเครือข่ายไร้สายแบบแอดฮอค เพื่อนำมาใช้วิเคราะห์หาลักษณะการเป็นผู้บุกรุกของโหนด
- เพื่อหาแนวทางการเพิ่มประสิทธิภาพของการสื่อสารในเครือข่าย โดยการใช้ข้อมูลลักษณะการเป็นผู้บุกรุกของโหนดในเครือข่ายมาใช้พิจารณาหาเส้นทางการสื่อสารที่ปลอดภัยมากขึ้น

1.3 สมมุติฐานของการศึกษา

การโจมตีแบบลดทิ้งข้อมูล (Packet dropping) เป็นการโจมตีรูปแบบหนึ่งที่ผู้บุกรุกทำหน้าที่เป็นโหนดตัวกลางในเส้นทางไม่ทำการนำส่งข้อมูล (Packet forwarding) ไปยังโหนดตัวถัดไป (Next hop) หลังจากที่ได้รับข้อมูลจากโหนดก่อนหน้า (Previous hop) ทำให้เส้นทางการสื่อสารนั้นไม่สามารถให้บริการได้ พฤติกรรมการโจมตีดังกล่าวสร้างความเสียหายลักษณะเดียวกันกับการที่โหนดตัวกลางเคลื่อนที่ออกจากรัศมีการสื่อสาร ซึ่งถือเป็นความเสียหายทั่วไปที่เกิดขึ้นได้บนเครือข่ายไร้สายแบบแอดฮอค ความแตกต่างกันที่สามารถบ่งชี้ได้ว่าความเสียหายดังกล่าวมีสาเหตุจากการโจมตีหรือเกิดขึ้นตามปกติมีเพียงจำนวนครั้งของการเกิดพฤติกรรมเท่านั้น ในการตรวจจับความผิดปกติเพื่อตัดสินสภาพการเป็นผู้บุกรุกของโหนด จึงต้องทำการเฝ้าฟังพฤติกรรมการนำส่งข้อมูลของโหนดตัวกลางแต่ละตัวเพื่อหาความถี่ในการเกิดพฤติกรรมดังกล่าว โหนดที่มีความถี่ของการเกิดพฤติกรรมผิดปกติสูงกว่าปกติ จะถือว่ามีสภาพการเป็นผู้บุกรุก

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

ปัญหาสำคัญที่ทำให้ระบบตรวจจับความผิดปกติบนเครือข่ายแบบสายไม่สามารถนำมาประยุกต์ใช้กับระบบเครือข่ายไร้สายแบบแอดฮอคได้ เนื่องจากเครือข่ายไร้สายแบบแอดฮอคไม่มีการทำงานผ่านอุปกรณ์รวมและกระจายสัญญาณผ่านทางเราเตอร์หรือสวิตช์ดังเช่นเครือข่ายแบบใช้สาย ทำให้การรวบรวมข้อมูลทั้งหมดในเครือข่ายเพื่อนำมาวิเคราะห์ทำได้ยาก และไม่ครบถ้วน

โหนดสื่อสารถือเป็นทรัพยากรที่สำคัญที่สุดในเครือข่าย นอกเหนือจากการทำหน้าที่รับส่งข้อมูลเพื่อบริการแก่ผู้ใช้งานแล้ว การใช้โหนดสื่อสารเพื่อทำหน้าที่เป็นผู้ตรวจจับความผิดปกติจะ

ช่วยให้ระบบตรวจจับมีประสิทธิภาพสูงขึ้นมาก เนื่องจากโหนดสื่อสารมีการกระจายตัวในเครือข่ายอยู่แล้ว เมื่อนำโหนดสื่อสารมาทำหน้าที่เฝ้าฟังเพื่อตรวจสอบพฤติกรรมการนำส่งข้อมูลของโหนดตัวกลาง จะทำให้ระบบตรวจจับความผิดปกติรวบรวมข้อมูลพฤติกรรมของโหนดต้องสงสัยได้อย่างถูกต้องครบถ้วน

1.5 ขอบเขตของการศึกษา

เพื่อศึกษาและทดลองถึงประสิทธิภาพการทำงานของตรวจจับโหนดที่มีพฤติกรรมการนำส่งข้อมูลที่ผิดปกติ โดยที่

1. วิทยานิพนธ์นี้เป็นการตรวจจับโหนดในเครือข่ายไร้สายแบบแอดฮอค ที่ใช้โปรโตคอลการค้นหาเส้นทางแบบ DSR เท่านั้น
2. การทำงานของโปรโตคอลค้นหาเส้นทางจะทำงานแบบพื้นฐานเท่านั้น กระบวนการทำงานที่เป็นส่วนขยายของโปรโตคอลจะไม่นำมาพิจารณาในการทดลอง
3. เป้าหมายหลักของวิทยานิพนธ์คือการค้นหาโหนดที่มีพฤติกรรมผิดปกติ และหลีกเลี่ยงการใช้โหนดดังกล่าวในเส้นทางการสื่อสาร ประเด็นความปลอดภัยในด้านอื่นที่เกิดจากการทำงานภายใต้วิธีการของวิทยานิพนธ์นี้ จะไม่นำถูกนำมาพิจารณา แต่วิทยานิพนธ์จะนำเสนอถึงแนวทางการแก้ไขในประเด็นดังกล่าว
4. การทดลองในวิทยานิพนธ์นี้ใช้การจำลองการทำงานของเครือข่ายไร้สาย ผ่านทางโปรแกรม NS-2 (Network Simulation 2)
5. สภาพแวดล้อมของเครือข่ายที่ใช้ในการทดลอง เป็นการใช้ข้อมูลที่อ้างอิงจากงานวิจัยที่เกี่ยวข้อง เพื่อให้ผลที่ได้สามารถนำไปอ้างอิงหรือทำการวิจัยต่อได้ภายใต้สภาพแวดล้อมเดียวกัน

1.6 ขั้นตอนของการศึกษา

- ศึกษารูปแบบการโจมตี และวิธีการตรวจจับจากงานวิจัยที่เคยมีผู้นำเสนอ
- ศึกษาทฤษฎีและแนวทางการสร้างระบบตรวจจับพฤติกรรมที่ผิดปกติของโหนดสื่อสารสำหรับเครือข่ายไร้สายแบบแอดฮอค
- สร้างสภาพแวดล้อมจำลองเครือข่ายเพื่อทดลองและวัดผล
- ศึกษาผลกระทบที่เกิดขึ้นเมื่อระบบตรวจจับมีการทำงานบนเครือข่าย
- สรุปผลการทดลองพร้อมจัดทำเอกสารวิทยานิพนธ์

1.7 ประโยชน์ที่เกิดจากงานวิจัยนี้

- แสดงให้ทราบถึงการใช้ประโยชน์จากข้อมูลของโปรโตคอลการสื่อสารนอกเหนือจากการควบคุมการสื่อสารแล้ว ยังสามารถนำมาใช้พิจารณาลักษณะความผิดปกติของโหนดได้อีกด้วย
- แสดงการเปรียบเทียบความสามารถของระบบตรวจจับความผิดปกติแบบต่างๆ ที่มีจุดเด่นและจุดด้อยเมื่อทำงานบนสภาพแวดล้อมทางเครือข่ายที่แตกต่างกัน เพื่อนำข้อมูลดังกล่าวไปใช้ในการพิจารณาเลือกใช้งานระบบตรวจจับต่อไป

1.8 รายละเอียดในแต่ละบท

วิทยานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 6 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ ขอบเขตของงานวิจัยและขั้นตอนการศึกษา

บทที่ 2 กล่าวถึงระบบเครือข่ายความเป็นมาและจุดเด่นของไร้สายแบบแอดฮอค รูปแบบการทำงานที่มีความแตกต่างกับเครือข่ายแบบสายหรือเครือข่ายไร้สายแบบอื่นๆ รวมถึงการทำงานโปรโตคอลค้นหาเส้นทางการสื่อสารที่มีการใช้งานบนเครือข่ายไร้สายแบบแอดฮอค

บทที่ 3 กล่าวถึงการโจมตีรูปแบบต่างๆ บนเครือข่ายไร้สายแบบแอดฮอคที่มีวิวัฒนาการมาจากการโจมตีบนเครือข่ายแบบสาย จนกระทั่งถึงรูปแบบการโจมตีที่เกิดเฉพาะบนเครือข่ายไร้สายแบบแอดฮอค ในส่วนท้ายของบทจะได้กล่าวถึงการทำงานของตรวจจับความผิดปกติที่ได้มีการศึกษามาก่อนจากนักวิจัยอื่นๆ รวมถึงชี้ให้เห็นถึงจุดด้อยของระบบดังกล่าว

บทที่ 4 กล่าวถึงแนวคิดและการออกแบบระบบตรวจจับความผิดปกติของโหนดสื่อสารในเครือข่ายของงานวิจัยที่นำเสนอ โดยมีการแบ่งเป็นสามส่วนใหญ่ๆ คือ วิธีการเฝ้าฟัง, การตรวจสอบและยืนยันความถูกต้องของข้อมูลจากการเฝ้าฟัง และการแลกเปลี่ยนข้อมูลเพื่อตัดสินลักษณะการเป็นผู้บุรุก

บทที่ 5 กล่าวถึงวิธีประเมินประสิทธิภาพการทำงานของระบบตรวจจับโดยใช้มาตรวัดต่างๆ การดำเนินการทดลองจากสภาพแวดล้อมจำลองและแสดงผลการทดลองทั้งหมด โดยเป็นการเปรียบเทียบความสามารถของระบบตรวจจับที่นำเสนอกับระบบตรวจจับอื่น

บทที่ 6 กล่าวถึงการสรุป ข้อเสนอแนะ และแนวทางการทำวิจัยต่อ

บทที่ 2
ระบบเครือข่ายไร้สายแบบแอดฮอค

2.1 บทนำ

เครือข่ายไร้สายแบบแอดฮอค [1][2][3] คือการรวมตัวกันของอุปกรณ์ไร้สายตั้งแต่ 2 ตัวขึ้นไป ที่มีความสามารถทำการสื่อสารกันได้โดยปราศจากการใช้อุปกรณ์กระจายสัญญาณใดๆ โดยเครือข่ายจะคอยจัดการตัวเองและดัดแปลงรูปแบบการสื่อสาร (Self-organization and Adaptive) เพื่อสร้างเส้นทางการสื่อสารระหว่างโหนดต้นทางและปลายทางอยู่ตลอดเวลา โดยไม่ต้องมีการควบคุมจากศูนย์กลาง (De-centralize system) ทำให้เครือข่ายไร้สายแบบแอดฮอคเหมาะสมอย่างยิ่งสำหรับงานที่ต้องการความรวดเร็วในการจัดตั้งและยกเลิกการใช้งานเครือข่าย เช่นระบบเครือข่ายในงานประชุม หรือในสนามรบ

2.2 การทำงานของเครือข่ายไร้สายแบบแอดฮอค

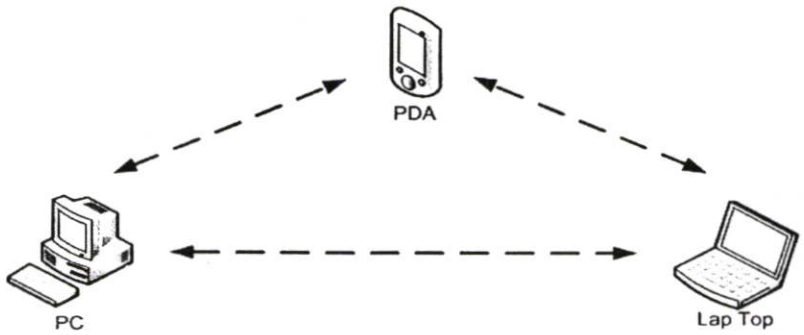
รูปแบบการสื่อสารในเครือข่ายไร้สายแบบแอดฮอค ทำงานอยู่บนพื้นฐานของการสื่อสารแบบเพียร์ทูเพียร์ (Peer to Peer Network [4]) โหนดแต่ละตัวจะมีหน้าที่หลักคือการนำส่งข้อมูลไปยังโหนดข้างเคียง (Neighbor Node) ให้เป็นไปอย่างถูกต้องเท่านั้น ส่วนกระบวนการนำส่งไปยังโหนดปลายทางจะขึ้นอยู่กับโครงสร้างการเชื่อมต่อโครงข่าย (Network Topology) ของโหนดในเครือข่าย ซึ่งมีอยู่สองรูปแบบคือ

2.2.1 การสื่อสารโดยตรง (Directly connect)

เป็นรูปแบบการส่งสำหรับเครือข่ายมีพื้นที่ไม่กว้างนัก ทำงานโดยสัญญาณวิทยุที่มีกำลังเพียงพอที่ทำให้โหนดต้นทางสามารถส่งข้อมูลไปยังโหนดปลายทางได้โดยตรง การทำงานลักษณะนี้เป็นรูปแบบที่พื้นฐานที่สุดสำหรับเครือข่ายแบบไร้สายแบบแอดฮอค ซึ่งคอมพิวเตอร์ส่วนบุคคลหรืออุปกรณ์พกพาต่างๆ ในท้องตลาดที่มีการติดตั้งอุปกรณ์ไร้สายมักจะถูกออกแบบมาให้สื่อสารให้รูปแบบนี้ได้โดยไม่ต้องมีการติดตั้งซอฟแวร์เพิ่มเติม เนื่องจากระบบปฏิบัติการคอมพิวเตอร์ทั้งวินโดว์สและลีนุกซ์ต่างมีความสามารถในการเชื่อมต่อรูปแบบนี้มาอยู่แล้ว

ข้อเสียเปรียบของการสื่อสารโดยตรง คือรัศมีการสื่อสารหรือพื้นที่การให้บริการที่ถูกจำกัดจากความสามารถของตัวอุปกรณ์ไร้สายเอง เนื่องจากขีดความสามารถของอุปกรณ์ในการนำส่งข้อมูลที่ทำได้ไม่ไกลนักเพราะมีข้อจำกัดด้านพลังงานและขนาดของเสาอากาศ ทำให้การสื่อสารรูปแบบนี้จะทำได้ก็ต่อเมื่ออุปกรณ์ทั้งสองอยู่ในรัศมีการสื่อสารของกันและกันเท่านั้น การใช้งานที่

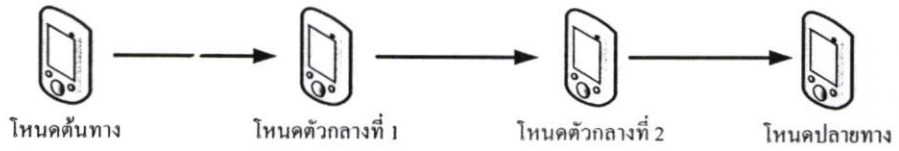
พบเห็นโดยทั่วไปจะเป็นการสื่อสารกันระหว่างอุปกรณ์ในบ้านหรือสำนักงานขนาดเล็ก โดยมีจุดประสงค์เพื่อแลกเปลี่ยนข้อมูลระหว่างกันเท่านั้น



รูปที่ 2.1 แสดงการสื่อสารโดยตรงระหว่างโหนด

2.2.2 การสื่อสารผ่านโหนดตัวกลาง (Multi-hop connect)

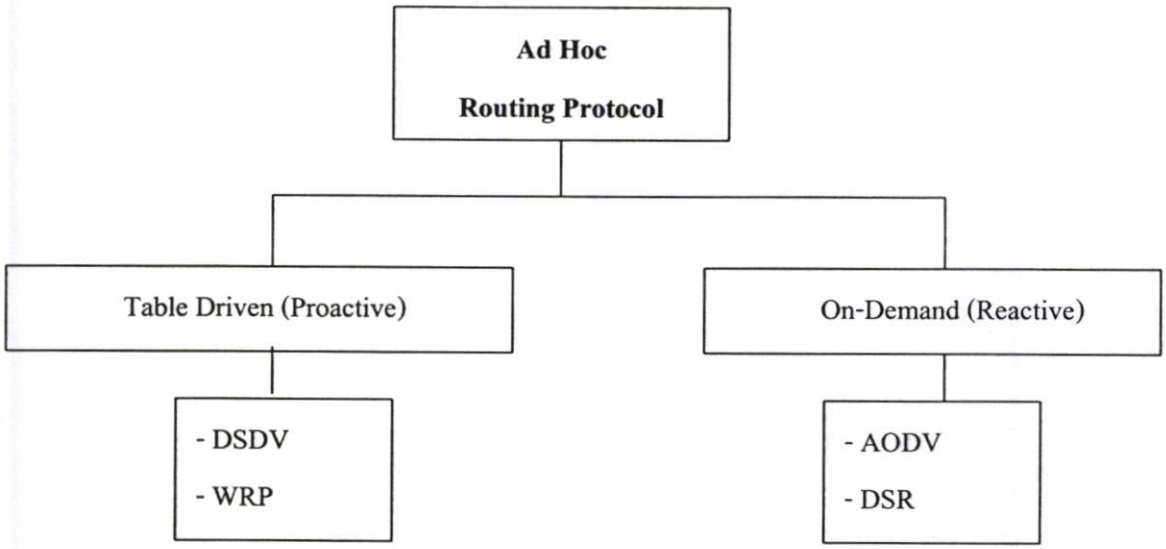
การสื่อสารลักษณะนี้ถูกออกแบบมารองรับการทำงานสำหรับเครือข่ายที่มีพื้นที่เครือข่ายที่กว้างซึ่งโหนดต้นทางอาจไม่สามารถสื่อสารกับโหนดปลายทางได้โดยตรง เนื่องจากรัศมีการสื่อสารของอุปกรณ์มีระยะไม่เพียงพอ จึงต้องมีอุปกรณ์ทำหน้าที่ทวนหรือกระจายสัญญาณเพื่อเพิ่มระยะทางการสื่อสาร แนวคิดพื้นฐานของเครือข่ายไร้สายแบบแอดฮอคคือการให้โหนดข้างเคียงทำหน้าที่เป็นตัวกลางช่วยส่งข้อมูลต่อกันไปจนถึงโหนดปลายทาง โดยเลียนแบบการทำงานของเราเตอร์ที่ทำหน้าที่เชื่อมต่อเครือข่ายย่อยๆ หลายเครือข่ายเพื่อให้เครือข่ายที่อยู่ห่างกันสามารถสื่อสารกันได้



รูปที่ 2.2 แสดงการนำส่งบนเครือข่ายโดยข้อมูลถูกนำส่งผ่านโหนดตัวกลาง

2.3 โปรโตคอลค้นหาเส้นทางบนเครือข่ายไร้สายแบบแอดฮอค

โปรโตคอลค้นหาเส้นทางสำหรับเครือข่ายไร้สายแบบแอดฮอค (Ad hoc Routing Protocol [5]) ถือเป็นองค์ประกบสำคัญที่ทำให้โหนดสามารถสื่อสารกันภายในเครือข่ายได้ มีหน้าที่หลักคือการค้นหาเส้นทางที่เป็นไปได้สำหรับการนำส่งข้อมูลจากต้นทางไปยังปลายทาง และทำการปรับปรุงข้อมูลเส้นทางการสื่อสารเมื่อโครงสร้างเครือข่ายมีการเปลี่ยนแปลง ในปัจจุบันโปรโตคอลค้นหาเส้นทางสำหรับเครือข่ายไร้สายแบบแอดฮอคถูกคิดค้นและพัฒนาขึ้นมาเป็นจำนวนมาก สามารถจำแนกประเภทของโปรโตคอลค้นหาเส้นทางที่มีอยู่ได้เป็นสองประเภทคือ โปรโตคอลการค้นหาเส้นทางที่ทำงานแบบ Table Driven (Proactive) และโปรโตคอลการค้นหาเส้นทางที่ทำงานแบบ On-Demand (Reactive)



รูปที่ 2.3 ประเภทและตัวอย่างของโปรโตคอลค้นหาเส้นทางบนเครือข่ายไร้สายแบบแอดฮอคที่ได้รับความนิยม

2.3.1 Table Driven (Proactive) Routing Protocol

การทำงานของโปรโตคอลค้นหาเส้นทางประเภทนี้ เป็นการประยุกต์วิธีการค้นหาเส้นทางมาจากเครือข่ายแบบสาย ที่มีการกำหนดช่วงเวลาปรับปรุงตารางเส้นทางการสื่อสาร (Routing Table) เพื่อเตรียมพร้อมสำหรับการใช้เส้นทางสื่อสารที่อาจเกิดขึ้น ตัวอย่างของโปรโตคอลที่ได้รับความนิยมคือ

2.3.1.1 Destination Sequence Distance Vector (DSDV)

DSDV [6] เป็นโปรโตคอลที่ทำงานบนพื้นฐานทฤษฎีของ Bellman-Ford Algorithm [7] ซึ่งถือเป็นแม่แบบของโปรโตคอลค้นหาเส้นทางบนเครือข่ายแบบสายที่ใช้กันในปัจจุบัน มีหลักการคือ โหนดในเครือข่ายจะสร้างตารางการเชื่อมต่อจากตนเองไปยังโหนดปลายทางทุกตัวในเครือข่าย ไม่ว่าจะโหนดดังกล่าวจะเคยมีการสื่อสารมากก่อนหรือไม่ ภายในตารางจะระบุถึงเมตริกซ์หรือจำนวนฮอปที่ต้องใช้ในการสื่อสารไปยังโหนดปลายทาง เพื่อระบุว่าโหนดปลายทางนั้นมีการเชื่อมต่อกับตนเอง (Reachable) ข้อมูลในตารางการเชื่อมต่อจะถูกแลกเปลี่ยนกันกับโหนดข้างเคียงที่สามารถติดต่อได้ โดยทุกโหนดจะต้องปรับปรุงข้อมูลการเชื่อมต่อตามเวลาที่กำหนด หรือเมื่อมีข้อผิดพลาดจากการนำส่งข้อมูล

2.3.1.2 Wireless Routing Protocol (WRP)

WRP [2] ถูกพัฒนาให้ลดความเสียหายเมื่อโครงสร้างเครือข่ายเกิดการเปลี่ยนแปลง โดยมีแนวคิดการในทำงานของคือการเพิ่มวิธีการตรวจสอบสภาพการเชื่อมต่อกับโหนดข้างเคียง โดยการส่งข้อความ (Message) เพื่อตรวจสอบการเชื่อมต่อภายในเวลาที่กำหนด และใช้ข้อมูลตอบกลับ (Acknowledge) เพื่อตรวจสอบความล้มเหลวของเส้นทางการสื่อสารแทนการแลกเปลี่ยนตารางการเชื่อมต่อทั้งหมด เพื่อลดภาระการทำงานของเครือข่าย ทำให้นอกเหนือจากข้อมูลตารางการเชื่อมต่อที่มีการเก็บไว้บนโหนดแล้ว โปรโตคอล WRP ยังมีการเก็บข้อมูลสำคัญเช่นข้อมูล Message List ซึ่งจะคอยบอกถึงเวลาการปรับปรุงข้อมูลการสื่อสารในแต่ละเส้นทาง ส่งผลให้การปรับปรุงหรือแลกเปลี่ยนข้อมูลในตารางการเชื่อมต่อสามารถทำได้โดยไม่ต้องรอให้ครบตามเวลาที่กำหนด

2.3.2 On-Demand (Reactive) Routing Protocol

โปรโตคอลการค้นหาเส้นทางแบบตามความต้องการหรือ On-Demand ได้ถูกพัฒนาขึ้นเพื่อแก้ไขจุดอ่อนของโปรโตคอลแบบแรกที่ต้องมีการปรับปรุงเส้นทางการสื่อสารตามช่วงเวลาที่กำหนดเท่านั้น หากเครือข่ายมีการเปลี่ยนแปลงโครงสร้างหลังจากมีการปรับปรุงเส้นทางการสื่อสารแล้ว จะไม่สามารถนำข้อมูลดังกล่าวมาใช้ในการนำส่งได้ ซึ่งไม่เหมาะสมกับการนำมาใช้ในเครือข่ายที่โครงสร้างมีการเปลี่ยนแปลงบ่อยครั้งอย่างเครือข่ายไร้สายแบบแอดฮอค โปรโตคอลการค้นหาเส้นทางแบบตามความต้องการจึงถูกออกแบบให้ค้นหาเส้นทางการสื่อสารเมื่อโหนดต้องการจะส่งข้อมูลเท่านั้น โดยเมื่อโปรโตคอลค้นหาเส้นทางที่ทำงานอยู่ในระดับชั้นเน็ตเวิร์ก (Network Layer [8]) รับทราบว่าชั้นแอพพลิเคชันมีข้อมูลที่ต้องการส่งจึงจะเริ่มทำการค้นหาเส้นทาง เมื่อได้เส้นทางการสื่อสารแล้วจึงจะนำส่งข้อมูลไปยังปลายทาง และจะใช้งานเส้นทางที่ค้นหาได้นั้นทำการนำส่งข้อมูลเพียงเส้นทางเดียวจนเสร็จสิ้น (Single path transmission) โปรโตคอลการค้นหาเส้นทางแบบตามความต้องการที่ได้รับความนิยมกันในปัจจุบันมีดังนี้

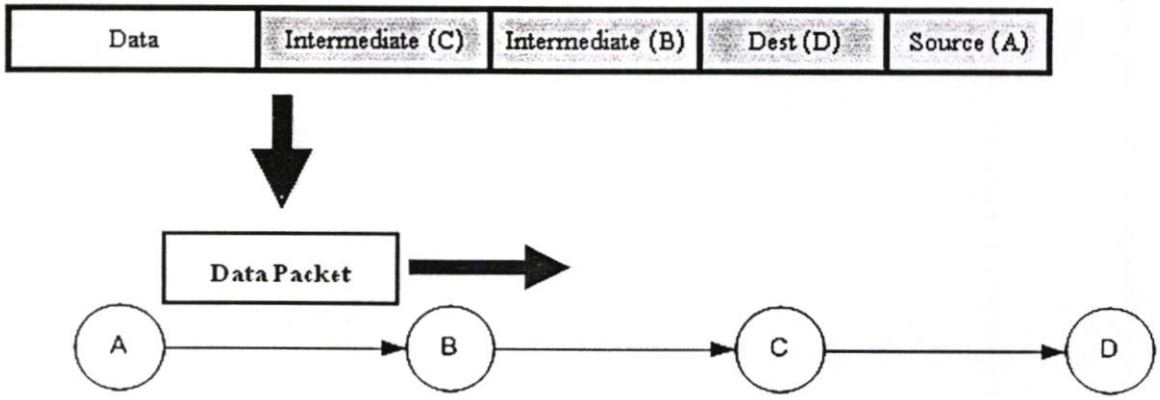
2.3.2.1 Ad Hoc On-Demand Distance Vector (AODV)

AODV [9] เป็นโปรโตคอลการค้นหาเส้นทางที่ได้รับการพัฒนาจากโปรโตคอล DSDV โดยทุกโหนดจะยังคงสร้างตารางการเชื่อมต่อจากตนเองไปยังโหนดข้างเคียง แต่เส้นทางดังกล่าวจะต้องถูกค้นหาเมื่อต้องการส่งข้อมูลเท่านั้น การทำงานจะเริ่มจากการส่งข้อมูลร้องขอเส้นทาง (Route Request) ไปยังโหนดข้างเคียงทุกตัว โหนดข้างเคียงจะทำหน้าที่เป็นตัวกลางส่งต่อการร้องขอจนกระทั่งถึงโหนดปลายทาง ซึ่งโหนดปลายทางจะตอบกลับด้วยข้อมูลตอบกลับ (Route Reply) ผ่านเส้นทางที่สั้นที่สุด (Shortest Path) โหนดตัวกลางในเส้นทางจะบันทึกข้อมูลลงในตารางการเชื่อมต่อของตนเองในระหว่างที่ข้อมูลตอบกลับถูกนำส่ง เมื่อโหนดต้นทางได้รับข้อมูลตอบกลับจึงจะทำการส่งข้อมูลออกไปในเส้นทางที่ค้นหาได้

2.3.2.2 Dynamic Source Routing (DSR)

โปรโตคอลค้นหาเส้นทางที่กล่าวมาแล้วทั้งหมดนั้น ล้วนได้รับพัฒนาจากพื้นฐานที่ไม่มีความเหมาะสมกับเครือข่ายไร้สายแบบแอดฮอคอย่างแท้จริง ด้วยเหตุนี้จึงทำให้มหาวิทยาลัย Carnegie Mellon ในประเทศสหรัฐอเมริกาได้จัดตั้งโครงการชื่อ Monarch [10] ที่มีจุดมุ่งหมายเพื่อทำการวิจัยและพัฒนาโปรโตคอลการค้นหาเส้นทาง ที่เหมาะสมกับกับการทำงานบนเครือข่ายไร้สายแบบแอดฮอค จนได้โปรโตคอลการค้นหาเส้นทางที่ชื่อว่า DSR [11]

แนวคิดการออกแบบที่ทำให้โปรโตคอล DSR มีความแตกต่างกับโปรโตคอลอื่นอย่างเด่นชัด คือการที่โปรโตคอล DSR จะไม่มีการเก็บข้อมูลตารางเชื่อมต่อในรูปของหน่วยความจำไว้บนโหนดที่เป็นตัวกลางการสื่อสาร แต่เส้นทางการสื่อสารที่ได้จากกระบวนการค้นหาจะถูกแสดงไว้ในส่วนหัว (Header) ของทุกแพ็กเก็ต โดยโหนดตัวกลางจะใช้ข้อมูลดังกล่าวในการระบุถึงผู้รับเมื่อทำการส่งข้อมูล ประโยชน์ของแนวคิดนี้คือการที่โหนดแต่ละตัวสามารถทราบถึงเส้นทางการสื่อสารในเครือข่ายได้ โดยการเฝ้าฟังแพ็กเก็ตข้อมูลที่โหนดอื่นทำการสื่อสารอยู่แบบโพรมิสคิวอัส (Promiscuous [12]) ข้อมูลเส้นทางการสื่อสารที่เฝ้าฟังจะช่วยให้โหนดที่เฝ้าฟังสามารถใช้เส้นทางการสื่อสารดังกล่าวได้โดยไม่จำเป็นต้องทำกระบวนการค้นหาเส้นทางใหม่



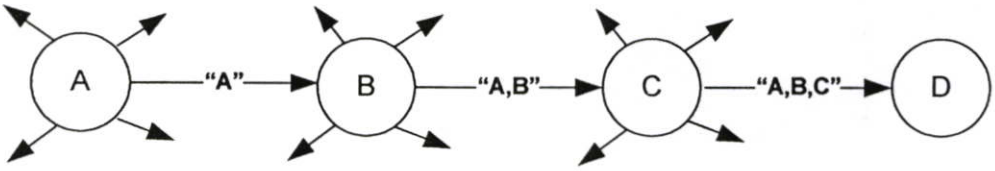
รูปที่ 2.4 แสดงข้อมูลที่นำส่งเมื่อใช้โปรโตคอลค้นหาเส้นทางแบบ DSR

2.4 การค้นหาเส้นทางของโปรโตคอล DSR

การค้นหาเส้นทางสื่อสารของโปรโตคอล DSR จะเริ่มต้นทำงานเมื่อระดับชั้นเน็ตเวิร์กของโหนดต้นทางตรวจพบว่ามีข้อมูลที่ต้องการนำส่งไปยังปลายทาง โดยกระบวนการค้นหาเส้นทางจะมีการทำงานเป็นสองขั้นตอนคือ

1. การร้องขอข้อมูลเส้นทาง (Route Request)

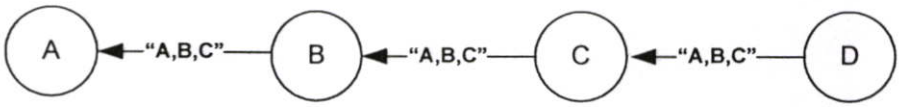
การร้องขอข้อมูลเส้นทางจะทำโดยโหนดต้นทางที่ต้องการส่งข้อมูล เพื่อค้นหาว่ามีเส้นทางใดที่เชื่อมต่อระหว่างตนเองและโหนดปลายทางบ้าง เริ่มต้นโดยโหนดต้นทางจะสร้างแพ็กเก็ตร้องขอข้อมูลเส้นทาง (Route Request Packet) และส่งไปยังโหนดข้างเคียงทุกตัวในลักษณะการส่งแบบบรอดแคสต์ โหนดที่ได้รับแพ็กเก็ตจะตรวจสอบว่าตนเองเป็นปลายทางของการร้องขอหรือไม่ หากตนเองไม่ได้เป็นโหนดปลายทางจะต้องส่งต่อแพ็กเก็ตดังกล่าวออกไปอีกครั้ง โดยก่อนที่จะส่งข้อมูลออกไปนั้นจะต้องทำการเพิ่มชื่อโหนดตนเองลงไปในแพ็กเก็ตร้องขอข้อมูลเส้นทาง เพื่อเป็นการบันทึกเส้นทางการสื่อสารที่มีการเชื่อมต่อไปยังปลายทาง ทำให้โหนดตัวถัดไปทราบได้ว่าแพ็กเก็ตนี้ถูกส่งต่อมาจากโหนดใดช่วยให้โหนดปลายทางทราบถึงจำนวนฮอปของเส้นทาง



รูปที่ 2.5 การส่งแพ็กเก็ตร้องขอข้อมูลเส้นทางจากโหนดต้นทาง A ไปยังโหนดปลายทาง D

2. การตอบกลับข้อมูลเส้นทาง (Route Reply)

เมื่อโหนดปลายทางได้รับแพ็กเก็ตร้องขอข้อมูลเส้นทาง โหนดปลายทางจะทำการส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทาง (Route Reply Packet) กลับมายังโหนดต้นทาง ในแพ็กเก็ตนี้จะแสดงรายชื่อโหนดตัวกลางที่สามารถเชื่อมต่อระหว่างต้นทางและปลายทางได้ สำหรับกรณีที่มีเส้นทางที่สามารถเชื่อมต่อได้หลายเส้นทาง โหนดปลายทางจะเลือกใช้เส้นทางที่สั้นที่สุด (Shortest Path) สำหรับให้โหนดต้นทางนำไปใช้งานพิจารณาจากจำนวนฮอป ในกระบวนการตอบกลับข้อมูลเส้นทางนี้จะเป็นการส่งแบบยูนิแคสต์เพื่อลดภาระการทำงานของเครือข่าย



รูปที่ 2.6 การส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทางจากโหนดปลายทาง D กลับมายังโหนดต้นทาง A

2.5 การตรวจสอบสภาพเส้นทางการสื่อสารของโปรโตคอล DSR

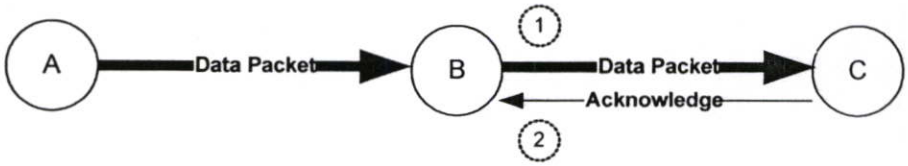
กระบวนการตรวจสอบและรักษาสภาพเส้นทางการสื่อสาร (Route Maintenance) เป็นสิ่งสำคัญอย่างยิ่งสำหรับเครือข่ายไร้สายแบบแอดฮอค เนื่องจากโหนดมีการเคลื่อนที่อยู่ตลอดเวลาจึงมีความเป็นไปได้ว่าการนำส่งข้อมูลแต่ละครั้งอาจไม่ไปถึงยังผู้รับ สาเหตุที่ทำให้การนำส่งข้อมูลมีความผิดพลาดมีอยู่ด้วยกันหลายประการเช่น

- โหนดต้นทางหรือปลายทางเคลื่อนที่ออกจากรัศมีการสื่อสารระหว่างกัน
- ข้อมูลเสียหายเพราะถูกแทกแซงจากสัญญาณวิทยุของโหนดอื่นๆ
- การประมวลผลบนโหนดปลายทางไม่สามารถรองรับและจัดการข้อมูลที่เข้ามาได้ทัน

การตรวจสอบสภาพเส้นทางการสื่อสารสำหรับโปรโตคอล DSR เป็นการตรวจสอบแบบโหนดต่อโหนดในระดับชั้นดาตาลิงค์ (Datalink Layer [8]) โดยมีการทำงานอยู่สองรูปแบบดังนี้

2.5.1 การตรวจสอบสภาพเส้นทางกรณีการสื่อสารเป็นปกติ

ในสภาวะที่การสื่อสารเป็นปกติ เมื่อโหนดใดผู้รับได้รับข้อมูลจากผู้ส่งเรียบร้อยแล้วจะทำการตอบกลับมายังผู้ส่งด้วยข้อมูล Acknowledge เพื่อแจ้งให้โหนดที่ทำการส่งข้อมูลทราบว่าการนำส่งข้อมูลมีความสมบูรณ์ ดังรูป 2.7



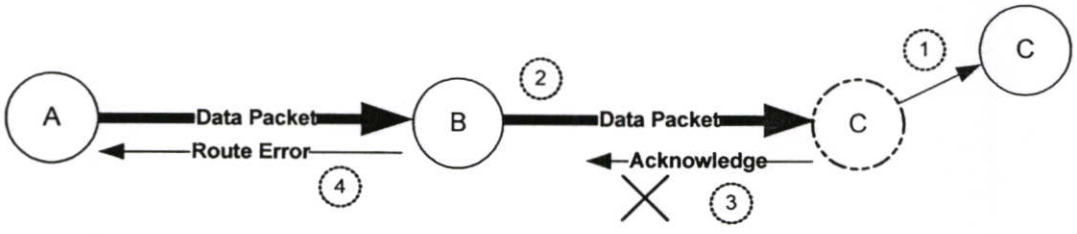
รูปที่ 2.7 การตอบกลับด้วยข้อมูล Acknowledge ในกรณีการนำส่งข้อมูลมีความสมบูรณ์

ขั้นตอนการทำงานมีดังนี้

1. โหนดตัวกลาง B ส่งข้อมูลที่ได้รับจากโหนด A ไปยังโหนด C ซึ่งอาจเป็นโหนดข้างเคียงในเส้นทางหรือโหนดปลายทางก็ได้
2. เมื่อโหนด C ได้รับข้อมูลแล้วจะทำการตรวจสอบความถูกต้อง และตอบกลับด้วยข้อมูลAcknowledge กลับมายังโหนด B
3. เมื่อโหนด B รับทราบว่าข้อมูลที่ส่งไปนั้น โหนด C ได้รับเรียบร้อยแล้วจึงจะทำการส่งข้อมูลที่เหลือต่อไป

2.5.2 การตรวจสอบสภาพเส้นทางกรณีเส้นทางสื่อสารเสียหาย

ในกรณีเส้นทางการสื่อสารเสียหายอันเกิดจากโหนดมีการเคลื่อนที่ห่างจากกัน จะทำให้ไม่มีการตอบกลับด้วยข้อมูล Acknowledge โหนดผู้ส่งจึงทราบว่าการนำส่งข้อมูลไม่สมบูรณ์ ซึ่งต้องแจ้งกลับไปยังโหนดต้นทางด้วยข้อมูล Route Error [13] ดังรูปที่ 2.8



รูปที่ 2.8 ขั้นตอนการตรวจสอบสภาพเส้นทางเมื่อเส้นทางการสื่อสารเสียหาย

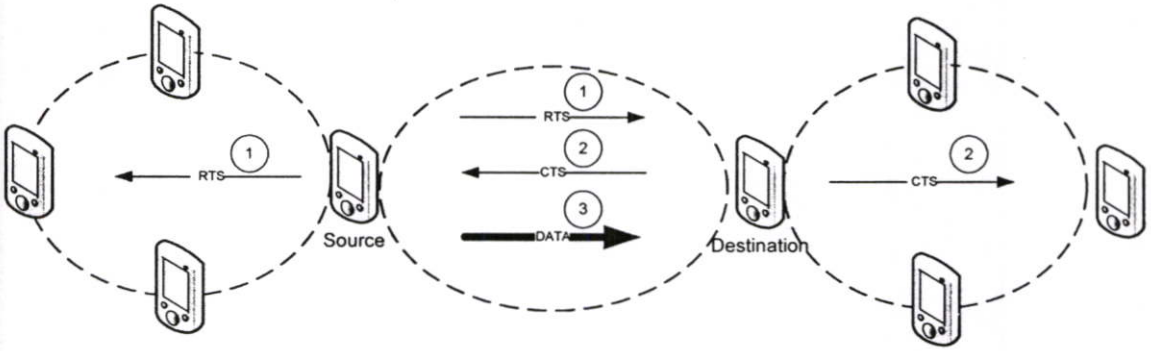
ขั้นตอนการทำงานมีดังนี้

1. โหนด C มีการเคลื่อนที่ออกนอกรัศมีการสื่อสารกับโหนด B
2. เมื่อโหนด B ส่งข้อมูลไปยังโหนด C จะไม่ได้รับข้อมูล Acknowledge จากโหนด C ทำให้โหนด B ทราบว่าการนำส่งข้อมูลไปยังโหนด C ไม่สมบูรณ์
3. โหนด B รายงานโหนดต้นทาง A ด้วยข้อมูล Route Error เพื่อให้โหนดต้นทางทราบว่าข้อมูลไม่สามารถส่งไปยังปลายทางได้เนื่องจากเส้นทางการสื่อสารเสียหาย
4. โหนด A ต้องทำการเริ่มการค้นหาเส้นทางใหม่ เพื่อส่งข้อมูลที่ยังคงเหลือให้ครบ

2.6 โปรโตคอลการเข้าใช้งานช่องสัญญาณสื่อสาร

ช่องสัญญาณการสื่อสาร (Transmission channel) ถือเป็นทรัพยากรที่จำกัดและทุกโหนดต้องใช้งานร่วมกัน การควบคุมให้ทุกโหนดได้เข้าใช้ช่องสัญญาณอย่างเป็นระเบียบและยุติธรรมนับเป็นสิ่งสำคัญ เพราะหากโหนดสามารถส่งข้อมูลออกมาโดยไม่มีการควบคุม จะทำให้เกิดการชนกันของข้อมูล (Collision) จนทำให้ข้อมูลเสียหายและไม่สามารถใช้งานได้ หากเครือข่ายมีการชนกันของข้อมูลบ่อยครั้งอาจส่งผลทำให้ประสิทธิภาพของเครือข่ายลดลง

โปรโตคอลควบคุมการใช้งานช่องสัญญาณของระบบเครือข่ายไร้สาย (Wireless Media Access Protocols) ที่ใช้กันในปัจจุบันเป็นโปรโตคอลที่ได้รับการพัฒนาเพิ่มเติมจากโปรโตคอล CSMA/CD (Carrie Sent Multiple Access with Collision Detection [14]) ซึ่งเป็นโปรโตคอลมาตรฐานในการควบคุมการใช้งานช่องสัญญาณบนเครือข่ายแบบสาย และได้รับการตั้งชื่อเรียกใหม่ว่า CSMA/CA (Carrie Sent Multiple Access with Collision Avoidance [15]) แม้ว่าโปรโตคอล CSMA/CA จะมีพื้นฐานการพัฒนาจาก CSMA/CD แต่กลับมีความแตกต่างกันอย่างชัดเจนในกระบวนการตรวจสอบการชนกันของข้อมูล โดย CSMA/CD จะตรวจสอบการชนกันของข้อมูลในทุกครั้งที่ทำการส่งโดยอาศัยสัญญาณสะท้อนกลับของข้อมูลในสายส่ง หากข้อมูลเสียหายจากการชนกันโปรโตคอล CSMA/CD จะทำการส่งข้อมูลซ้ำอีกครั้งโดยทันที แต่สำหรับการสื่อสารแบบไร้สายนั้นจะไม่มีการสะท้อนกลับของข้อมูลในสายส่ง ทำให้ไม่สามารถตรวจสอบการชนกันของข้อมูลเมื่อทำการส่งได้เลย แนวคิดของโปรโตคอล CSMA/CA จึงเน้นไปที่การหลีกเลี่ยงและลดการชนกันของข้อมูลให้มีโอกาสเกิดขึ้นน้อยที่สุด โดยใช้วิธีการส่งข้อมูลขนาดเล็กไปยังโหนดข้างเคียงทุกตัวก่อนที่จะมีการส่งข้อมูลจริง ข้อมูลที่มีขนาดเล็กดังกล่าวจะทำหน้าที่เป็นตัวร้องขอให้โหนดข้างเคียงระงับการส่งข้อมูลออกมาเมื่อตนเองจะทำการส่งข้อมูล ดังตัวอย่างในรูปที่ 2.9

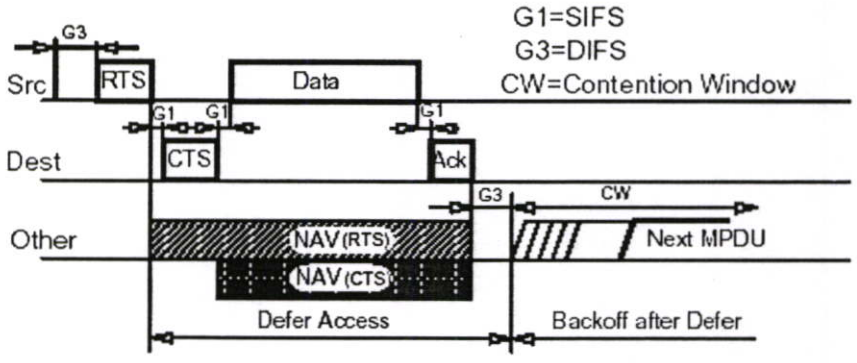


รูปที่ 2.9 การทำงานของโปรโตคอล CSMA/CA

ในรูปที่ 2.9 เป็นการแสดงการทำงานของโปรโตคอล CSMA/CA ซึ่งมีขั้นตอนดังนี้

1. โหนดที่ต้องการส่งข้อมูลร้องขอเครือข่ายเพื่อใช้งานช่องสัญญาณด้วยการส่งแพ็กเก็ต RTS (Request To Send) ไปยังโหนดปลายทาง โดยภายในแพ็กเก็ตจะประกอบด้วยชื่อโหนดต้นทาง, ปลายทาง, และระยะเวลาที่ใช้ในการส่งข้อมูลแต่ละเฟรม
2. โหนดปลายทางเมื่อได้รับข้อมูล RTS แล้ว จะตอบกลับด้วยแพ็กเก็ต CTS (Clear To Send) โดยภายในประกอบด้วยข้อมูลที่ถูกสำเนามาจากแพ็กเก็ต RTS ที่รับมา
3. โหนดทุกตัวในเครือข่ายมีหน้าที่ต้องรับแพ็กเก็ต RTS และ CTS เพื่อประมวลผลตลอดเวลา ทำให้โหนดในบริเวณนั้นทราบว่าจะมีการสื่อสารจากโหนดใดและใช้เวลาเท่าใด โหนดในบริเวณดังกล่าวจึงเข้าสู่สภาวะการรอคอย (Defer Access) ในสภาวะดังกล่าวโหนดจะไม่มีการส่งแพ็กเก็ตใดๆ ออกมา

สถานะการทำงานของโหนดในเครือข่ายไร้สายเมื่อได้รับข้อมูล RTS และ CTS จะมีการกำหนดช่วงเวลาดังรูปที่ 2.10



รูปที่ 2.10 ช่วงเวลาการทำงานของโหนดเมื่อได้รับข้อมูล RTS และ CTS

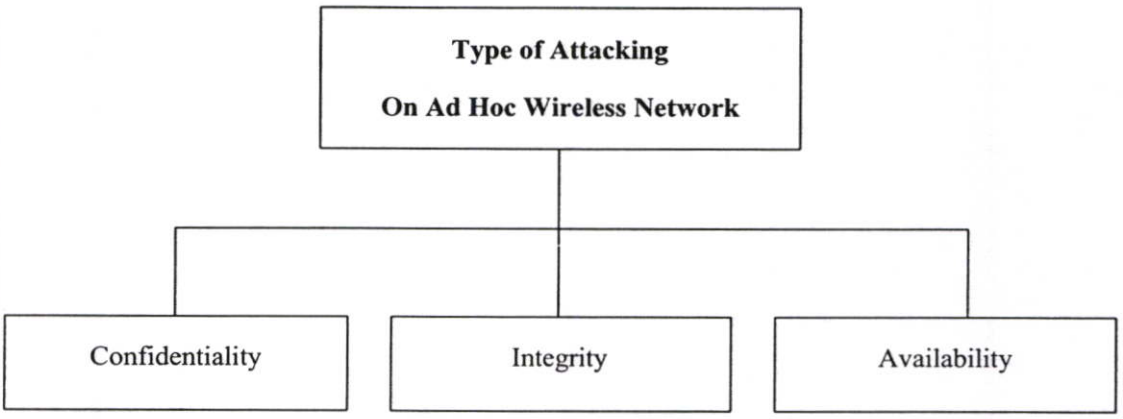
บทที่ 3
ความปลอดภัยบนเครือข่ายไร้สายแบบแอดฮอค

3.1 บทนำ

ในปัจจุบันความปลอดภัยของเครือข่ายถูกรบกวนจากผู้ไม่ประสงค์ดี หรือที่เรียกกันว่าผู้บุกรุกทางเครือข่าย (Network Intruder) ทำลายสภาพแวดล้อมของเครือข่ายให้ทำงานผิดปกติ เช่นการทำลายเส้นทางการสื่อสาร, การเปลี่ยนแปลงข้อมูลที่ถูกนำส่ง หรือแม้กระทั่งการทำให้โหนดสื่อสารไม่สามารถทำงานได้ โดยอาจมีวัตถุประสงค์เพียงเพื่อความสนุก จนกระทั่งต้องการนำข้อมูลที่สำคัญไปใช้งานอย่างผิดกฎหมาย ในบทนี้จะได้กล่าวถึงรูปแบบการโจมตีบนเครือข่ายไร้สายแบบแอดฮอค และแนวทางการตรวจจับความผิดปกติของเครือข่ายจากงานวิจัยที่เกี่ยวข้อง รวมถึงชี้ให้เห็นถึงจุดอ่อนของวิธีการตรวจจับดังกล่าว อันเป็นที่มาของการแก้ปัญหาของวิทยานิพนธ์นี้

3.2 การโจมตีบนเครือข่ายไร้สายแบบแอดฮอค

ผู้บุกรุกทางเครือข่าย และระบบตรวจจับเปรียบเสมือนผู้ร้ายกับตำรวจ ในแต่ละวันผู้ร้ายจะคอยพัฒนารูปแบบการทำความผิดเพื่อให้ยากต่อการทำงานของตำรวจอยู่เสมอ ตำรวจหรือระบบตรวจจับที่ดีต้องคอยศึกษาพฤติกรรมของผู้ร้าย และหาวิธีป้องกันการทำงานของผู้ร้ายเพื่อไม่ให้สร้างความเดือนร้อนแก่สังคม ในหัวข้อนี้จะเป็นการอธิบายการโจมตีเครือข่ายไร้สายแบบแอดฮอคในรูปแบบต่างๆ [16] ได้จัดรูปแบบไว้สามประเภทใหญ่ๆ ดังนี้

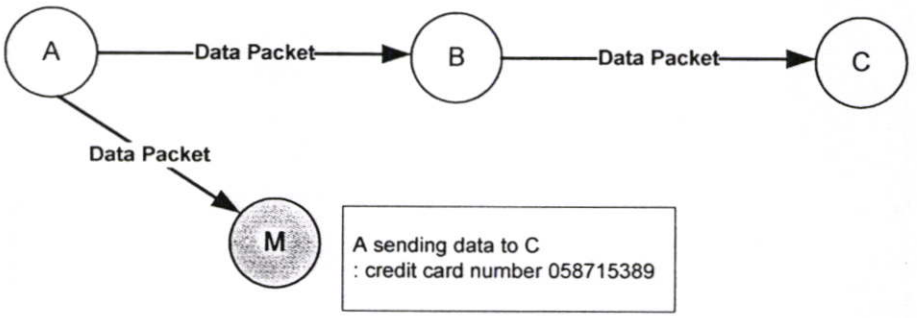


รูปที่ 3.1 แสดงการโจมตีบนเครือข่ายไร้สายแต่ละประเภท

3.3 Confidentiality Attack

การโจมตีประเภทนี้มีจุดประสงค์เพื่อเปิดเผยความลับของข้อมูลในเครือข่าย เช่นข้อมูลธุรกรรมทางการเงินหรือข้อมูลทางธุรกิจ โดยผู้ส่งมีความประสงค์ให้ผู้รับที่แท้จริงเท่านั้นที่สามารถเปิดอ่านและใช้งานข้อมูลดังกล่าว เนื่องจากข้อมูลดังกล่าวหากมีผู้บุกนำไปเปิดเผยหรือนำไปใช้ในทางที่ผิดสามารถส่งผลเสียหายต่อเจ้าของข้อมูลได้

บนระบบเครือข่ายท้องถิ่นขนาดเล็กแบบใช้สายส่งนั้น ปัญหาดังกล่าวสามารถป้องกันในเบื้องต้นได้จากอุปกรณ์เครือข่าย โดยการเลือกใช้สวิตช์แทนฮับในการกระจายสัญญาณเพื่อให้ข้อมูลถูกส่งไปยังผู้รับที่แท้จริงเพียงโหนดเดียวเท่านั้น แต่สำหรับเครือข่ายไร้สายซึ่งเป็นเครือข่ายแบบเปิดและข้อมูลถูกส่งออกอากาศไปในทุกทิศทาง ผู้ส่งไม่สามารถกำหนดให้ข้อมูลเดินทางไปยังผู้รับเพียงโหนดเดียวได้ จึงเป็นการง่ายที่ผู้บุรุกจะทำการดักฟังข้อมูลโดยเพียงแต่เข้ามาในพื้นที่การสื่อสารของเครือข่ายและกำหนดให้อุปกรณ์ไร้สายทำงานแบบโพรมิสคิวอัส (Promiscuous) เท่านั้น ผู้บุกรุกก็จะสามารถได้ข้อมูลทั้งหมดที่มีการรับส่งในบริเวณนั้นทันที



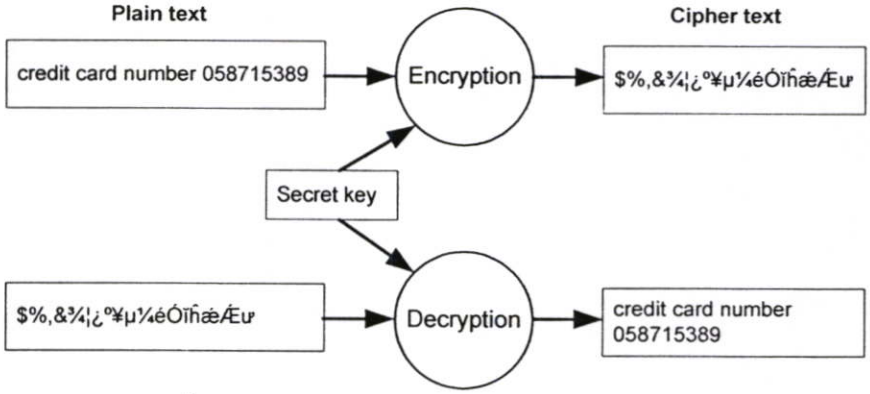
รูปที่ 3.2 แสดงการดักฟังข้อมูลในเครือข่ายของผู้บุกรุก

เนื่องจากการควบคุมไม่ให้โหนดผู้บุกรุกเข้ามาในพื้นที่การทำงานของเครือข่ายนั้น ในทางปฏิบัติทำได้ยากและอาจสร้างความยุ่งยากในการใช้งาน ในปัจจุบันการป้องกันการโจมตีประเภทนี้จึงนิยมใช้วิธีการเข้ารหัสลับข้อมูล (Data Encryption) เพื่อทำให้ข้อมูลสามารถแปลความหมายได้โดยง่าย ซึ่งการเข้ารหัสลับข้อมูลจำเป็นจะต้องมีองค์ประกอบที่สำคัญสองส่วนคือ

- อัลกอริธึมในการเข้ารหัส (Encryption Algorithm)
- กุญแจสำหรับเข้าและถอดรหัส (Secret key)

วิธีการทำให้ข้อมูลเป็นความลับ จะเริ่มจากโหนดผู้ส่งจะทำการเข้ารหัสข้อมูลที่ต้องการส่ง (Plain text) โดยใช้อัลกอริธึมการเข้ารหัสร่วมกับกุญแจ เพื่อให้ได้ข้อมูลที่ถูกเข้ารหัส (Cipher text) ผลลัพธ์ของการเข้ารหัสจะได้ข้อมูลที่ไม่สามารถอ่านและนำไปใช้ได้ เมื่อข้อมูลที่ถูกเข้ารหัสถูกส่ง

ถึงผู้รับเรียบร้อยแล้ว ฝั่งผู้รับจะต้องใช้อัลกอริธึมเดียวกันและกุญแจตัวเดิมทำการถอดรหัส ผลที่ได้จะเป็นข้อมูลเดิมก่อนเข้ารหัสซึ่งสามารถนำไปใช้งานได้



รูปที่ 3.3 การรักษาความลับของข้อมูลโดยการเข้ารหัสลับ

อัลกอริธึมการเข้ารหัสที่ได้รับความนิยมในปัจจุบันได้แก่นี้ เช่น DES [17], 3DES [17] และ AES [17] โดยทุกอัลกอริธึมแทบจะมีระดับความปลอดภัยเท่าเทียมกัน แต่สิ่งที่ควรให้ความสำคัญมากที่สุดในการเข้ารหัสคือความยาวของกุญแจ (Key length) ซึ่งควรมีความยาวอย่างน้อย 128 ไบต์ขึ้นไป [18] ทั่วไปแล้วยิ่งความยาวของกุญแจมากเท่าใดความปลอดภัยก็จะยิ่งสูงขึ้นเท่านั้น เพราะต้องใช้เวลานานยิ่งขึ้นในการถอดรหัสจากผู้บุกรุก

3.4 Integrity Attack

นอกเหนือจากการลักลอบดักฟังข้อมูลจากผู้บุกรุกแล้ว การปลอมแปลงหรือแก้ไขเนื้อหาของข้อมูล (Content modification) ในระหว่างที่ข้อมูลเดินทางในเครือข่าย เพื่อให้ผู้รับได้ข้อมูลที่บิดเบือนไปจากต้นฉบับ ผลเสียที่เกิดขึ้นอาจมีได้หลายรูปแบบขึ้นอยู่กับประเภทของข้อมูลที่ถูกปลอมแปลง เช่นหากเป็นการปลอมแปลงข้อมูลที่เกี่ยวข้องกับเส้นทางการสื่อสาร อาจส่งผลให้เครือข่ายไม่สามารถใช้งานได้ หรือหากเป็นการปลอมแปลงข้อมูลธุรกรรมทางการเงิน อาจสร้างความเสียหายแก่ผู้ที่เกี่ยวข้องกับธุรกรรมดังกล่าว รูปแบบการโจมตีประเภทนี้บนเครือข่ายไร้สายแบบแอดฮอคได้ถูกแบ่งย่อยเป็นสองประเภทตามลักษณะข้อมูลที่ถูกโจมตี ดังนี้

รูปที่ 3.4 โหนดผู้บุกรุกทำการแก้ไขข้อมูลเส้นทางให้เป็นเส้นทางที่ไม่สามารถใช้งานได้

ในปัจจุบันได้มีการวิจัยที่มุ่งพัฒนาโปรโตคอลการค้นหาเส้นทาง ที่มีสามารถในการตรวจจับการแก้ไขหรือปลอมแปลงข้อมูลเส้นทางการในระหว่างการนำส่ง เช่น Ariadne [19] และ SEAD [20] โดยอาศัยเครื่องมือหลักคือระบบลายมือชื่ออิเล็กทรอนิกส์ (Digital signature [17]) และการเข้ารหัสแบบคีย์คู่ (Asymmetric key encryption [17]) มาทำหน้าตรวจสอบการเปลี่ยนแปลงข้อมูลและยืนยันการส่งจากโหนดต้นทาง ตัวอย่างเช่นโปรโตคอลค้นหาเส้นทาง Ariadne ที่เป็นการนำโปรโตคอล DSR มาประยุกต์ โดยการเพิ่มระบบการยืนยันผู้ส่งจากลายมือชื่ออิเล็กทรอนิกส์เพื่อให้ปลายทางตรวจสอบความถูกต้องของข้อมูลได้

3.4.2 การปลอมแปลงหรือแก้ไขข้อมูลในระหว่างการนำส่งข้อมูล

การโจมตีประเภทนี้ผู้บุกรุกมุ่งที่จะปลอมแปลงหรือแก้ไขเนื้อหาข้อมูลจากผู้ใช้งาน ซึ่งเป็นข้อมูลในระดับชั้นแอพพลิชัน (Application layer) เนื่องจากข้อมูลในระดับชั้นนี้มักจะเป็นข้อมูลที่มีความสำคัญสูงเนื่องจากมีความใกล้ชิดกับผู้ใช้มากที่สุด การโจมตีประเภทนี้ผู้บุกรุกจะต้องมีความเข้าใจรูปแบบและมาตรฐานของข้อมูลที่กำลังนำส่งอยู่ เพื่อให้ข้อมูลที่ถูกแก้ไขปลอมแปลงแล้วไม่สามารถถูกตรวจจับได้จากแอพพลิชัน

การป้องกันและตรวจจับการโจมตีประเภทนี้จะทำได้โดยใช้ระบบลายมือชื่ออิเล็กทรอนิกส์และการเข้ารหัสแบบคีย์คู่ในการยืนยันและรักษาความลับของข้อมูล ซึ่งในปัจจุบันได้มีการพัฒนาระบบการป้องกันที่ทำให้ผู้ใช้สามารถใช้งานได้โดยง่าย เช่น

- ระบบเครือข่ายเสมือนจริง (Virtual Private Network) เป็นการรักษาความปลอดภัยของข้อมูลในระดับชั้นเน็ตเวิร์ก ซึ่งเป็นชั้นที่ทำหน้าที่ควบคุมการสื่อสารในระดับโหนดต้นทางและปลายทาง ข้อดีของการใช้ระบบเครือข่ายเสมือนคือข้อมูลที่มีการนำส่งทุกอย่างบนโหนดจะได้รับความปลอดภัยทั้งหมด แต่มีข้อเสียคือมีการใช้ทรัพยากรในการประมวลผลข้อมูลมาก
- การรักษาความปลอดภัยในระดับแอพพลิชัน เป็นการรักษาความปลอดภัยที่รับผิดชอบโดยแอพพลิเคชันทั้งทางฝั่งผู้รับและผู้ส่ง ตัวอย่างเช่นเวปเซิร์ฟเวอร์ที่ทำงานบนโปรโตคอล HTTPS [21] หรือเทลเน็ต (Telnet) ที่ทำงานบน SSH [21] เป็นต้น

3.5 Availability Attack

เป็นรูปแบบการโจมตีที่เน้นสร้างความเสียหายแก่โหนดหรือเครือข่าย เพื่อทำให้โหนดและเครือข่ายไม่สามารถใช้งานได้หรือไม่เต็มประสิทธิภาพ เช่นการโจมตีแบบ Distribute Denial of Service [18] ที่เคยทำให้เวบไซต์ชื่อดังอย่าง yahoo.com, buy.com และ eBay ไม่สามารถให้บริการได้ในอดีต ซึ่งนับเป็นความเสียหายที่ปรากฏชัดเจนจากการโจมตีประเภทนี้ ปัจจุบันการโจมตี

ลักษณะนี้ได้ถูกพัฒนาให้มีความซับซ้อนและยากต่อการป้องกัน ทั้งการใช้ไวรัสคอมพิวเตอร์หรือหนอนอิเล็กทรอนิกส์ (Worm) ที่ส่งไปกับอีเมลเพื่อสั่งงานให้คอมพิวเตอร์หลายๆ ตัวร่วมกันทำลายเครือข่ายเป้าหมายที่ผู้บุกรุกต้องการ

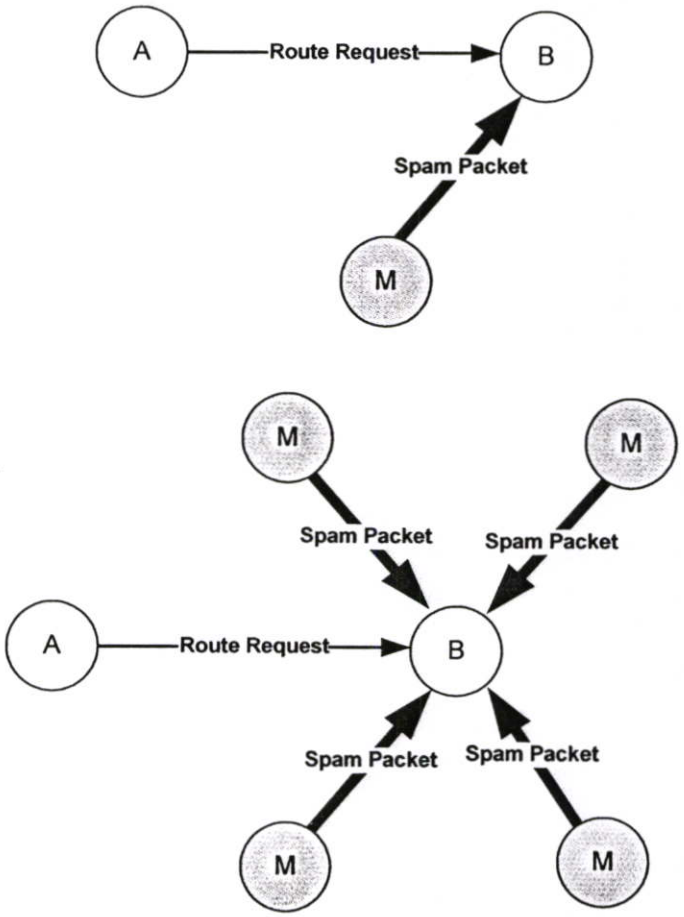
การโจมตีลักษณะนี้บนเครือข่ายไร้สายแบบแอดฮอค ผู้บุกรุกมักมีเป้าหมายอยู่ที่การลดความน่าเชื่อถือประสิทธิภาพของเครือข่าย เนื่องจากโครงสร้างการเชื่อมต่อของเครือข่ายมีความอ่อนไหวอย่างมากต่อการเปลี่ยนแปลง ทำให้การโจมตีมีความง่ายและมีรูปแบบที่หลากหลายมากกว่าเครือข่ายแบบใช้สาย ซึ่ง [16] ได้ทำการแบ่งประเภทการโจมตีลักษณะนี้บนเครือข่ายไร้สายแบบแอดฮอคไว้สองประเภทคือ

3.5.1 Route Discovery Attack

หน้าที่หลักของโปรโตคอลค้นหาเส้นทางการสื่อสาร คือค้นหาเส้นทางที่มีประสิทธิภาพในการนำส่งข้อมูลสูงสุด การโจมตีลักษณะนี้มีเป้าหมายทำให้โปรโตคอลค้นหาเส้นทางไม่สามารถค้นหาเส้นทางได้ หรืออาจทำให้โปรโตคอลค้นหาเส้นทางได้เส้นทางที่ผิดและไม่สามารถใช้งานได้ มีตัวอย่างการโจมตีคือ

3.5.1.1 Denial of Service

DoS [18] เป็นการโจมตีเพื่อหยุดให้บริการแบบง่ายและมีความซับซ้อนน้อยที่สุดผู้บุกรุกเพียงทำการส่งข้อมูลจำนวนมาก (Spam) ไปยังโหนดเป้าหมาย (Victim) เพื่อให้โหนดเป้าหมายไม่สามารถประมวลผลข้อมูลจำนวนมากดังกล่าวได้ทันและเกิดความผิดปกติที่เรียกกว่า Buffer Overflow ส่งผลให้โหนดดังกล่าวไม่สามารถให้บริการการได้ ตัวอย่างในรูปที่ 3.5 แสดงให้เห็นว่าโหนดผู้บุกรุก M ทำการส่งข้อมูลไปยังโหนด B จำนวนมาก จนทำให้โหนด B ไม่สามารถให้บริการค้นหาเส้นทางการสื่อสารที่โหนด A ร้องขอมาได้ ในกรณีที่ผู้บุกรุกมีจำนวนมากและมีการทำงานร่วมกัน อาจร่วมกันโจมตีแบบ Distribute Denial Of Service ซึ่งจะยิ่งสร้างความเสียหายให้แก่โหนดเป้าหมายมากยิ่งขึ้น



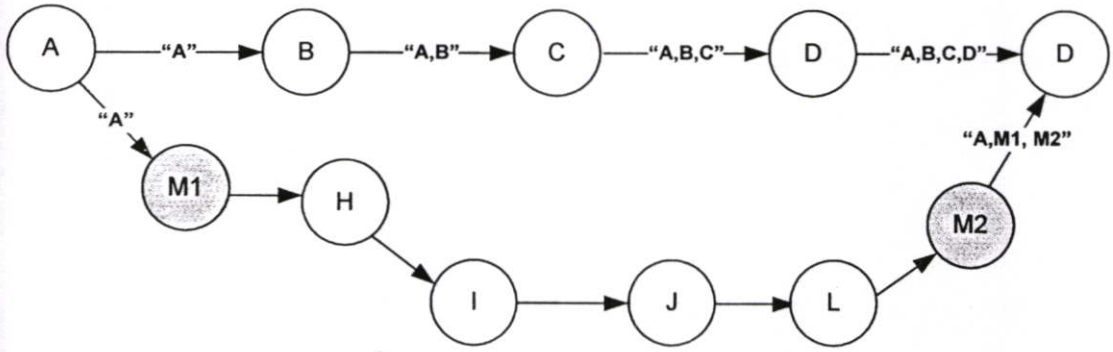
รูปที่ 3.5 แสดงการโจมตีแบบ Denial of Service และ Distribute Denial of Service

3.5.1.2 Tunneling

การโจมตีแบบนี้มีอีกชื่อหนึ่งว่า Wormhole Attack [18] มีรูปแบบทำงานที่ซับซ้อนและยากต่อการตรวจจับ มีเป้าหมายเพื่อปลอมแปลงเส้นทางการสื่อสารเพื่อให้ผู้บุกรุกได้ทำหน้าที่นำส่งข้อมูล เพื่อผลในการแก้ไขหรือเฝ้าฟังข้อมูลต่อไป

การโจมตีแบบนี้จะเป็นการทำงานร่วมกันระหว่างผู้บุกรุกอย่างน้อย 2 โหนด ดังตัวอย่างรูปที่ 3.6 ผู้บุกรุกตัวแรก (M1) จะสื่อสารกับผู้บุกรุกตัวที่สอง (M2) อยู่ตลอดเวลาเพื่อแลกเปลี่ยนข้อมูลเส้นทางการสื่อสารระหว่างกัน เมื่อโหนด A ต้องการส่งข้อมูลจะทำการค้นหาเส้นทางโดยการส่งแพ็กเก็ตร้องขอข้อมูลเส้นทางไปยังโหนดข้างเคียงทุกตัว ซึ่งเส้นทางที่สั้นที่สุดในความเป็นจริงคือเส้นทางที่ประกอบด้วยโหนด B,C และ D ที่มีจำนวนเพียง 3 ฮอปเท่านั้น แต่เมื่อมีการโจมตีเกิดขึ้น โหนด M1 จะสื่อสารกับโหนด M2 ให้รายงานโหนดปลายทาง D ว่ามีเส้นทางที่ประกอบด้วยโหนด M1 และ M2 เชื่อมต่ออยู่กับโหนด A ทำให้โหนด D ทำการเลือกเส้นทางดังกล่าวเนื่องจากมีจำนวน

เพียง 2 ฮอปเท่านั้น ส่งผลให้การสื่อสารที่เกิดขึ้นระหว่างโหนด A และ D ต้องใช้เส้นทางที่ผู้บุกรุกทำการปลอมแปลง



รูปที่ 3.6 แสดงการโจมตีแบบ Tunneling

ในปัจจุบันได้มีงานวิจัยเพื่อตรวจจับการโจมตีแบบ Tunneling ยังอยู่ในวงจำกัด โดยมีการเสนอวิธีการตรวจจับในหลายรูปแบบ เช่น Yih-Chun Hu ได้เสนอวิธีการค้นหาเส้นทางโดยพิจารณาจากจำนวนฮอปร่วมกับเวลาเพื่อหลีกเลี่ยงการโจมตี หรือ Lingxuan Hu [23] ที่เสนอการตรวจจับการโจมตีโดยพิจาณาตำแหน่งของโหนดในเครือข่ายจากการใช้เสาอากาศแบบมีทิศทาง

3.5.2 Transmission Attack

การโจมตีรูปแบบนี้ผู้บุกรุกจะทำในช่วงเวลาที่กำลังมีการนำส่งข้อมูล โดยการทำให้โหนดตัวกลางที่ทำหน้าที่นำส่งข้อมูลไม่สามารถให้บริการได้ หรือผู้บุกรุกอาจปลอมแปลงตัวเองเป็นโหนดตัวกลางในเส้นทางแล้วจึงทำการลดทิ้งข้อมูลเพื่อให้การนำส่งข้อมูลล้มเหลว ซึ่งการโจมตีในระหว่างการนำส่งข้อมูลมักจะมีผลกระทบต่อเครือข่ายสูงกว่าการโจมตีที่เกิดขึ้นในระหว่างที่ทำการค้นหาเส้นทาง เนื่องจากต้องมีการค้นหาเส้นทางใหม่ทุกครั้งที่ข้อมูลนำส่งผิดพลาด ตัวอย่างของการโจมตีประเภทนี้มีดังนี้

3.5.2.1 Intermediate node Denial of Service

เป็นการโจมตีที่ผู้บุกรุกต้องการทำให้โหนดตัวกลางที่นำส่งข้อมูลไม่สามารถให้บริการได้ มีลักษณะการโจมตีเหมือน 3.5.1.1 คือการส่งข้อมูลจำนวนมากเพื่อทำให้เกิดนความผิดปกติบนโหนดตัวกลาง

3.5.2.2 Packet Dropping

เป็นรูปแบบการโจมตีที่วิทยานิพนธ์นี้มุ่งทำการศึกษาเพื่อพัฒนาระบบตรวจจับ ในการโจมตีลักษณะนี้ผู้บุกรุกจะทำหน้าที่เป็นโหนดตัวกลางในเส้นทาง โดยพฤติกรรมการโจมตีคือโหนดผู้บุกรุกจะมีการรับข้อมูลจากโหนดก่อนหน้าในเส้นทางตามปกติ แต่ผู้บุกรุกจะไม่ทำการส่ง

ต่อข้อมูลไปยังโหนดตัวถัดไป และทำการหลีกเลี่ยงการตรวจสอบสถานะการสื่อสารจากโปรโตคอลสื่อสารที่มีการตรวจสอบสถานะการสื่อสาร โดยทำการสร้างข้อมูล Acknowledge ปลอมเพื่อให้โหนดก่อนหน้ารับทราบว่ามีการนำส่งข้อมูลสมบูรณ์ ซึ่งจะทำให้โปรโตคอลการสื่อสารไม่สามารถตรวจพบความผิดปกติได้ ดังแสดงในรูปที่ 3.7

รูปที่ 3.7 การโจมตีแบบลดทิ้งข้อมูลทำโดยโหนดตัวกลางของเส้นทาง

แม้ว่ารูปแบบการโจมตีจะทำได้โดยง่ายและไม่ซับซ้อน แต่การโจมตีแบบลดทิ้งข้อมูลกลับสามารถสร้างความเสียหายให้แก่เครือข่ายอย่างหนักได้ เพราะนอกจากจะเป็นการโจมตีที่ไม่สามารถตรวจจับได้จากโปรโตคอลการสื่อสารแล้ว แนวทางการพัฒนาระบบตรวจจับความผิดปกติสำหรับค้นหาโหนดที่เป็นผู้บุกรุกยังทำได้ยากอีกด้วย เนื่องการพฤติกรรมการโจมตีมีลักษณะเดียวกันกับการนำส่งข้อมูลที่ไม่สมบูรณ์จากการเคลื่อนที่ของโหนดในเส้นทาง ซึ่งถือเป็นเหตุการณ์ปกติที่เกิดขึ้นได้บนเครือข่ายไร้สายแบบแอดฮอค ระบบตรวจจับจึงไม่สามารถแยกแยะได้ว่าความเสียหายที่เกิดขึ้นนั้นมีสาเหตุมาจากการโจมตีหรือจากการเคลื่อนที่ออกนอกรัศมีการสื่อสารของโหนด และความยากในการตรวจจับการโจมตีลักษณะนี้อีกประการหนึ่ง คือกระบวนการรวบรวมข้อมูลเพื่อนำมาวิเคราะห์เพื่อตัดสินสภาพการเป็นผู้บุกรุกของโหนด เนื่องจากทุกโหนดบนเครือข่ายมีการเคลื่อนที่อยู่ตลอดเวลา การเฝ้าฟังจากจุดใดจุดหนึ่งของเครือข่ายจึงทำให้ได้ข้อมูลพฤติกรรมของโหนดไม่ครบถ้วน

3.6 ระบบตรวจจับความผิดปกติบนเครือข่ายไร้สายแบบแอดฮอค

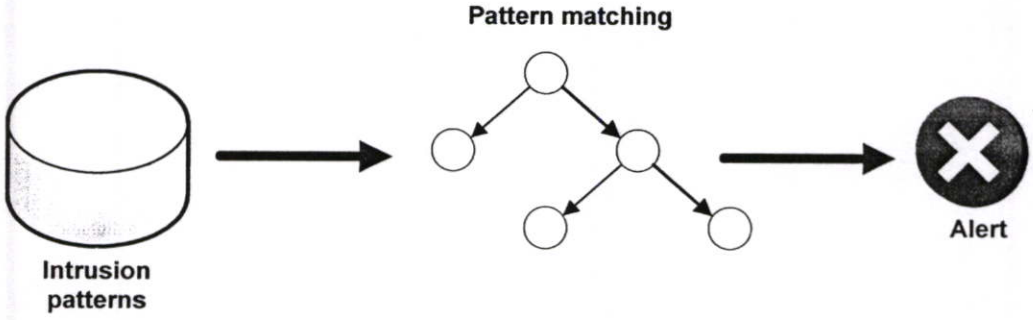
ในอดีตการพัฒนาระบบตรวจจับผู้บุกรุกบนระบบเครือข่าย (Network Intrusion Detection System: NIDS [24]) นับเป็นงานวิจัยที่ยังอยู่ในวงแคบ เนื่องจากความปลอดภัยของเครือข่ายถือประเด็นที่มีความสำคัญน้อย เมื่อเปรียบเทียบกับการพัฒนาด้านความเร็วและประสิทธิภาพของการสื่อสาร แต่ในระยะหลังนี้ปัญหาด้านความปลอดภัยบนเครือข่ายกลับกลายประเด็นที่มีการกล่าวถึงอย่างมาก เพราะความเสียหายที่เกิดขึ้นเมื่อเครือข่ายถูกโจมตีแสดงให้เห็นอย่างชัดเจนในด้านมูลค่าทางธุรกิจ โดยเฉพาะอย่างยิ่งความเสียหายที่เกิดแก่เครือข่ายซึ่งรองรับการทำธุรกรรมทางการเงิน

และพาณิชย์อิเล็กทรอนิกส์ ส่งผลปัจจุบันมีงานวิจัยและผลิตภัณฑ์ที่เกี่ยวข้องกับระบบความปลอดภัยของเครือข่ายคอมพิวเตอร์ถูกพัฒนาออกมาเป็นจำนวนมาก

งานวิจัยด้านความปลอดภัยระบบเครือข่ายไร้สายแบบแอดฮอค นับเป็นหัวข้อใหม่ที่มีการวิจัยกันอย่างแพร่หลายในช่วงไม่กี่ปีที่ผ่านมา เนื่องจากมีการใช้งานอุปกรณ์เครือข่ายกันแพร่หลายมากขึ้น ระบบตรวจจับความผิดปกติของเครือข่ายถือเป็นงานวิจัยที่มีผู้ให้ความสนใจกันมาก เนื่องจากมีประเด็นในการศึกษาอย่างหลากหลาย เช่นการเฝ้าฟังและรวบรวมข้อมูล, การวิเคราะห์พฤติกรรมของโหนด และการค้นหาเส้นทางเพื่อหลีกเลี่ยงโหนดผู้บุกรุก แต่โดยทั่วไปแล้วระบบตรวจจับมีเป้าหมายหลักคือการค้นหาโหนดที่มีพฤติกรรมผิดปกติ โดยมีการแบ่งประเภทของระบบตรวจจับไว้สองประเภทตามลักษณะการโจมตีคือ

3.6.1 Misuse Detection

เป็นระบบตรวจจับที่ใช้เปรียบเทียบพฤติกรรมการทำงานว่าผิดปกติไปจากกฎเกณฑ์ที่กำหนดไว้หรือไม่ โดยมีพื้นฐานมาจากระบบตรวจจับผู้บุกรุกของเครือข่ายแบบสาย เนื่องจากรูปแบบการโจมตีในอดีตนั้นจะเป็นการสร้างข้อมูลที่ผิดไปจากกฎเกณฑ์หรือมาตรฐานที่กำหนดเพื่อให้โหนดเป้าหมายไม่สามารถประมวลผลข้อมูลดังกล่าวได้ ซึ่งจะทำให้เกิดความเสียหายแบบ Buffer Overflow ตัวอย่างเช่นการทำ Ping Loop back [24] หรือ Packet Fragmentation [24] การทำงานของระบบตรวจจับจะเป็นการเปรียบเทียบข้อมูลที่เข้ามากับกฎของโปรโตคอลสื่อสารต่างๆที่เครือข่ายให้บริการอยู่ หากข้อมูลดังกล่าวมีรูปแบบหรือลำดับผิดไปจากที่โปรโตคอลกำหนดไว้จะถือว่าข้อมูลนั้นมีถูกสร้างจากผู้บุกรุก เนื่องจากหากอยู่ในสภาวะแวดล้อมปกติแล้ว แทบจะไม่มีโอกาสเป็นไปได้เลยที่โหนดทั่วไปจะทำการสร้างข้อมูลที่ผิดปกติได้ลักษณะดังกล่าวได้

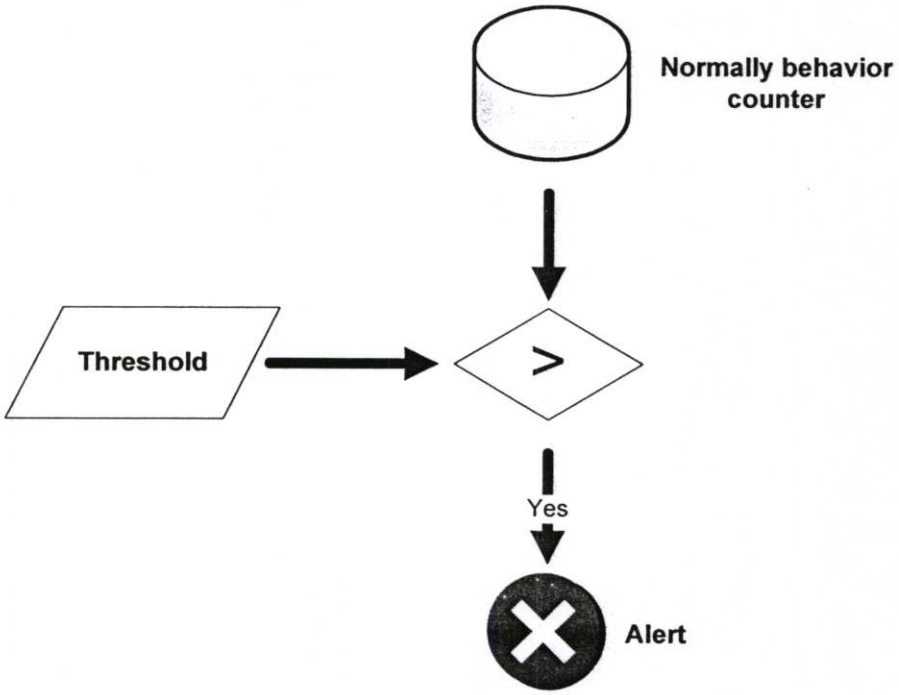


รูปที่ 3.8 การตรวจจับความผิดปกติของเครือข่ายแบบ Misuse Detection

3.6.2 Abnormally Detection

เป็นการตรวจจับสำหรับการโจมตีที่พฤติกรรมความความผิดปกติมีความคลุมเครือและไม่สามารถบ่งชี้ได้ชัดเจนว่าเกิดจากการโจมตี เนื่องจากผู้บุกรุกมีการทำงานถูกต้องตามกฎเกณฑ์ข้อบังคับตามที่โปรโตคอลต่างการสื่อสารกำหนดไว้ทุกประการ เพียงแต่มีปริมาณการใช้ทรัพยากรที่สูงกว่าโหนดอื่นๆ ในเครือข่ายเท่านั้น ตัวอย่างที่เห็นชัดเจนคือการส่งอีเมล์ หากเป็นการส่งตามปกติผู้ใช้อาจมีปริมาณการส่งไม่เกิน 30 อีเมล์ต่อวัน แต่หากผู้บุกรุกทำการส่งอีเมล์จำนวนมากหรือสแปมเมล์ (Spam mail) จำนวนการส่งสูงถึง 100,000 อีเมล์ต่อวัน ซึ่งหากพิจารณาถึงการส่งอีเมล์แต่ละฉบับนั้นจะไม่สามารถบ่งชี้ได้ว่าเป็นการส่งจากผู้บุกรุกหรือจากการใช้งานปกติ เนื่องจากผู้บุกรุกได้ทำการส่งอีเมล์ตามมาตรฐานของโปรโตคอลทุกประการ เพียงแต่มีจำนวนการส่งที่สูงกว่าค่าเฉลี่ยเท่านั้น

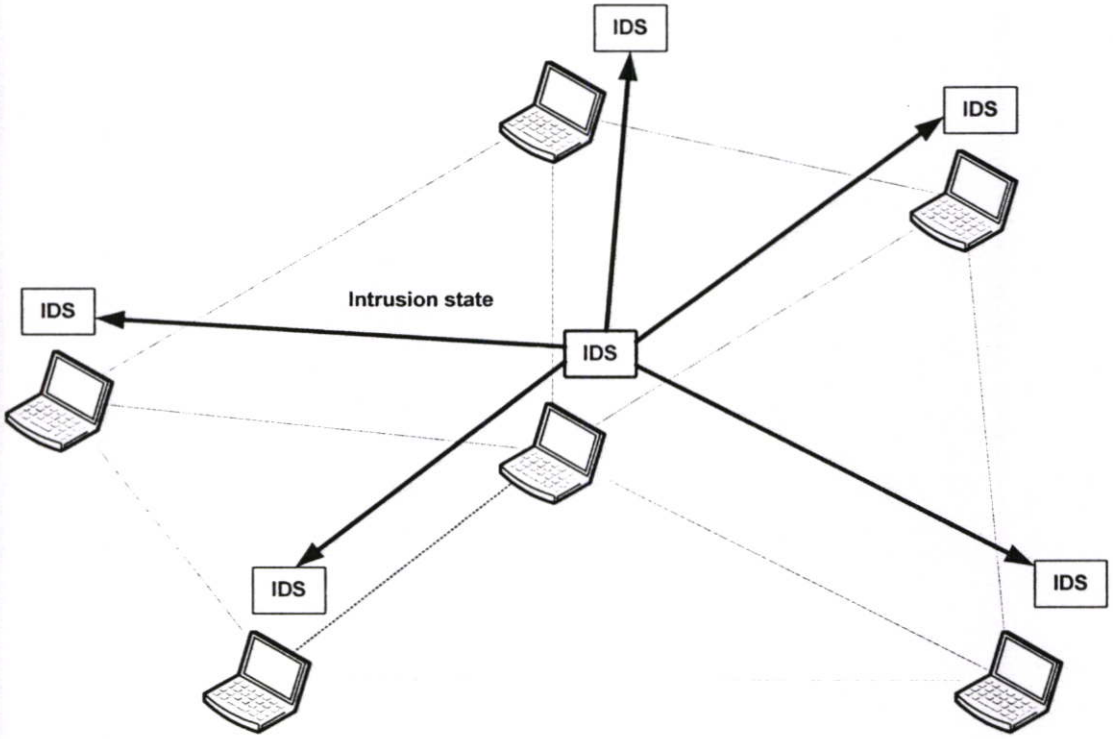
วิธีการตรวจจับการความผิดปกติประเภทนี้จะใช้การเปรียบเทียบจำนวนครั้งของการเกิดพฤติกรรมนั้นกับค่าเทรชโฮลด์ (Threshold) ที่มักเป็นค่าเฉลี่ยการการใช้งานของโหนดปกติ ความถูกต้องของระบบตรวจจับจึงขึ้นอยู่กับการกำหนดค่าเทรชโฮลด์ ที่ต้องมีความสามารถในการแบ่งแยกพฤติกรรมผิดปกติที่เกิดจากผู้บุกรุกหรือโหนดปกติได้



รูปที่ 3.9 การตรวจจับความผิดปกติของเครือข่ายแบบ Abnormally Detection

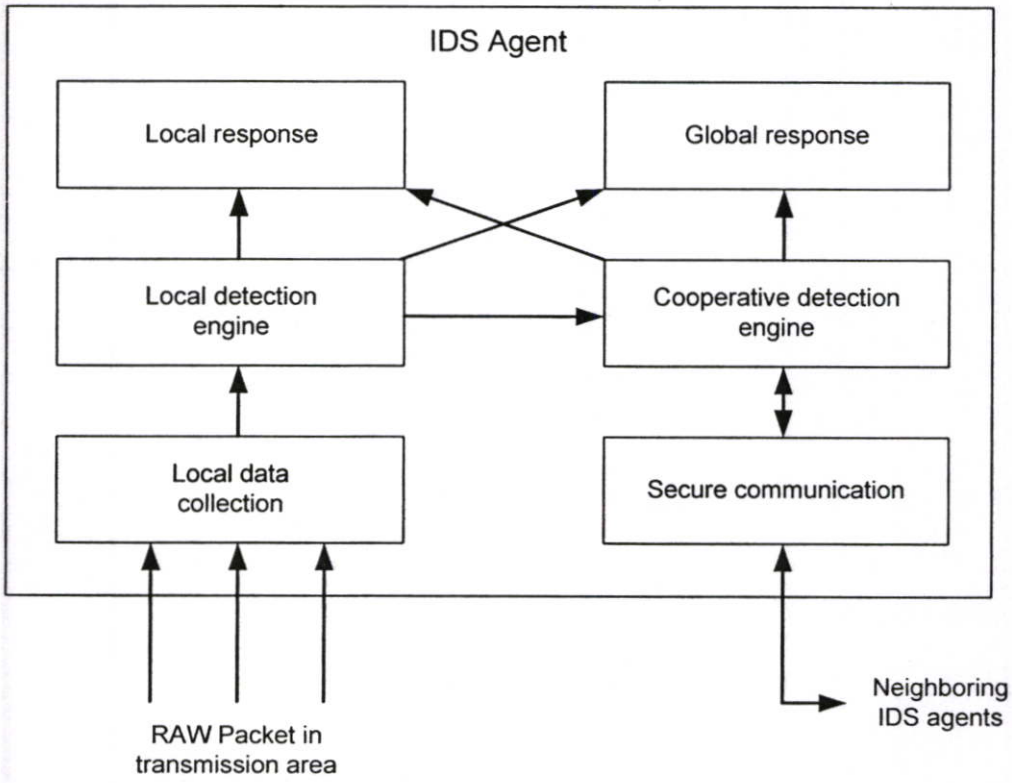
3.7 การออกแบบระบบตรวจจับความผิดปกติบนเครือข่ายไร้สายแบบแอดฮอค

ในปี ค.ศ. 2000 Yongguang Zhang และ Wenke Lee [25] ได้นำเสนอสถาปัตยกรรมของระบบตรวจจับความผิดปกติบนเครือข่ายไร้สายแบบแอดฮอค จากแนวคิดพื้นฐานคือการติดตั้งตัวตรวจจับความผิดปกติหรือผู้บุกรุก (Intrusion Detection System: IDS) ไว้บนโหนดสื่อสารที่ทำงานอยู่ในเครือข่าย ดังรูปที่ 3.10 โดยตัวตรวจจับทุกตัวจะมีการทำงานร่วมกันเพื่อแลกเปลี่ยนข้อมูลและรายงานการโจมตีต่างๆ



รูปที่ 3.10 สถาปัตยกรรมระบบตรวจจับความผิดปกติบนเครือข่ายไร้สายแบบแอดฮอค

ใน [25] ได้มีการเรียกโหนดสื่อสารที่ได้รับการติดตั้งระบบตรวจจับว่าเอเจนต์ (Agent) และได้กำหนดหน้าที่ให้เอเจนต์ทุกตัวจะยังคงทำหน้าที่เป็นโหนดทั่วไปที่มีหน้าที่พื้นฐาน 3 ประการคือ เป็นโหนดต้นทาง, โหนดตัวกลางและโหนดปลายทาง โดยโหนดที่ได้รับการติดตั้งระบบตรวจจับจะยังคงมีพฤติกรรมการเคลื่อนที่หรือการใช้งานเครือข่ายเหมือนเดิมทุกประการ และระบบตรวจจับความผิดปกติที่ถูกติดตั้งจะต้องทำงานโดยไม่กระทบต่อประสิทธิภาพของโหนดเครือข่าย นอกจากนี้ยังได้ออกแบบส่วนประกอบภายในของเอเจนต์ไว้อย่างละเอียดดังรูป 3.11



รูปที่ 3.11 โครงสร้างภายในเอเจนต์ตรวจจับความผิดปกติ

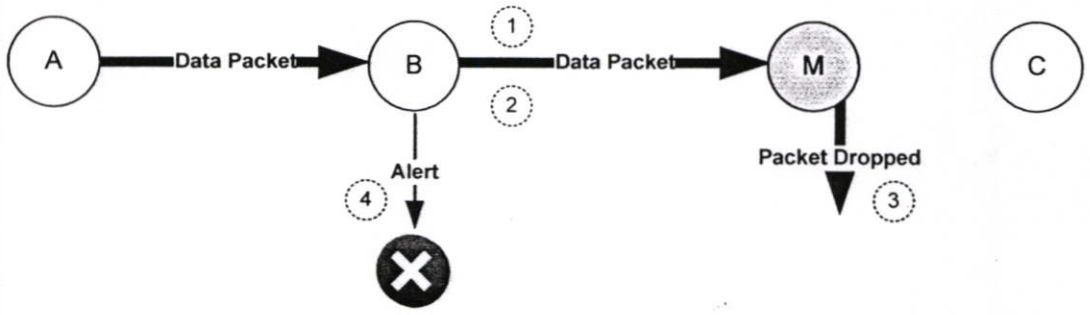
- **Local data collection** เป็นองค์ประกอบแรกที่อยู่ในเอเจนต์ ทำหน้าที่เฝ้าฟังและรวบรวบข้อมูลที่ถูกส่งออกมาจากโหนดข้างเคียงผ่านการทำงานแบบโพรมิสคิวอัสของอินเตอร์เฟส
- **Local detection engine** ทำหน้าที่วิเคราะห์ข้อมูลที่ได้จากการเฝ้าฟังว่ามีความผิดปกติหรือไม่ โดยเงื่อนไขที่ใช้ในการเฝ้าฟังจะสัมพันธ์กับการโจมตีรูปแบบต่างๆ
- **Local response** ทำหน้าที่รายงานผลที่ได้จากการวิเคราะห์ไปยังเอเจนต์ในเครือข่าย
- **Secure communication** มีหน้าที่รับผิดชอบการสื่อสารระหว่างเอเจนต์ในเครือข่ายให้มีความปลอดภัยปราศจากการถูกปลอมแปลงและแก้ไข
- **Cooperative detection engine** ทำหน้าที่วิเคราะห์ผลในขั้นสุดท้ายเพื่อตัดสินว่าโหนดใดมีสภาพเป็นผู้บุกรุก โดยใช้ข้อมูลที่ได้รับการรายงานจากเอเจนต์อื่นๆ
- **Global response** ทำหน้าที่รายงานว่าโหนดใดมีสภาพเป็นผู้บุรุกแก่ระบบแจ้งเตือนที่เกี่ยวข้อง หรือระบบจัดการเส้นทาง (Path manager) ที่เป็นการทำงานร่วมกันระหว่างโปรโตคอลค้นหาเส้นทางและระบบตรวจจับความผิดปกติในเครือข่าย

3.8 งานวิจัยที่เกี่ยวข้อง

ภายหลังจากได้มีการนำเสนอสถาปัตยกรรมของระบบตรวจจับความผิดปกติบนครือข่ายไร้สายแบบแอดฮอคแล้ว ได้มีหลายงานวิจัยที่นำโครงสร้างดังกล่าวมาเป็นแม่แบบในการพัฒนาระบบตรวจจับ โดยวิทยานิพนธ์นี้ได้ทำการศึกษาและรวบรวมมาเฉพาะระบบตรวจจับสำหรับการโจมตีแบบลดทิ้งข้อมูลดังนี้

3.8.1 Mitigating Routing Misbehavior in Mobile Ad Hoc Networks (Watchdog)

Sergio Marti [27] ได้นำเสนอระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติแบบลดทิ้งข้อมูลบนเครือข่ายไร้สายแบบแอดฮอคที่ใช้โปรโตคอลค้นหาเส้นทาง DSR และนับเป็นงานในระยะแรกที่มีการตรวจสอบพฤติกรรมของโหนดต้องสงสัยด้วยกระบวนการเฝ้าฟัง และได้ตั้งชื่อวิธีการเฝ้าฟังและตรวจจับที่นำเสนอในงานวิจัยนี้ว่าวอทช์ด็อก (Watchdog) มีแนวคิดคือการให้โหนดก่อนหน้าที่ส่งข้อมูลออกไปแล้วนั้น ทำการตรวจสอบว่าโหนดตัวถัดไปมีการส่งข้อมูลไปยังโหนดถัดไปอีกตัวหรือไม่ ดังตัวอย่างการทำงานในรูป 3.12



รูปที่ 3.12 แสดงการตรวจสอบการโจมตีโดยใช้วอทช์ด็อก

ขั้นตอนการทำงานของระบบตรวจจับแบบวอทช์ด็อกในรูป 3.12 มีดังนี้

1. ในระหว่างการนำส่งข้อมูลโหนดตัวกลาง B จะส่งข้อมูลไปยังโหนด M (ซึ่งเป็นผู้บุกรุก) เพื่อให้โหนด M นำส่งข้อมูลต่อไปยังโหนด C
2. หลังจากโหนด B นำส่งข้อมูลออกไปเรียบร้อยแล้วจะเริ่มทำการตรวจสอบพฤติกรรมการนำส่งข้อมูลของโหนด M โดยเฝ้าฟังว่าโหนด M ทำการส่งข้อมูลไปยังโหนด C ซึ่งเป็นโหนดตัวถัดไปหรือไม่
3. โหนด M ซึ่งเป็นผู้บุกรุก จะทำการโจมตีเส้นทางโดยการลดทิ้งข้อมูลที่ได้รับ
4. โหนด B จะทราบว่าโหนด M ไม่มีการนำส่งข้อมูลไปยังโหนด C จากการเฝ้าฟังที่ครบกำหนดเวลา ทำให้โหนด B ใช้ข้อมูลดังกล่าวทำการตัดสินสภาพการเป็นผู้บุกรุกของโหนด M ได้

องค์ประกอบที่ให้การทำงานของระบบตรวจจับแบบวอทช์ด็อกทำงานได้อย่างถูกต้องนั้น จำเป็นอย่างยิ่งที่เครือข่ายจะต้องมีสภาพแวดล้อมดังนี้

- โปรโตคอลที่ใช้ในการค้นเส้นทางต้องเป็นโปรโตคอล DSR เนื่องจากโหนดที่ทำกระบวนการวอทช์ด็อกต้องทราบถึงรูปแบบและเส้นทางการสื่อสาร
- เสาอากาศของโหนดทุกตัวต้องเป็นแบบไม่มีทิศทาง (Omni-Directional antenna) เพราะกระบวนการเฝ้าฟังจำเป็นต้องทำได้ในทุกทิศทางรอบตัวโหนด

จากรูปแบบการโจมตีที่ไม่มีความซับซ้อนในขณะนั้น ระบบตรวจจับแบบวอทช์ด็อกจึงนับเป็นระบบตรวจจับที่ดีและมีความถูกต้องให้การตรวจจับสูง แต่ในภายหลังได้มีการคิดค้นการโจมตีแบบร่วมกระทำขึ้น (Collusion Attack [28]) โดยการโจมตีจะทำโดยผู้บุกรุกอย่างน้อยสองตัวทำงานร่วมกันเพื่อปิดบังการเฝ้าฟังจากเอเจนต์ ทำให้ระบบตรวจจับแบบวอทช์ด็อกไม่สามารถรองรับการโจมตีแบบนี้ได้ เนื่องจากการเฝ้าฟังที่มีจุดอ่อนคือสามารถเฝ้าฟังได้จากโหนดข้างเคียงได้ในระดับเดียวเท่านั้น

รูปที่ 3.13 การโจมตีแบบร่วมกระทำที่สามารถหลีกเลี่ยงการตรวจจับแบบวอทช์ด็อก

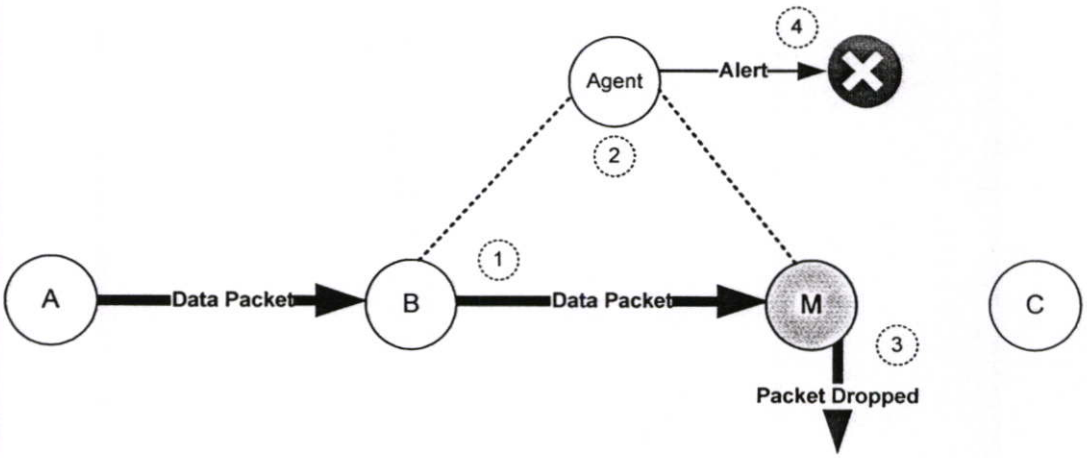
จากรูปที่ 3.13 การโจมตีแบบร่วมกระทำสามารถซ่อนตัวจากการเฝ้าฟังแบบวอทช์ด็อกได้จากขั้นตอนดังนี้

1. ในการนำส่งข้อมูลโหนดตัวกลาง B ทำการส่งข้อมูลไปยังโหนด M1 (ซึ่งเป็นผู้บุกรุก) เพื่อให้โหนด M1 นำส่งข้อมูลต่อไปยังโหนด M2 (ซึ่งเป็นผู้บุกรุกตัวที่ 2)
2. หลังจากโหนด B นำส่งข้อมูลออกไปเรียบร้อยแล้วจะเริ่มทำการตรวจสอบพฤติกรรมโดยวิธีวอทช์ด็อกเพื่อเฝ้าฟังการส่งข้อมูลไปยังโหนด M2 แต่การเฝ้าฟังจะพบว่าโหนด M1 มีการส่งข้อมูลไปยังโหนด M2 ตามที่ปกติ ทำให้โหนด B ไม่ถือว่าโหนด M1 เป็นผู้บุกรุก
3. โหนด M2 ซึ่งเป็นผู้บุกรุก จะทำการโจมตีเส้นทางโดยการลดทิ้งข้อมูลที่ได้รับ

โหนด M1 จะไม่ทำการรายงานความผิดปกติเนื่องจากเป็นผู้บุกรุก ทำให้เส้นทางการสื่อสารถูกทำลายโดยไม่สามารถตรวจสอบความผิดปกติของโหนดได้

3.8.2 On Intrusion Detection and Response for Mobile Ad Hoc Networks

James Parker [29] ได้นำเสนอการตรวจจับการโจมตีแบบลดทิ้งข้อมูลที่พัฒนาเพิ่มเติมจากระบบตรวจจับแบบวอท์ชด็อกเพื่อให้สามารถรองรับการโจมตีแบบร่วมกระทำได้ และได้เรียกวิธีการตรวจจับนี้ใหม่ว่า Snooping Protocol โดยมีความแตกต่างกับระบบตรวจจับแบบวอท์ชด็อกที่เทคนิคในการเฝ้าฟังที่อาศัยโหนดข้างเคียงรอบโหนดต้องสงสัย มาทำหน้าที่เฝ้าฟังพฤติกรรมการนำส่งข้อมูลแทนการใช้เพียงโหนดเดียวเหมือนวอท์ชด็อก จึงมีจุดเด่นที่สามารถขยายพื้นที่การเฝ้าฟังได้ครอบคลุมโหนดต้องสงสัยมากขึ้น และความแตกต่างอีกประการหนึ่งคือเงื่อนไขในตัดสินพฤติกรรมผิดปกติของการนำส่งข้อมูล เนื่องจากโหนดที่เฝ้าฟังไม่ได้เป็นโหนดในเส้นทาง ทำให้ไม่ทราบถึงสภาวะการนำส่งข้อมูลของ จึงไม่สามารถใช้เงื่อนไขการตัดสินแบบเดียวกับระบบตรวจจับแบบวอท์ชด็อกได้ วิธีการที่นำเสนอในงานวิจัยนี้คือการเปรียบเทียบข้อมูลขาเข้า (Incoming packet) และข้อมูลขาออก (Outgoing packet) ของโหนดตัวกลาง โดยอาศัยสมมุติฐานว่าหลังจากโหนดตัวกลางรับข้อมูลเข้ามาแล้วจะต้องส่งข้อมูลดังกล่าวออกไปทันที การตัดสินสภาพความผิดปกติของโหนดจึงทำได้โดยนำข้อมูลทั้งสองมาเปรียบเทียบกัน หากไม่ได้เป็นข้อมูลเดียวกันจะถือว่าโหนดตัวกลางมีสภาพผิดปกติ



รูปที่ 3.14 การตรวจจับการโจมตีโดยใช้วิธีการ Snooping protocol

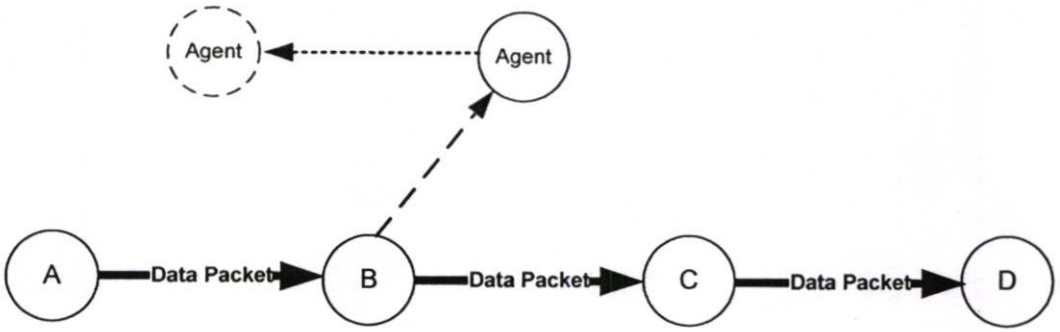
จากรูป 3.14 ได้แสดงถึงขั้นตอนการทำงานของ Snooping protocol ดังนี้

1. ในการนำส่งข้อมูลโหนดตัวกลาง B นำส่งข้อมูลไปยังโหนด M (ซึ่งเป็นผู้บุกรุก) เพื่อให้โหนด M นำส่งต่อไปยังโหนด C
2. โหนดที่อยู่ในรัศมีการสื่อสารของโหนด B และโหนด M จะทำการเฝ้าฟังว่าโหนด M มีการส่งข้อมูลออกไป ภายหลังจากที่ได้รับข้อมูลมาจากโหนด B หรือไม่
3. โหนด M เป็นซึ่งผู้บุกรุก จะทำการลดทิ้งข้อมูลโดยไม่นำส่งต่อไปยังโหนดตัวถัดไป

4. โหนดที่เฝ้าจะตรวจจับได้ว่าโหนด M ไม่มีการนำส่งข้อมูล เนื่องจากไม่มีการส่งข้อมูลออกมาภายหลังจากได้รับข้อมูลเข้าไปแล้ว

ความสามารถที่ Snooping Protocol ทำได้นอกเหนือจากตรวจจับการนำส่งข้อมูลที่ผิดปกติแล้ว คือการตรวจสอบการแก้ไขเปลี่ยนแปลงเนื้อหาข้อมูลของโหนดตัวกลางจากการเปรียบเทียบความแตกต่างระหว่างข้อมูลขาเข้าและขาออก

แม้ว่าการเทคนิคการเฝ้าฟังที่นำมาใช้บน Snooping Protocol จะสามารถตรวจจับการโจมตีทั้งแบบโหนดเดียวและแบบร่วมกระทำได้ แต่วิธีการเฝ้าฟังแบบนี้มีจุดอ่อนอยู่ตรงรัศมีการทำงานของโหนดเฝ้าฟัง [28][30] เนื่องจากการตรวจจับความผิดปกติจะทำได้ต่อเมื่อสามารถเฝ้าฟังได้ทั้งข้อมูลขาเข้าและขาออก ตำแหน่งของโหนดเฝ้าฟังจึงต้องอยู่ในรัศมีการส่งข้อมูลของทั้งโหนดก่อนหน้าและโหนดต้องสงสัย ทำให้ระบบตรวจจับไม่สามารถทำงานได้ดีเมื่อมีระยะห่างระหว่างทั้งสองโหนดมาก หรือในเครือข่ายที่การเคลื่อนที่ของโหนดมีผลต่อระยะการสื่อสาร ซึ่งจะทำให้การเฝ้าฟังทำได้ไม่สมบูรณ์และมีการรายงานความผิดปกติที่ผิดพลาด



รูปที่ 3.15 การเคลื่อนที่ของโหนด ทำให้ไม่สามารถเฝ้าฟังข้อมูลทั้งสองจุดได้

ในรูปที่ 3.15 ได้แสดงให้เห็นถึงการเคลื่อนที่ของโหนดเฝ้าฟังหลังจากได้รับข้อมูลขาเข้าของโหนด C แล้ว หากตำแหน่งใหม่ของโหนดเฝ้าฟังไม่อยู่ในรัศมีการนำส่งข้อมูลของโหนด C จะทำให้โหนดเฝ้าฟังไม่ได้รับข้อมูลขาออกแม้ว่าโหนด C จะส่งข้อมูลไปยังโหนด D ตามปกติ โหนดที่ทำการเฝ้าฟังจึงพิจาณาโหนด C ว่ามีพฤติกรรมผิดปกติ แต่ในความเป็นจริงโหนด C มีการทำงานถูกต้อง การเฝ้าฟังที่ไม่ครบถ้วนดังกล่าวจึงทำให้ระบบตรวจจับเกิดความผิดพลาดในการทำงานได้

บทที่ 4
ระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติแบบลดทิ้งข้อมูลในเครือข่ายไร้สายแบบแอดฮอค

4.1 บทนำ

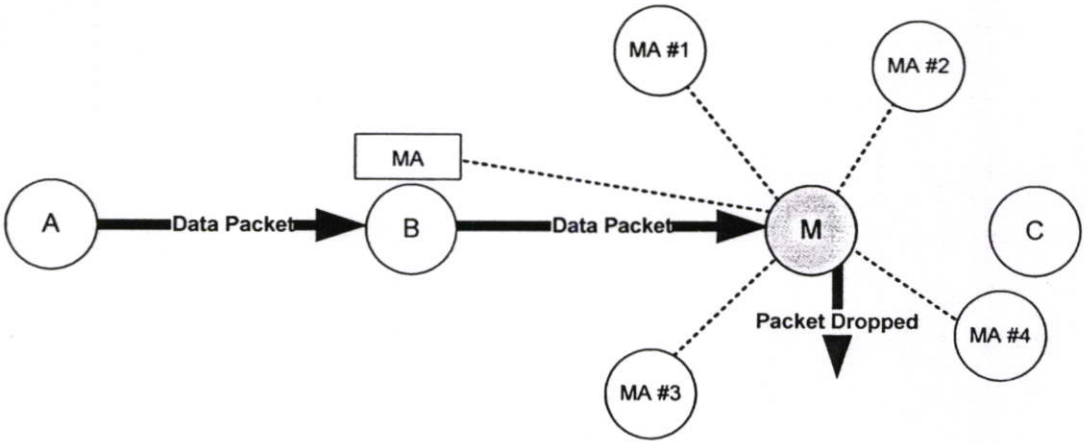
ในบทที่แล้วได้กล่าวถึงการโจมตีรูปแบบแบบต่างๆ บนเครือข่ายไร้สายแบบแอดฮอค รวมทั้งระบบตรวจจับความผิดปกติของโหนดในเครือข่ายจากงานวิจัยที่เคยมีการนำเสนอ โดยเน้นไปที่ระบบตรวจจับสำหรับการโจมตีแบบลดทิ้งข้อมูลเป็นหลัก แม้ว่าระบบดังกล่าวจะทำงานได้ดีและมีประสิทธิภาพเป็นที่น่าพอใจ แต่ปัจจุบันรูปแบบการโจมตีเครือข่ายได้ถูกพัฒนาให้มีความซับซ้อนและยากต่อการตรวจจับอยู่ตลอดเวลา จำเป็นอย่างยิ่งที่ระบบตรวจจับจะต้องได้รับการปรับปรุงและพัฒนาให้พร้อมรับมือกับการโจมตีรูปแบบใหม่ ในบทนี้ผู้วิจัยได้นำเสนอระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติแบบลดทิ้งข้อมูลแบบใหม่ โดยการใช้โมไบล์เอเจนต์ (Mobile agent) มาทำหน้าที่เฝ้าฟังเพื่อความครบถ้วนของข้อมูล รวมทั้งนำเสนอกระบวนการตรวจสอบและแลกเปลี่ยนข้อมูลที่มีความถูกต้องสูง โดยมีจุดประสงค์หลักเพื่อเพิ่มความแม่นยำในการตัดสินว่าโหนดใดมีสภาพเป็นผู้บุกรุก ซึ่งในส่วนท้ายของบทจะได้กล่าวถึงการเปรียบเทียบความสามารถในการตรวจจับกับระบบตรวจจับประเภทอื่นในแง่มุมต่างๆ รวมถึงการโจมตีที่อาจเกิดผลกระทบต่อความถูกต้องเมื่อมีการใช้ระบบตรวจจับในเครือข่าย

4.2 ความหมายและจุดประสงค์ในการใช้โมไบล์เอเจนต์

จุดอ่อนของการเฝ้าฟังที่อาศัยโหนดเพียงตัวเดียวเช่นในระบบตรวจจับแบบวอทช์ด็อก คือ ไม่สามารถตรวจจับการโจมตีแบบร่วมกระทำได้ เนื่องจากสามารถทำการเฝ้าฟังพฤติกรรมการนำส่งจากโหนดตัวถัดไปในเส้นทางการสื่อสารเท่านั้น ทำให้ผู้บุกรุกสามารถปิดบังและซ่อนการโจมตีได้

จากแนวคิดการนำโหนดบริเวณข้างเคียงมาทำหน้าที่เฝ้าฟังและตรวจจับพฤติกรรมการนำส่งข้อมูลของ Snooping Protocol วิทยานิพนธ์ฉบับนี้จึงเสนอการใช้โมไบล์เอเจนต์ ซึ่งความหมายหลักของคือโหนดสื่อสารทั่วไปที่ได้รับการติดตั้งระบบตรวจจับความผิดปกติ มาหน้าที่เฝ้าฟังแทนการใช้โหนดเพียงตัวเดียว โดยมีจุดประสงค์เพื่อเพิ่มพื้นที่ในการทำงานของระบบตรวจจับให้ครอบคลุมเครือข่ายมากที่สุด และเพิ่มโอกาสที่ระบบตรวจจับจะยังได้รับข้อมูลที่

ครบถ้วนแม้ว่าจะมีเอเจนต์บางตัวเคลื่อนที่ออกนอกรัศมีการเฝ้าฟัง ส่งผลให้การตัดสินว่าโหนดมีสภาพเป็นผู้บุกรุกมีความถูกต้องสูงสุด



รูปที่ 4.1 แสดงการเฝ้าฟังพฤติกรรมของผู้บุกรุกจากโมไบล์เอเจนต์

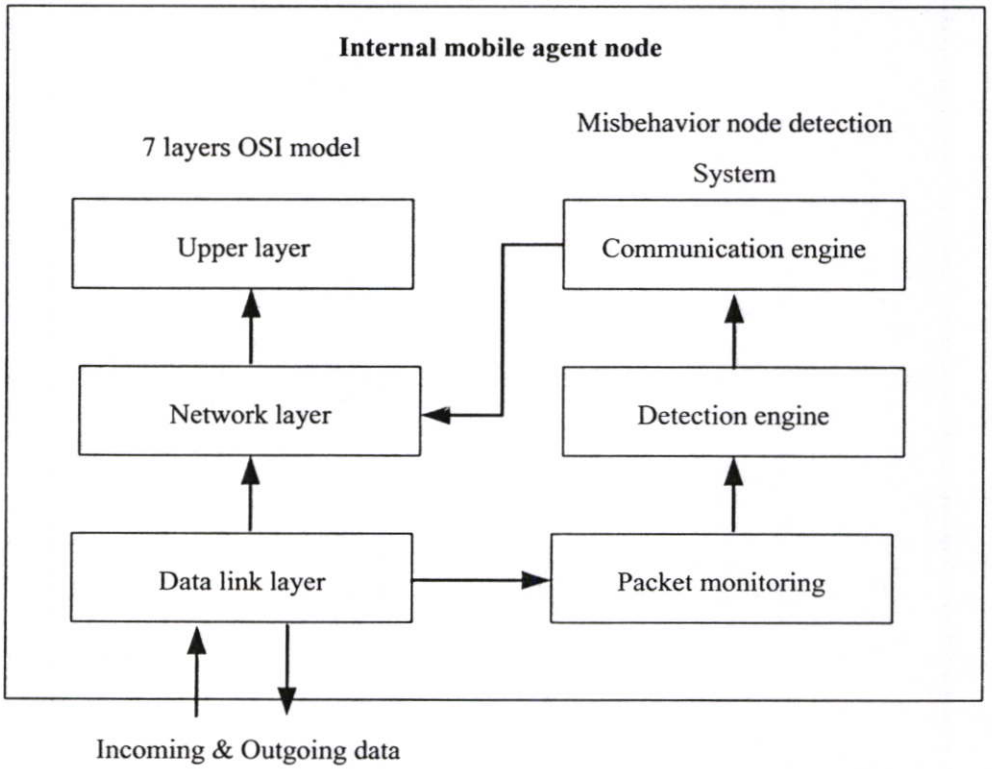
ตัวอย่างการเฝ้าฟังของโมไบล์เอเจนต์ที่ทำงานร่วมกันดังรูปที่ 4.1 จะพบว่าเป็นเฝ้าฟังทั้งจากโหนด B ซึ่งเป็นโหนดในเส้นทางการดังเช่นเดียวกับวอท์ชด็อก และอาศัยโหนดอื่นที่อยู่ข้างเคียงดังเช่นการเฝ้าฟังแบบ Snooping protocol (โมไบล์เอเจนต์ MA ทั้งสี่โหนด) จากสภาพแวดล้อมดังกล่าวทำให้รับประกันได้ว่าโหนดผู้บุกรุก M จะถูกเฝ้าฟังจากโหนดใดโหนดหนึ่งอย่างแน่นอน

แม้ว่าการใช้โมไบล์เอเจนต์จะทำให้ระบบตรวจจับมีโอกาสที่จะได้ข้อมูลครบถ้วนมากยิ่งขึ้น แต่ก็ยังมีความเสี่ยงที่จะทำให้กระบวนการเฝ้าฟังบนโมไบล์เอเจนต์ได้รับข้อมูลที่ผิดพลาด เช่นกรณีที่โมไบล์เอเจนต์หรือโหนดที่ถูกเฝ้าฟังมีการเคลื่อนที่ออกจากกันหรือเมื่อมีการชนกันของข้อมูล ซึ่งถือเป็นเหตุการณ์ปกติที่เกิดขึ้นได้บนเครือข่ายไร้สายแบบแอดฮอค เหตุการณ์ดังกล่าวจะส่งผลทำโมไบล์เอเจนต์ที่เฝ้าฟังอยู่นั้นได้รับข้อมูลที่ไม่ครบถ้วน และจากจำนวนโมไบล์เอเจนต์ที่ทำการเฝ้าฟังที่มาก จึงมีความเป็นไปมากยิ่งขึ้นที่จะมีโหนดใดโหนดหนึ่งได้รับข้อมูลจากการเฝ้าฟังที่ไม่ครบถ้วน การเฝ้าฟังที่ทำได้ไม่ครบถ้วนจะส่งผลให้โมไบล์เอเจนต์ตัดสินว่าโหนดที่ถูกเฝ้าฟังอยู่นั้นมีพฤติกรรมที่ผิดปกติแม้ว่าโหนดดังกล่าวจะมีการนำส่งข้อมูลตามปกติก็ตาม ดังนั้นเพื่อให้ผลการทำงานของระบบตรวจจับมีความถูกต้องมากที่สุด ในระบบตรวจจับที่มีอาศัยข้อมูลการเฝ้าฟังจากหลายแหล่ง จึงต้องมีกระบวนการยืนยันความถูกต้องของการเฝ้าฟังเพื่อคอยตรวจสอบว่าข้อมูลที่ได้จากโมไบล์เอเจนต์นั้นมีความผิดพลาดหรือไม่

4.3 โครงสร้างภายในของโหนดสื่อสารที่ทำหน้าที่เป็นโมไบล์เอเจนต์

การที่โหนดสื่อสารจะทำหน้าที่ทั้งการเป็นโมไบล์เอเจนต์และนำส่งได้ในขณะเดียวกันนั้น จะต้องมีส่วนประกอบภายในที่ต้องทำงานร่วมกันและแยกกันทำงาน โครงสร้างภายในของโหนดที่ทำงานเป็นโมไบล์เอเจนต์ในรูปที่ 4.2 มีส่วนประกอบดังนี้

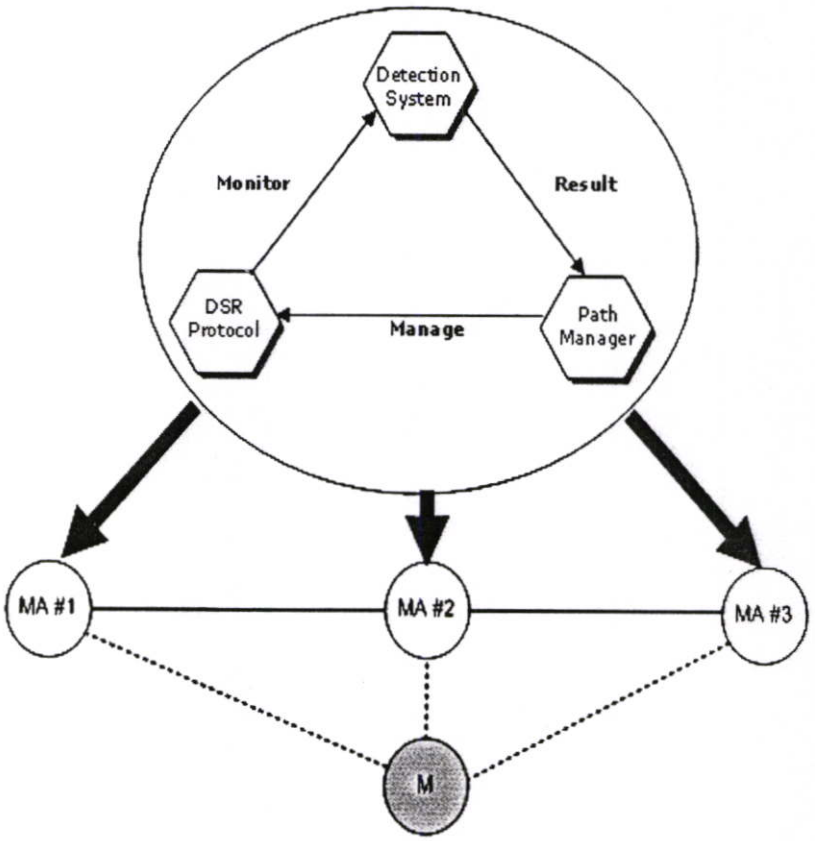
- **Packet monitoring** ทำหน้าที่เชื่อมต่อ (Tap) กับระดับชั้นดาตาลิงค์เพื่อเฝ้าฟังข้อมูลในรัศมีของการสื่อสาร เนื่องจากโปรโตคอล DSR ที่งานวิจัยนี้เลือกใช้เป็นต้นแบบในการศึกษามีการทำงานแบบโพรมิสคิวอัสในระดับชั้นดาตาลิงค์อยู่แล้ว ทำให้การเฝ้าฟังการสื่อสารของโหนดใกล้เคียงสามารถทำได้ แม้ว่าข้อมูลที่ส่งมาจะไม่ได้กำหนดผู้รับเป็นโหนดโมไบล์เอเจนต์ก็ตาม
- **Detection engine** ทำหน้าที่ตรวจจับพฤติกรรมที่ผิดปกติ โดยใช้ข้อมูลพฤติกรรมการสื่อสารที่ได้จากการเฝ้าฟัง มาทำการวิเคราะห์โดยเปรียบเทียบกับขั้นตอนทำงานของโหนดต้องสงสัยตามข้อกำหนดในโปรโตคอลการสื่อสาร
- **Communication engine** ทำหน้าที่สื่อสารกับโมไบล์เอเจนต์ตัวอื่นเพื่อแลกเปลี่ยนข้อมูล โดยโปรโตคอลการสื่อสารที่ใช้ได้ถูกออกแบบสำหรับระบบตรวจจับในงานวิจัยนี้โดยเฉพาะ



รูปที่ 4.2 โครงสร้างภายในโหนดสื่อสารที่ทำหน้าที่เป็นโมไบล์เอเจนต์

4.4 โครงสร้างและการทำงานระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติ

ในหัวข้อนี้จะเป็นการกล่าวถึงแนวคิดในการออกแบบโครงสร้างของระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติแบบลดทิ้งข้อมูล โดยมีความต้องการให้โหนดที่ทำหน้าที่เป็นโมไบล์เอเจนต์แต่ละตัวทำหน้าที่ตรวจจับและแลกเปลี่ยนข้อมูลกันอย่างสมบูรณ์แบบ ไม่จำเป็นต้องมีการจัดการหรือรวบรวมข้อมูลที่ศูนย์กลาง (De-centralize) และเมื่อระบบตรวจจับสามารถค้นพบว่าโหนดใดมีสภาพเป็นผู้บุกรุกแล้ว ข้อมูลดังกล่าวจะถูกนำมาใช้ในโปรโตคอล DSR เพื่อช่วยให้กระบวนการค้นหาเส้นทางที่จะเกิดขึ้นในครั้งต่อไปในเครือข่าย ให้สามารถหลีกเลี่ยงเส้นทางที่มีโหนดผู้บุกรุกปรากฏอยู่ได้ การทำงานแต่ละส่วนแสดงดังโครงสร้างในรูป 4.3



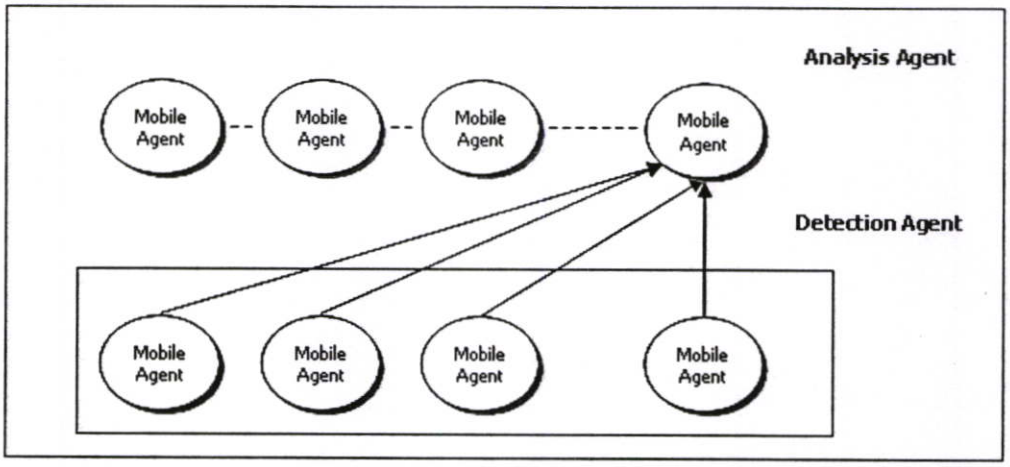
รูปที่ 4.3 โครงสร้างการทำงานของระบบตรวจจับที่นำเสนอ

4.4.1 การทำงานของระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติ

นอกจากกระบวนการเฝ้าฟังการสื่อสาร ที่ถือว่ามีความสำคัญอย่างมากต่อระบบตรวจจับความผิดปกติที่ทำงานบนเครือข่ายไร้สายแบบแอดฮอคแล้ว ขั้นตอนที่สำคัญอีกอย่างหนึ่งคือการนำ

ข้อมูลการเฝ้าฟังมาวิเคราะห์เพื่อตัดสินสภาพการเป็นผู้บุกรุก เนื่องจากต้องนำข้อมูลดังกล่าวไปใช้สำหรับกระบวนการค้นหาเส้นทางในครั้งต่อไป หน้าที่การทำงานของโมไบล์เอเจนต์บนระบบตรวจจับความผิดปกติที่นำเสนอในวิทยานิพนธ์ในฉบับนี้ จึงถูกออกแบบเป็นสองระดับดังรูปที่ 4.4

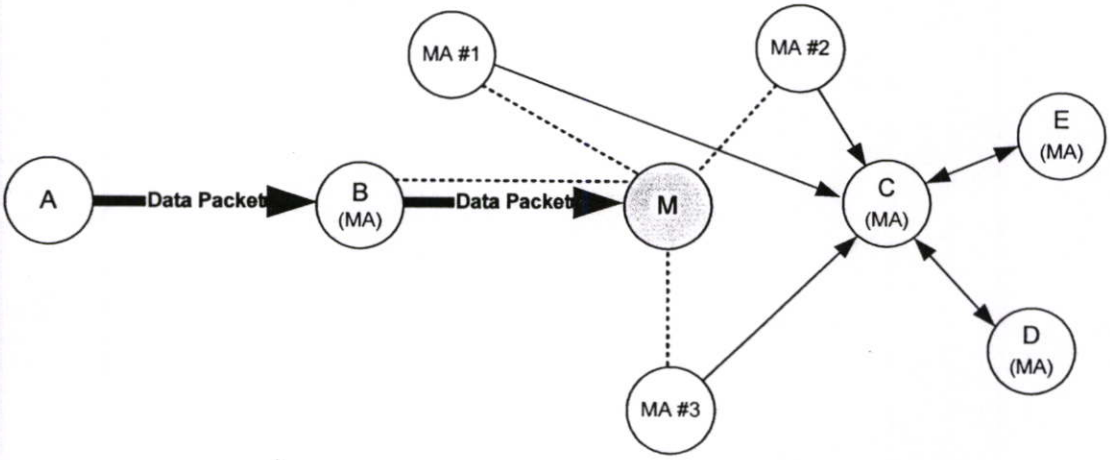
1. เฝ้าฟังและวิเคราะห์พฤติกรรมของโหนดต้องสงสัย (Detection agent) โมไบล์เอเจนต์จะทำหน้าที่นี้เมื่อตนเองอยู่ในบริเวณพื้นที่ที่มีการสื่อสาร หรืออาจเป็นส่วนหนึ่งของเส้นทางการสื่อสารนั้น ข้อมูลการวิเคราะห์ที่ได้จะรายงานไปยังโมไบล์เอเจนต์ที่ทำหน้าที่ตัดสินสภาพการเป็นผู้บุกรุกต่อไป
2. ตัดสินสภาพการเป็นผู้บุกรุกของโหนดต้องสงสัย (Analysis agent) หน้าที่นี้เป็นของโมไบล์เอเจนต์เมื่อตนเองเป็นโหนดปลายทางของเส้นทางสื่อสาร ข้อมูลที่ใช้ในการตัดสินจะได้ทั้งจากโมไบล์เอเจนต์ที่ทำหน้าที่เฝ้าฟัง และโมไบล์เอเจนต์ที่เคยทำหน้าที่ตัดสินสภาพผู้บุกรุกมาก่อน หรืออีกนัยหนึ่งคือโมไบล์เอเจนต์ที่เคยเป็นโหนดปลายทางในเส้นทางการสื่อสารอื่นในอดีต



รูปที่ 4.4 การทำงานร่วมกันของโมไบล์เอเจนต์ทั้งสองภาระหน้าที่

ตัวอย่างการทำงานของโมไบล์เอเจนต์รูปที่ 4.5 แสดงให้เห็นถึงขั้นตอนการทำงานที่มีการสื่อสารระหว่างกันในเครือข่าย โมไบล์เอเจนต์ที่ทำหน้าที่เฝ้าฟังซึ่งประกอบด้วยโหนด B ที่เป็นโหนดตัวกลางในเส้นทาง โหนด MA#1, MA#2 และ MA#3 ที่เป็นโหนดสื่อสารในเครือข่ายและอยู่ในรัศมีการเฝ้าฟัง จะคอยตรวจสอบพฤติกรรมการสื่อสารของโหนด M ที่ต้องสงสัยว่าเป็นผู้บุกรุก เมื่อโมไบล์เอเจนต์ที่ทำการเฝ้าฟังตรวจพบพฤติกรรมการนำส่งข้อมูลที่ผิดปกติของโหนด M จะทำการรายงานความผิดปกติดังกล่าวไปยังโหนด C ซึ่งเป็นโหนดปลายทางของเส้นทางการสื่อสารและทำหน้าที่ตัดสินสภาพผู้การเป็นบุกรุก เมื่อโหนด C ได้รับข้อมูลความผิดปกติจะทำการตรวจสอบความถูกต้องของข้อมูลดังกล่าว เมื่อพบว่าข้อมูลมีความถูกต้องและยืนยันได้ว่าโหนด M มี

พฤติกรรมการนำส่งข้อมูลที่ผิดปกติ โหนด C จะมีการสื่อสารกับโมไบล์เอเจนต์อื่นที่เคยทำหน้าที่ตัดสินสภาพผู้บุกรุกมาก่อน (จากรูปคือโหนด E และ D) เพื่อแลกเปลี่ยนข้อมูลความผิดปกติของโหนด C สำหรับการตัดสินสภาพความเป็นผู้บุกรุกของโหนด M ต่อไป



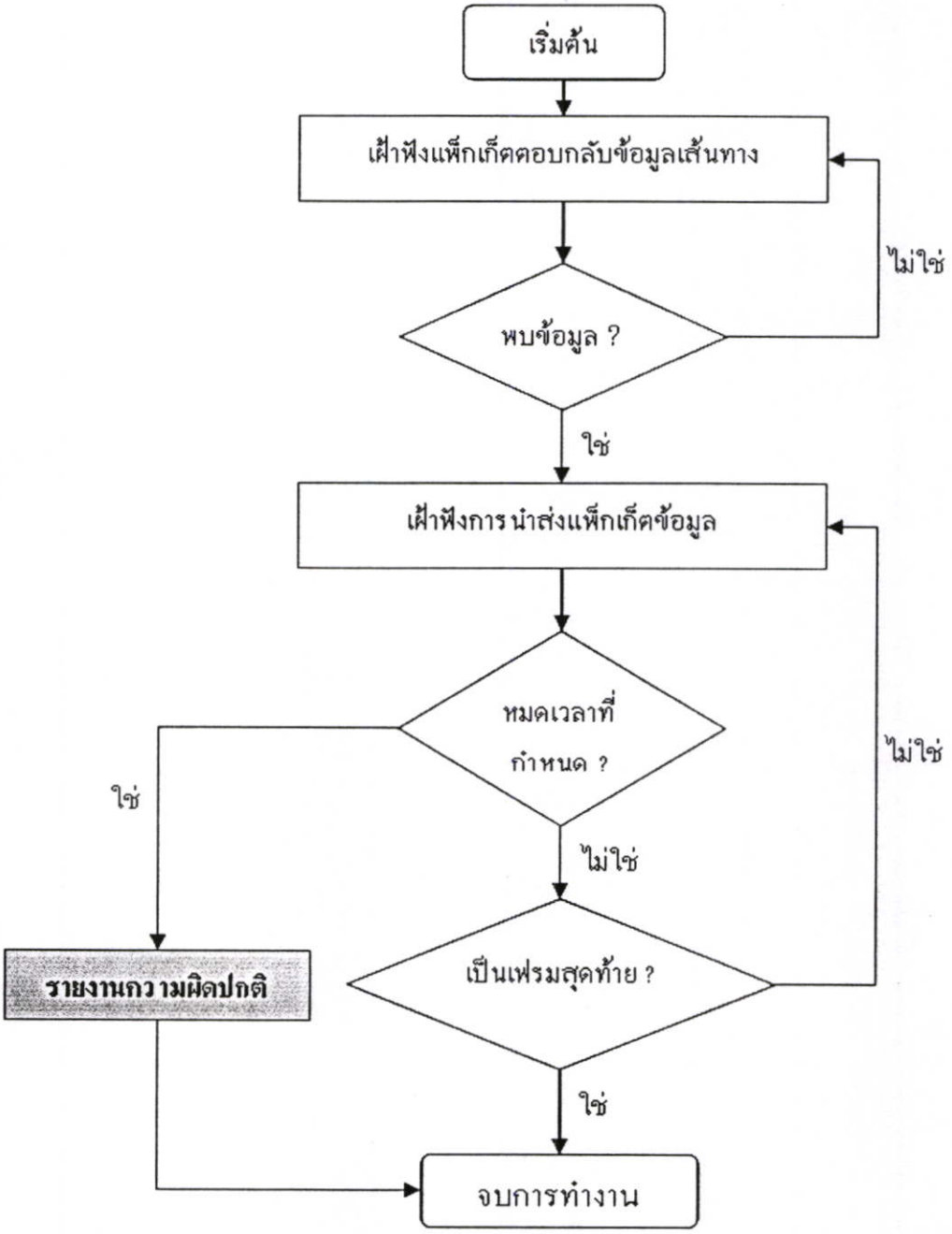
รูปที่ 4.5 การทำงานร่วมกันของโมไบล์เอเจนต์ในเครือข่าย

4.4.2 การทำงานของโมไบล์เอเจนต์เมื่อทำหน้าที่เฝ้าฟัง

การเฝ้าฟังถือเป็นกระบวนการที่สำคัญและมีผลต่อความถูกต้องในการทำงานของตรวจจับความผิดปกติ การใช้โมไบล์เอเจนต์ทำการเฝ้าฟังในวิทยานิพนธ์นี้มีจุดประสงค์เพื่อให้การเฝ้าฟังสามารถทำได้ครอบคลุมพื้นที่การสื่อสารให้มากที่สุดเท่าที่เป็นไปได้ การเฝ้าฟังพฤติกรรมการสื่อสารของโหนดต้องสงสัยจึงต้องพยายามให้มีจำนวนโมไบล์เอเจนต์ทำการเฝ้าฟังมากเท่าที่มากได้เพื่อลดความผิดพลาดที่อาจเกิดในระหว่างการเฝ้าฟังขึ้น

ข้อมูลเส้นทางการสื่อสารที่ปรากฏในโปรโตคอลค้นหาเส้นทางแบบ DSR ถือได้ว่าเป็นข้อมูลที่มีประโยชน์สำหรับการกำหนดสถานะการเฝ้าฟังและสถานะของโหนดที่เป็นตัวกลางของเส้นทาง เทคนิคการเฝ้าฟังที่นำเสนอในวิทยานิพนธ์นี้เกิดจากการค้นคว้าและศึกษาการทำงานของโปรโตคอล DSR อย่างหนักเพื่อให้โมไบล์เอเจนต์มีการทำงานร่วมกับโปรโตคอลค้นหาเส้นทางอย่างใกล้ชิด โดยเฉพาะการควบคุมสถานะการเฝ้าฟังของโมไบล์เอเจนต์ที่ใช้ประโยชน์จากข้อมูลในกระบวนการค้นหาเส้นทาง

หน้าที่สำคัญอย่างหนึ่งของโมไบล์เอเจนต์หลังนอกเหนือจากการเฝ้าฟัง คือการรายงานสภาพความผิดปกติของโหนดต้องสงสัยไปยังโหนดปลายทาง เพื่อทำการตัดสินสภาพความเป็นผู้บุกรุกของโหนดต้องสงสัยต่อไป

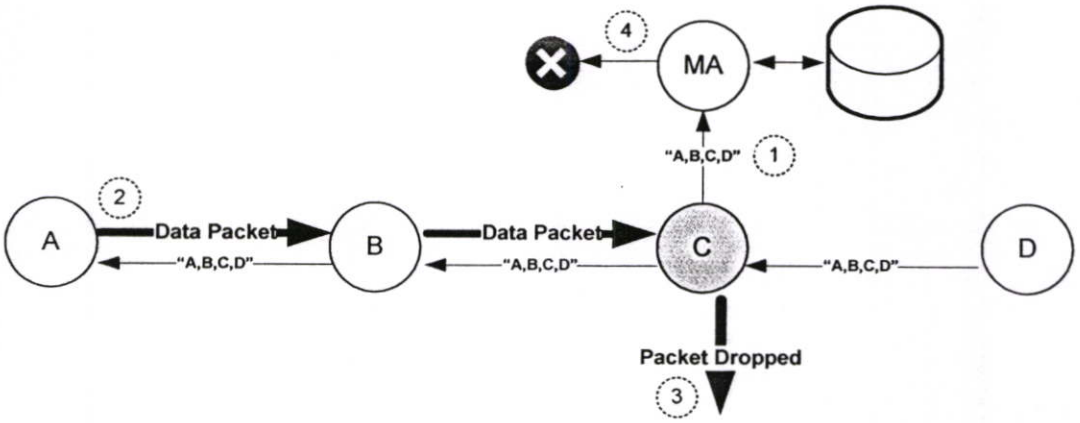


รูปที่ 4.6 วิธีการทำงานของโมไบล์เอเจนต์เมื่อทำหน้าที่เฝ้าฟัง

4.4.2.1 วิธีการเฝ้าฟังของโมไบล์เอเจนต์สำหรับโปรโตคอลค้นหาเส้นทาง DSR

จากวิธีการเฝ้าฟังในรูปที่ 4.6 ได้แสดงให้เห็นถึงกระบวนการเฝ้าฟังของโมไบล์เอเจนต์ที่มีการทำงานร่วมกับโปรโตคอลค้นหาเส้นทาง DSR อย่างใกล้ชิด โดยเทคนิคการเฝ้าฟังที่นำเสนอนี้ทำงานบนสมมติฐานที่ว่า ภายหลังจากโปรโตคอล DSR เสร็จสิ้นกระบวนการค้นหาเส้นทางแล้ว โหนดที่อยู่ในเส้นทางจะต้องต้องมีการรับและส่งต่อข้อมูลภายในระยะเวลาที่กำหนด เพราะ

โปรโตคอลค้นหาเส้นทาง DSR อยู่มีการทำงานแบบ On-Demand ขั้นตอนการเฝ้าฟังจึงเริ่มต้นด้วยการที่โมไบล์เอเจนต์เฝ้าฟังแพ็กเก็ตตอบกลับข้อมูลเส้นทางซึ่งถูกส่งออกมาจากโหนดในเส้นทาง เมื่อพบว่าโหนดใดมีการส่งแพ็กเก็ตดังกล่าวออกมา โมไบล์เอเจนต์จะทำการบันทึกข้อมูลที่ใช้สำหรับการวิเคราะห์พฤติกรรมไว้ในฐานข้อมูล โดยกำหนดในเบื้องต้นว่าโหนดดังกล่าวเป็นโหนดต้องสงสัย หลังจากจากนั้นโมไบล์เอเจนต์จะเริ่มการตรวจสอบการนำส่งข้อมูลของโหนดต้องสงสัย หากโหนดดังกล่าวไม่มีการส่งข้อมูลออกมาภายในเวลาที่กำหนดไว้ จะตัดสินได้ว่าโหนดต้องสงสัยนั้นมีพฤติกรรมการนำส่งข้อมูลที่ผิดปกติ



รูปที่ 4.7 ขั้นตอนการตรวจสอบการนำส่งข้อมูลที่ผิดปกติบนเครือข่าย

ตัวอย่างเครือข่ายในรูปที่ 4.7 แสดงขั้นตอนที่จะระบบตรวจจับเริ่มทำการเฝ้าฟัง ซึ่งมีลำดับการทำงานดังนี้

1. โมไบล์เอเจนต์ MA เฝ้าฟังแพ็กเก็ตตอบกลับข้อมูลเส้นทางที่ส่งออกมาจากโหนด C ที่เป็นผู้บุรุก เหตุผลที่การเฝ้าฟังสามารถทำได้แม้ว่าปลายทางของแพ็กเก็ตจะเป็นโหนด B เนื่องจากเสาอากาสที่ใช้เป็นแบบรอบทิศทาง และการทำงานแบบโพรมิสคิวอัสของโมไบล์เอเจนต์
2. เมื่อแพ็กเก็ตตอบกลับข้อมูลเส้นทางถูกส่งกลับมายังต้นทางเรียบร้อยแล้ว โหนดจะเริ่มทำการส่งแพ็กเก็ตข้อมูลผ่านเส้นทางที่แจ้งในแพ็กเก็ตตอบกลับข้อมูลเส้นทาง โดยใช้เส้นทางดังกล่าวเพียงเส้นทางเดียวจนเสร็จสิ้น
3. เมื่อโหนด B นำส่งข้อมูลไปยังโหนดผู้บุกรุก C โหนดผู้บุกรุกทำการโจมตีโดยลดทิ้งข้อมูลที่ต้องส่งไปยังโหนด D

4. โมไบล์เอเจนต์ MA ที่ทำการเฝ้ารอว่าโหนดผู้บุกรุกมีการนำส่งข้อมูลออกมาหรือไม่ หลังจากการทำงานในขั้นตอนที่ 1 จะตรวจจับได้ว่าโหนดผู้บุกรุกไม่มีการนำส่งข้อมูลออกมา จึงตัดสินในเบื้องต้นนี้ว่าโหนด C มีความผิดปกติเกิดขึ้น

4.4.2.2 การเก็บข้อมูลและการกำหนดสถานะ

โมไบล์เอเจนต์ที่อยู่ในสภาวะการเฝ้าฟังจะมีการทำงานแบ่งเป็นสองสภาวะคือ เฝ้าฟังการส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทางและเฝ้าฟังการนำส่งข้อมูล บนโมไบล์เอเจนต์จึงต้องมีการเก็บข้อมูลเพื่อระบุว่ากำลังอยู่สภาวะการทำงานใด รูปที่ 4.8 แสดงให้เห็นถึงรูปแบบการเก็บข้อมูล

Sender	Source	Destination	Path	Received Time
C	A	D	B,C	3.072346242
J	L	I	M,N	4.382356840
I	M	H	Y,Z,I	6.788355280

รูปที่ 4.8 ตัวอย่างข้อมูลการเฝ้าฟังที่บันทึกบนโมไบล์เอเจนต์

ข้อมูลที่ถูกจัดเก็บมีดังนี้

- โหนดที่ทำการส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทางออกมาซึ่งจะถือว่าเป็นโหนดต้องสงสัย
- โหนดต้นทางของเส้นทางการสื่อสาร
- โหนดปลายทางของเส้นทางการสื่อสาร
- ลำดับของโหนดตัวกลางในเส้นทาง
- เวลาที่ได้รับแพ็กเก็ตตอบกลับข้อมูลเส้นทาง

โหนดที่ถูกบันทึกว่าเป็นโหนดต้องสงสัยจะถูกโมไบล์เอเจนต์ทำการเฝ้าฟังพฤติกรรมการนำส่งข้อมูลอยู่ตลอดเวลาที่โหนดต้นทางยังคงทำการส่งข้อมูล การเฝ้าฟังยุติเมื่อโมไบล์เอเจนต์ตรวจพบว่าโหนดต้องสงสัยมีพฤติกรรมผิดปกติจากการไม่นำส่งข้อมูล หรือโหนดต้องสงสัยทำการนำส่งข้อมูลครบถ้วนแล้วซึ่งจะถือว่าโหนดมีสภาพปกติ

4. 4.2.3 การเฝ้าฟังข้อมูลที่ถูกแบ่งเป็นเฟรมย่อย

ขนาดของข้อมูลที่สามารถนำส่งได้ในแต่ละครั้ง (Maximum Transfer Unit: MTU) จะถูกกำหนดจากโปรโตคอลการสื่อสารเพื่อให้อุปกรณ์แต่ละชนิดสามารถใช้งานร่วมกันได้ หากข้อมูลที่โหนดต้องทางต้องการส่งมีขนาดใหญ่เกินกว่าที่กำหนดไว้ ข้อมูลทั้งหมดจะถูกแบ่งย่อย (Fragment)

ออกเป็นเฟรมขนาดเล็กหลายเฟรม และจะถูกส่งไปโหนดยังปลายทางผ่านเส้นทางการสื่อสารทีละเฟรมตามลำดับจนครบ เมื่อโหนดปลายทางได้รับข้อมูลทั้งหมดจะทำการประกอบ (Re-assemble) เฟรมย่อยเหล่านั้นให้กลับมาเป็นข้อมูลเดิมเพื่อใช้งาน

ในกรณีที่มีการเฝ้าฟังข้อมูลที่ถูกแบ่งเป็นเฟรมย่อย ระบบตรวจจับความผิดปกติจะต้องตรวจสอบว่าโหนดต้องสงสัยทำการนำส่งข้อมูลจนครบทุกเฟรมหรือไม่ วิทยานิพนธ์นี้ได้เสนอวิธีการตรวจสอบความครบถ้วนของข้อมูลจากแฟลกระบุข้อมูลคงเหลือ (More Flag: MF) ในระดับชั้นเน็กเวิร์ก ข้อมูลขนาด 1 บิตจากแฟลกระบุข้อมูลคงเหลือสามารถอธิบายความครบถ้วนของข้อมูลดังนี้

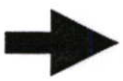
- MF = 0 แสดงไม่มีข้อมูลที่จะส่งมาหลังจากเฟรมนี้ จะเกิดขึ้นในกรณีโหนดส่งข้อมูลเพียงเฟรมเดียว หรือเฟรมที่ได้รับนี้เป็นเฟรมสุดท้ายของข้อมูลทั้หมด
- MF = 1 แสดงว่ายังคงข้อมูลคงเหลือในเฟรมต่อไป ซึ่งจะส่งมาหลังจากเฟรมนี้

จากสถานะดังกล่าว การตรวจสอบว่าโหนดส่งข้อมูลครบถ้วนหรือไม่จึงสามารถทำได้โดยให้โมไบล์เอเจนต์เฝ้าฟังไปจนกระทั่งพบเฟรมข้อมูลที่มีค่า MF = 0 จึงจะถือว่าโหนดต้องสงสัยทำหน้าที่นำส่งข้อมูลได้ครบถ้วนและโมไบล์เอเจนต์จะยุติการเฝ้าฟัง แต่หากโมไบล์เอเจนต์ไม่พบการส่งเฟรมข้อมูลดังกล่าว จะตัดสินว่าโหนดต้องสงสัยมีพฤติกรรมการนำส่งข้อมูลที่ผิดปกติและยุติการเฝ้าฟังเช่นเดียวกัน

การเก็บข้อมูลพฤติกรรมของโหนดต้องสงสัยสำหรับการเฝ้าฟังกรณีนี้ โมไบล์เอเจนต์จะทำการปรับเวลาการได้รับแพ็กเก็ตทุกครั้งที่ตรวจพบเฟรมข้อมูลที่มีค่า MF = 1 เพื่อให้การเฝ้าฟังเริ่มนับเวลาการเฝ้าคอยใหม่อีกครั้ง

Current time = t

Sender	Last Received Time
C	3.072346242
J	4.382356840
I	6.788355280



Current time = t'

Sender	Last Received Time
C	3.978979879
J	5.587998548
I	7.587859965

รูปที่ 4.9 การปรับเวลาที่ได้รับแพ็กเก็ตเพื่อเริ่มการรอคอยข้อมูลเฟรมต่อไป

4. 4.2.4 ระยะเวลารอคอยข้อมูล

การตัดสินว่าโหนดต้องสงสัยมีพฤติกรรมผิดปกติในการนำส่งข้อมูลหรือไม่ วิทยานิพนธ์นี้ได้ใช้วิธีเดียวกันกับระบบตรวจจับแบบวอทช์ด็อกและ Snooping protocol คือการตัดสินจากเวลาการเฝ้าคอยข้อมูลเป็นตัวตัดสิน ซึ่งเป็นการตัดสินบนการทำงานบนหลักการของโปรโตคอลค้นหา

เส้นทางที่ทำงานแบบ On-demand ที่ ข้อมูลจะต้องถูกนำส่งจากต้นทางมายังปลายทางทันทีหลักจากเสร็จสิ้นกระบวนการค้นหาเส้นทางการสื่อสาร และในกรณีที่ข้อมูลถูกแบ่งออกเป็นเฟรมย่อย แต่ละเฟรมจะต้องถูกนำส่งจนเสร็จสิ้นการสื่อสารเพียงครั้งเดียวเท่านั้น เวลาสำหรับการรอคอยข้อมูลทั้งสองกรณีสามารถประมาณค่าได้ดังนี้

1. เวลาในการรอคอยสำหรับข้อมูลเฟรมแรก โดยเริ่มตั้งแต่โมไบล์เอเจนต์ตรวจพบว่ามีการส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทาง สามารถประมาณค่าได้ดังนี้

$$1^{st}\ \text{Arrival Time} = \sum_{i}^{N} RRPtime + \sum_{i}^{N} DStime \qquad (4.1)$$

โดย RRPtime คือเวลาที่ใช้ในนำส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทางกลับไปยังโหนดต้นทาง และ DStime คือเวลาที่ใช้ในการนำส่งเฟรมข้อมูล โดยเวลาทั้งสองส่วนจะเพิ่มมากขึ้นหากเส้นทางการสื่อสารประกอบด้วยโหนดตัวกลางจำนวนมาก

2. เวลาในการรอคอยข้อมูลระหว่างเฟรม จะมีระยะเวลาขึ้นอยู่กับความล่าช้าของกระบวนการนำส่งข้อมูลในแต่ละโหนด ซึ่งจะมีความแตกต่างเล็กน้อยจากระดับความสามารถในการประมวลของแต่ละโหนด

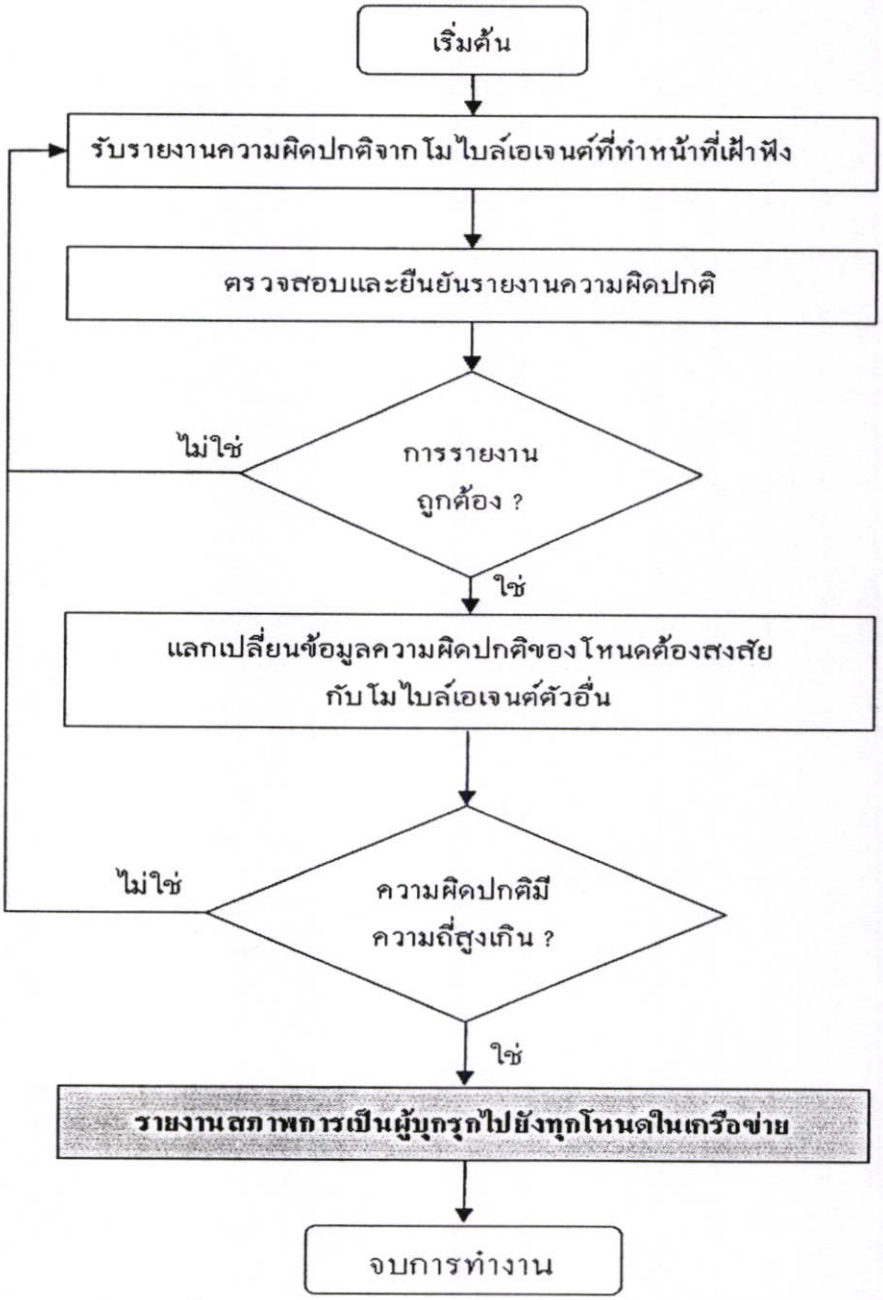
เพื่อพิจารณาถึงเวลาการเฝ้ารอข้อมูลทั้งสองกรณี จะพบว่าหน่วยเวลาที่ได้มีความละเอียดสูงมากในในระดับ Millisecond ซึ่งยากต่อการคำนวณและนำมาใช้ในสภาพแวดล้อมเครือข่ายจริงที่มีตัวแปรเกี่ยวข้องมากมาย เช่นความสามารถในการประมวลผลที่แตกต่างกันในแต่ละโหนด, ขนาดและวิธีการจัดการคิว (Queue) ของระบบปฏิบัติการที่แตกต่างกัน, หรือแม้แต่ขนาดของข้อมูลแต่ละเฟรมที่จะส่งผลต่อระยะเวลาในการนำส่งที่อาจแตกต่างกัน การกำหนดระยะเวลาการเฝ้ารอข้อมูลสำหรับการเฝ้าฟังบนระบบตรวจจับแบบต่างๆ จึงมักจะมีการกำหนดแบบหยาบโดยอาศัยตัวแปรทางเครือข่ายสองประการคือ

1. การหมดเวลา (Time out) ของโปรโตคอลที่ทำงานในระดับแอพพลิเคชัน เช่นกรณีของเวบเซิร์ฟเวอร์ การกำหนดระยะเวลานำส่งข้อมูลแต่ละเฟรมได้ถึง 30 วินาที หรือแอพพลิเคชันที่เกี่ยวข้องกับข้อมูลภาพและเสียง อาจมีการกำหนดเวลาการนำส่งข้อมูลแต่ละเฟรมไม่ให้เกิน 0.5 วินาที เป็นต้น

2. เวลาความล่าช้าสูงสุดของการนำส่งในเครือข่ายปกติ เป็นการใช้ข้อมูลที่ได้จากการทำสถิติบนเครือข่ายจริง เพื่อให้ได้ระยะเวลาการรอคอยข้อมูลมีความสัมพันธ์กับสภาพเครือข่าย

4.4.3 การทำงานของโมไบล์เอเจนต์เมื่อทำหน้าที่ตัดสินสภาพความผิดปกติ

การตัดสินสภาพความผิดปกติ จะทำโดยโมไบล์เอเจนต์ที่เป็นโหนดปลายทางของเส้นทางหลังจากที่ได้รับรายงานจากโมไบล์เอเจนต์ที่รับหน้าเฝ้าฟังแล้ว การตัดสินสภาพความผิดจะใช้การเปรียบเทียบทางสถิติ โหนดต้องสงสัยใดที่มีความถี่สะสมของพฤติกรรมความผิดปกติสูงเกินกว่าค่าที่ยอมรับได้ จะถือว่าโหนดนั้นมีสภาพเป็นผู้บุกรุกและจะถูกยกเลิกการใช้งานในเครือข่าย



รูปที่ 4.10 ขั้นตอนการตัดสินสภาพผู้บุกรุกของโหนดที่ต้องสงสัย

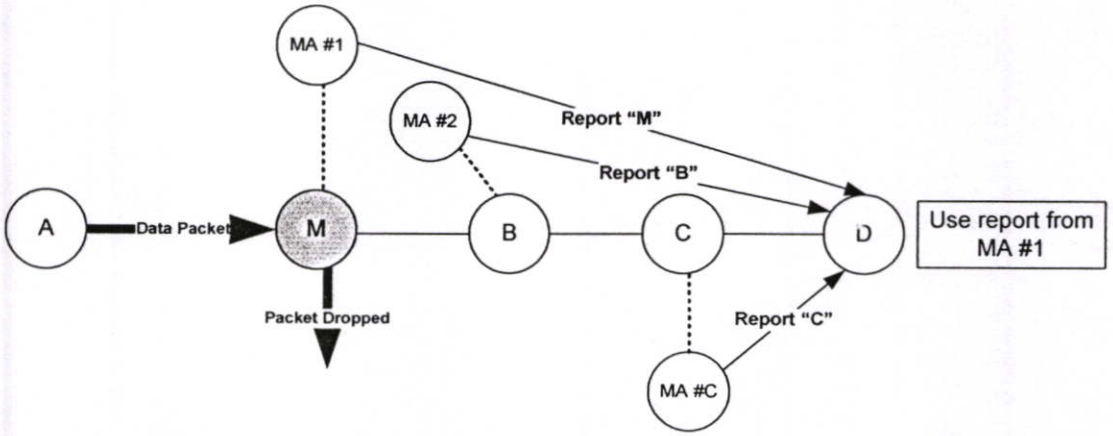
4.4.3.1 รายงานความผิดปกติจากโมไบล์เอเจนต์ที่ทำหน้าที่เฝ้าฟัง

การรายงานความผิดปกติจะเกิดขึ้นหลังจากโมไบล์เอเจนต์ที่ทำการเฝ้าฟังตรวจพบพฤติกรรมการนำส่งข้อมูลที่ผิดปกติของโหนดต้องสงสัย การรายงานจะทำให้เพื่อให้โหนดปลายทางทราบว่าโหนดตัวกลางใดมีพฤติกรรมผิดปกติและเกิดขึ้นในเวลาใด ดังตัวอย่างข้อมูลในรูปที่ 4.11

Misbehavior Node	Path	Time Stamp
C	B,C	6.788355280

รูปที่ 4.11 รายงานชื่อโหนดที่มีพฤติกรรมผิดปกติและเวลาที่ตรวจจับได้

ในเส้นทางการสื่อสารที่ประกอบด้วยโหนดตัวกลางหลายตัว หากโหนดตัวกลางใดมีพฤติกรรมการลดทิ้งข้อมูลเกิดขึ้น จะส่งผลให้โหนดตัวกลางตัวถัดไปที่แม้ไม่ได้เป็นผู้บุกรุก ไม่ทำการนำส่งข้อมูลตามได้ด้วยเนื่องจากไม่ได้รับข้อมูลจากโหนดก่อนหน้า ส่งผลให้โหนดตัวกลางทุกตัวที่อยู่ในเส้นทางถัดจากผู้บุกรุกถูกตรวจพบว่ามีพฤติกรรมผิดปกติด้วย เพื่อป้องกันไม่ให้การตรวจจับทำงานผิดพลาดจากกรณีดังกล่าว ในกรณีที่โหนดปลายทางได้รับการรายงานความผิดปกติจากโมไบล์เอเจนต์หลายรายงาน โหนดปลายทางจะเลือกใช้รายงานจากโมไบล์เอเจนต์ที่เฝ้าฟังโหนดที่อยู่ใกล้ต้นทางมากที่สุดเท่านั้น

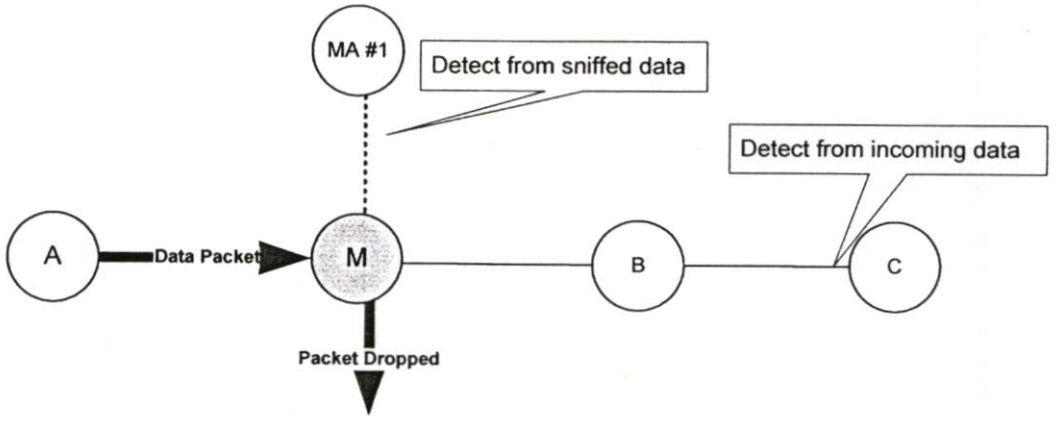


รูปที่ 4.12 โหนดตัวกลางที่อยู่ถัดจากผู้บุกรุกจะถูกระบุว่าไม่มีการนำส่งข้อมูลเสมอ

4.4.3.2 การตรวจสอบและยืนยันรายงานที่ได้จากโมไบล์เอเจนต์

การตัดสินว่าโหนดตัวกลางใดไม่ทำการนำส่งข้อมูล อาจเกิดความผิดพลาดขึ้นได้จากการที่โมไบล์เอเจนต์หรือโหนดต้องสงสัยเคลื่อนที่ออกห่างจากกันจนพ้นรัศมีการเฝ้าฟัง หรือเกิดการชนกันของข้อมูลในระหว่างการเฝ้าฟัง ส่งผลให้โมไบล์เอเจนต์ตัดสินว่าโหนดต้องสงสัยไม่มีการนำส่งข้อมูล ซึ่งในความเป็นจริงโหนดดังกล่าวอาจมีการนำส่งข้อมูลตามปกติเพียงแต่โมไบล์เอเจนต์ไม่สามารถเฝ้าฟังได้ ถือเป็นความผิดพลาดแบบ False Positive [31] เพื่อป้องกันไม่ให้ระบบตรวจจับทำการตัดสินสภาพความเป็นผู้บุกรุกบนข้อมูลการเฝ้าฟังที่ผิดพลาด จึงต้องมีการตรวจสอบและยืนยันว่ารายงานที่ได้จากโมไบล์เอเจนต์นั้นมีความถูกต้อง โดยใช้แนวคิดว่าหากโหนดปลายทางได้รับข้อมูลครบถ้วนแล้ว จะถือว่าโหนดทุกตัวในเส้นทางการสื่อสารไม่มีสภาพเป็นผู้บุกรุกโดยปริยาย ซึ่งหากมีโมไบล์เอเจนต์ทำการรายงานความผิดปกติมายังโหนดปลายทาง จะถือว่าข้อมูลดังกล่าวมีความผิดพลาดจากการเฝ้าฟังซึ่งจะไม่นำมาใช้ตัดสินสภาพการเป็นผู้บุกรุก แต่ในกรณีข้อมูลที่โหนดปลายทางได้รับนั้นยังไม่ครบถ้วนและมีการรายงานความผิดปกติจากโมไบล์เอเจนต์จะถือว่าการรายงานดังกล่าวถูกต้องและนำมาใช้ตัดสินสภาพการเป็นผู้บุกรุก

วิธีการตรวจสอบว่าโหนดปลายทางได้รับข้อมูลครบถ้วนหรือไม่นั้น จะใช้วิธีเดียวกับการเฝ้าฟังของโมไบลเอเจนต์ที่อาศัยสถานะของแฟลกระบุข้อมูลคงเหลือเป็นเครื่องมือ จากวิธีการดังกล่าวแสดงให้เห็นว่าการทำงานของโมไบล์เอเจนต์ในหน้าที่การเฝ้าฟังและการตัดสินสภาพการเป็นผู้บุกรุก ต่างก็มีความสามารถในการตรวจสอบความครบถ้วนของข้อมูลทั้งคู่ ต่างกันเพียงโมไบล์เอเจนต์ในทำการเฝ้าฟังจะใช้ข้อมูลที่ดักฟังได้ แต่ในโมไบล์เอเจนต์ที่ทำหน้าที่ตัดสินสภาพการเป็นผู้บุกรุกจะใช้ข้อมูลที่ตนเองได้รับโดยตรง

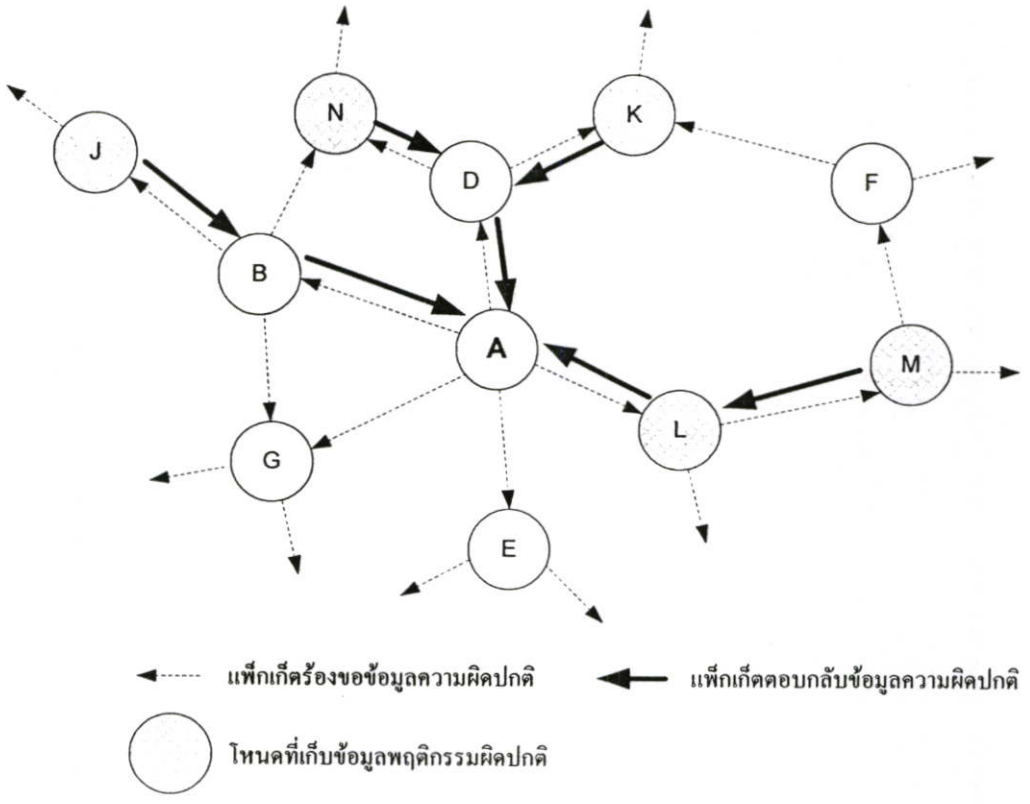


รูปที่ 4.13 การตรวจสอบความครบถ้วนของข้อมูลจากการได้มาที่แตกต่างกัน

4.4.3.3 การแลกเปลี่ยนข้อมูลความผิดปกติระหว่างโมไบล์เอเจนต์

วิธีการตัดสินสภาพการเป็นผู้บุกรุกในวิทยานิพนธ์ฉบับนี้ ได้ใช้การพิจารณาจากความถี่สะสมของพฤติกรรมผิดปกติสะสมของโหนดต้องสงสัย แต่เนื่องจากพฤติกรรมผิดปกติของผู้บุกรุกสามารถเกิดได้ทั่วพื้นที่เครือข่ายขึ้นอยู่กับตำแหน่งของโหนด ทำให้ข้อมูลพฤติกรรมที่ผิดปกติถูกเก็บไว้บนโหนดปลายทางในแต่ละเส้นทางอย่างกระจัดกระจาย เมื่อจะทำการตรวจสอบสภาพการเป็นผู้บุกรุกของโหนดต้องสงสัยใด จะต้องทำการรวบรวมข้อมูลพฤติกรรมของโหนดต้องสงสัยนั้นให้มาอยู่บนโมไบล์เอเจนต์ที่ทำหน้าที่ตัดสินสภาพการเป็นผู้บุกรุกเสียก่อน

การรวบรวมข้อมูลพฤติกรรมจากโมไบล์เอเจนต์ตัวอื่นๆ มายังตนเองนั้น จะใช้วิธีการร้องขอ (Request) และตอบกลับ (Response) โดยเมื่อใดที่โมไบล์เอเจนต์ทำการตัดสินสภาพการเป็นผู้บุกรุกจะต้องส่งการร้องขอข้อมูลความผิดปกติของโหนดต้องสงสัย (Request Misbehavior data) ไปยังโหนดทุกตัวในเครือข่ายโดยวิธีบรอดแคสต์ หากโหนดใดมีข้อมูลความผิดปกติของโหนดต้องสงสัยดังกล่าวในฐานข้อมูล จะตอบกลับด้วยข้อมูลความผิดปกติของโหนดต้องสงสัย (Response Misbehavior data) ซึ่งระบุถึงเส้นทางและเวลาที่สามารถตรวจจับความผิดปกติของโหนดต้องสงสัยดังกล่าวได้ สำหรับส่งข้อมูลตอบกลับจะเป็นการส่งแบบยูนิแคสต์เพื่อลดโอเวอร์เฮดของเครือข่าย



รูปที่ 4.14 การนำส่งข้อมูลร้องขอและตอบกลับข้อมูลความผิดปกติ

Request	
Investigated Node	**Path**
C	B,C

Response (Investigated Node = "C")	
Path	**Detecting Time**
A,B,C	6.788355280
H,C,J,K	9.854215879
I,C,O	12.879135467
C,P,Q,R	16.8681354528

รูปที่ 4.15 ตัวอย่างข้อมูลการร้องขอตอบกลับข้อมูลความผิดปกติของโหนด C

4.4.3.4 การพิจารณาสภาพการเป็นผู้บุกรุกและการรายงานผล

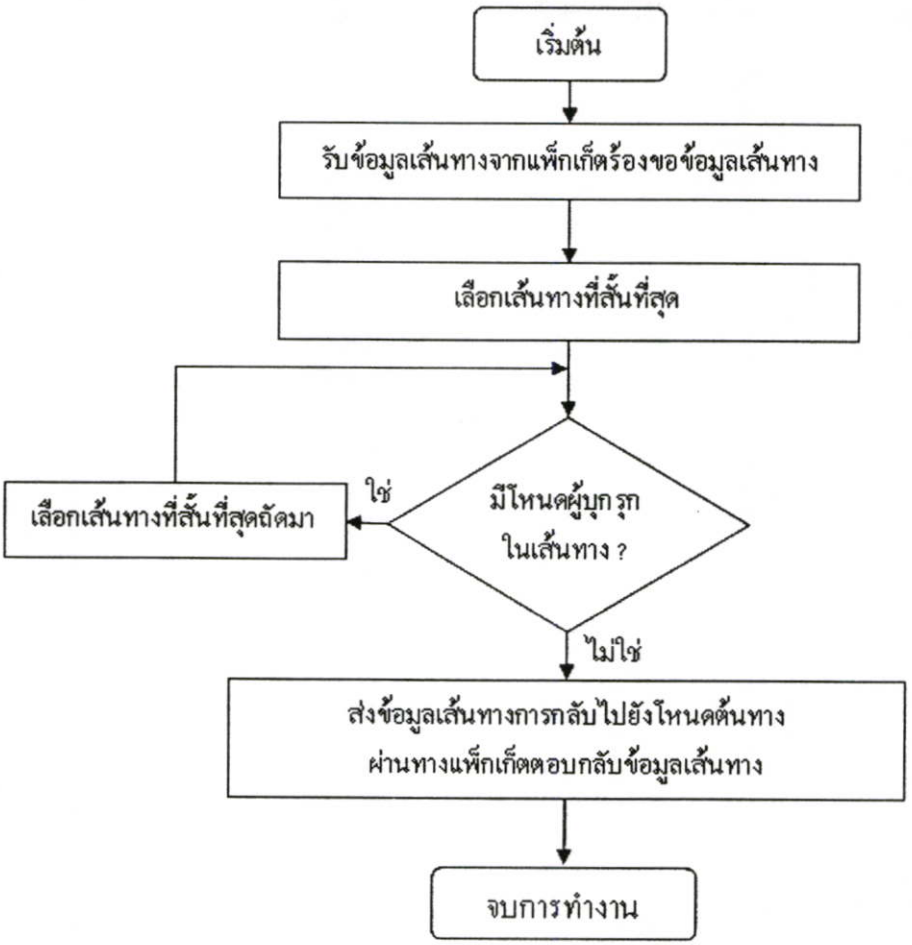
เมื่อโมไบล์เอเจนต์ที่ทำหน้าที่ตัดสินสภาพการเป็นผู้บุกรุก ได้รับข้อมูลพฤติกรรมความผิดปกติของโหนดต้องสงสัยจากโมไบล์เอเจนต์ตัวอื่นผ่านทางกระบวนการแลกเปลี่ยนข้อมูลแล้ว จะนำข้อมูลที่ได้ทั้งหมดมาคำนวณหาความถี่พฤติกรรมผิดปกติสะสม (Fr) ซึ่งแสดงได้ดังนี้

$$Fr = \frac{M}{t}$$

โดย M คือจำนวนครั้งการเกิดพฤติกรรมการนำส่งข้อมูลที่ผิดปกติ และ t คือคาบเวลาที่ใช้พิจารณาความถี่พฤติกรรมผิดปกติสะสมของโหนดต้องสงสัยจะถูกนำมาเปรียบเทียบกับค่าเทรชโฮลด์ ซึ่งถือเป็นค่าความผิดปกติสูงสุดที่ยอมรับได้บนเครือข่าย หากความถี่ของการเกิดพฤติกรรมผิดปกติมีค่าสูงกว่าค่าเทรชโฮลด์จะถือว่าโหนดดังกล่าวมีสภาพเป็นผู้บุกรุก และชื่อของโหนดที่มีสภาพเป็นผู้บุกรุกจะถูกรายงานไปยังโหนดทุกตัวในเครือข่าย เพื่อนำไปใช้เป็นข้อมูลในการหาเส้นทางที่เหมาะสมของกระบวนการค้นหาเส้นทางการสื่อสารต่อไป

4.4.3.5 การค้นหาเส้นทางโดยพิจารณาจากสภาพการเป็นผู้บุกรุก

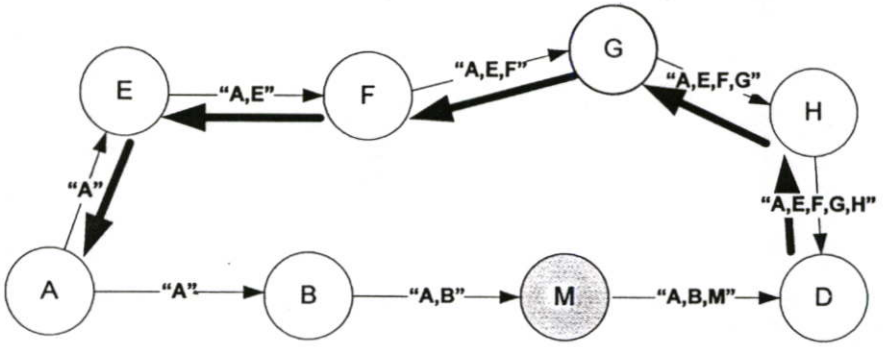
โดยมาตรฐานของโปรโตคอลค้นหาเส้นทาง DSR นั้น ทำงานอยู่บนพื้นฐานของการค้นหาเส้นทางทางที่สั้นที่สุดเป็นหลัก เมื่อโปรโตคอลค้นหาเส้นทางต้องทำงานร่วมกับระบบตรวจจับความผิดปกติของโหนดสื่อสาร แนวทางการทำงานร่วมกันคือนำผลการตรวจจับที่ได้ไปมาตัวแปรสำหรับการค้นหาเส้นทาง ในงานวิจัยนี้ได้เสนอการค้นหาเส้นทางโดยหลีกเลี่ยงเส้นทางที่พบโหนดที่ถูกตัดสินว่ามีสภาพเป็นผู้บุกรุก การทำงานดังกล่าวจะอยู่ในขั้นตอนการส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทางของโหนดปลายทาง ซึ่งมีการทำงานดังนี้



รูปที่ 4.16 การหาเส้นทางการสื่อสารโดยพิจารณาจากสภาพการเป็นผู้บุกรุก

จากขั้นตอนดังรูป 4.16 จะพบว่าเส้นทางที่ได้จากกระบวนการค้นหาอาจไม่ใช่เส้นทางที่สั้นที่สุด แต่ถือเป็นเส้นทางที่มีความเสี่ยงต่ำที่จะถูกโจมตีจากผู้บุกรุก อย่างไรก็ตามเส้นทางที่ถูกเลือกจากขั้นตอนนี้อาจถูกโจมตีจากผู้บุกรุกได้ เนื่องจากในเส้นทางอาจมีโหนดผู้บุกรุกอยู่แต่ความถี่ของพฤติกรรมความผิดปกติของโหนดยังไม่มากพอที่จะถูกตัดสินให้มีสภาพเป็นผู้บุกรุกนั่นเอง

สำหรับกรณีที่ไม่พบเส้นทางที่ปราศจากผู้บุกรุกเลย โหนดปลายทางจะไม่ทำการส่งแพ็กเก็ตตอบกลับข้อมูลเส้นทางกลับไปยังโหนดต้นทาง เพราะถือว่าเส้นทางการสื่อสารที่ค้นหาได้ไม่สามารถนำส่งข้อมูลได้แน่นอน หากโหนดต้นทางยังคงต้องการส่งข้อมูลจำเป็นต้องรอให้สภาพเครือข่ายมีการเปลี่ยนแปลงจากการเคลื่อนที่ของโหนด เพื่อให้พบเส้นทางที่สามารถนำส่งได้โดยไม่โดนโจมตี ตัวอย่างการทำงานของโปรโตคอลค้นหาเส้นทาง DSR ที่มีการพิจารณาเส้นทางจากสภาพการเป็นผู้บุรุกแสดงดังรูปที่ 4.17



แพ็กเก็ตร้องขอข้อมูลเส้นทาง

แพ็กเก็ตตอบกลับข้อมูลเส้นทาง

Misbehavior node Status	
B	Normal
M	Attacker
E	Normal
G	Normal

รูปที่ 4.17 การค้นหาเส้นทางเมื่อพิจารณาเส้นทางจากสภาพการเป็นผู้บุกรุกของ

บทที่ 5
การประเมินประสิทธิภาพของระบบระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติแบบลดทิ้งข้อมูล

5.1 บทนำ

ระบบตรวจจับความผิดปกติบนเครือข่ายไร้สายแบบแอดฮอค มีทั้งความยากและประเด็นการศึกษาที่แตกต่างจากระบบตรวจจับความผิดปกติบนเครือข่ายแบบสายอย่างชัดเจน ในระบบเครือข่ายแบบสายนั้นกระบวนการเฝ้าฟังสามารถทำได้ง่ายและมีความครบถ้วนของข้อมูลสูง เนื่องจากมีการรวมจุดเพื่อกระจายข้อมูลทั้งในการส่งและรับเพียงจุดเดียว แต่ในระบบเครือข่ายไร้สายแบบแอดฮอคนั้นข้อมูลจะถูกกระจายไปในแต่ละพื้นที่ตามตำแหน่งที่โหนดนั้นทำงานอยู่ รูปแบบและวิธีการเฝ้าฟังจึงส่งผลอย่างมากต่อความครบถ้วนของข้อมูลที่ได้รับ

ระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติที่นำเสนอในงานวิจัยนี้ มุ่งประเด็นไปที่การศึกษาและพัฒนาโครงสร้างพื้นฐานของระบบตรวจจับ โดยเฉพาะการเฝ้าฟังและการแลกเปลี่ยนข้อมูล การประเมินประสิทธิภาพของการทำงานจึงเน้นที่ความถูกต้องของข้อมูลที่ได้จากการเฝ้าฟังเป็นหลัก โดยการทดลองทั้งหมดจะอยู่บนเงื่อนไขและสภาพแวดล้อมที่ใกล้เคียงกับการทดลองบนระบบตรวจจับแบบวอชด็อกซ์ เนื่องจากเป็นระบบตรวจจับที่มีการอ้างอิงจากหลายงานวิจัย

5.2 มาตรวัดประสิทธิภาพของระบบตรวจจับความผิดปกติ

ในหัวข้อนี้จะกล่าวถึงวิธีการประเมินความสามารถในการทำงานของระบบตรวจจับความผิดปกติ ในด้านความถูกต้องและผิดพลาดของผลเฝ้าฟังซึ่งเป็นมาตรวัดที่สำคัญต่อความถูกต้องในการทำงานของ และมาตรการวัดภาระของเครือข่ายที่เพิ่มขึ้นเมื่อมีการใช้ระบบตรวจจับความผิดปกติ

5.2.1 ความถูกต้องและความผิดพลาดในการเฝ้าฟังแบบ True Positive

ความถูกต้องในการตรวจจับและความผิดพลาดแบบ True Positive [27] ถือเป็นส่วนกลับกัน ความถูกต้องในการตรวจจับ คืออัตราส่วนความผิดปกติที่ตรวจจับเมื่อเทียบกับความผิดปกติที่เกิดขึ้นทั้งหมด และความผิดพลาดแบบ True Positive คืออัตราส่วนความผิดปกติที่ตรวจจับไม่ได้เทียบกับความผิดปกติที่เกิดขึ้นทั้งหมด แสดงได้ดังนี้

$$D = \frac{M}{N} \qquad (5.1)$$

$$K = \frac{N - M}{N} \qquad (5.2)$$

จากสมการที่ 5.1 D คือความถูกต้องในการตรวจจับ, M คือจำนวนความผิดปกติที่ระบบตรวจจับสามารถตรวจจับได้ และ N คือจำนวนความผิดปกติที่เกิดขึ้นทั้งหมด สำหรับสมการที่ 5.2 K หรือความผิดพลาดแบบ True Positive คือจำนวนความผิดปกติที่ไม่สามารถตรวจจับได้ เมื่อเทียบกับจำนวนครั้งความผิดปกติที่เกิดขึ้นทั้งหมด

นัยสำคัญของความผิดพลาดแบบ True Positive คือค่าความสามารถที่แสดงให้เห็นว่าระบบตรวจจับตรวจพบความผิดปกติได้อย่างถูกต้องเท่าใดเมื่อเทียบกับความผิดปกติทั้งหมด ซึ่งระบบตรวจจับที่ดีจะต้องมีความผิดพลาดแบบ True Positive ที่ต่ำ

5.2.2 ความผิดพลาดในการเฝ้าฟังแบบ False Positive

ความผิดพลาดในการเฝ้าฟังแบบ False Positive เป็นมาตรวัดที่สำคัญอย่างยิ่งสำหรับทั้งการตรวจจับการโจมตีแบบ Abnormally และในระบบตรวจจับที่กระบวนการเฝ้าฟังมีผลต่อความถูกต้องของข้อมูล เพราะเป็นความผิดพลาดที่ระบบตรวจจับระบุว่าโหนดมีพฤติกรรมการนำส่งข้อมูลที่ผิดปกติแต่ในความเป็นจริงโหนดไม่ได้มีพฤติกรรมผิดปกติ แต่การเฝ้าฟังหรือการตัดสินสภาพโหนดมีความผิดพลาด ความผิดพลาดในการตรวจจับประเภทนี้มีผลอย่างมากต่อความน่าเชื่อถือของระบบ เพราะมีผลทำให้โหนดที่ไม่ได้มีพฤติกรรมผิดปกติไม่สามารถใช้งานเครือข่ายได้ การประเมินความผิดพลาดในการตรวจจับแบบ False Positive แสดงได้ดังนี้

$$L = \frac{F}{T} \qquad (5.3)$$

จากสมการที่ 5.3 L คือความผิดพลาดในการตรวจจับแบบ False Positive, F คือจำนวนความผิดพลาดจากการเฝ้าฟังและตัดสินว่าโหนดมีพฤติกรรมการนำส่งข้อมูลที่ผิดปกติ และ T คือจำนวนการตรวจจับทั้งหมด สำหรับการประเมินความผิดพลาดแบบ False Positive ในวิทยานิพนธ์นี้ ได้ทำการประเมินหลังจากผ่านกระบวนการยืนยันข้อมูลความผิดปกติแล้ว

5.2.3 อัตราส่วนการนำส่งข้อมูล (Packet Delivery Ratio)

นัยสำคัญของอัตราส่วนการนำส่งข้อมูลเปรียบได้กับประสิทธิภาพของเครือข่าย ที่แสดงถึงความสามารถในการนำส่งข้อมูลจากต้นทางไปยังปลายทางได้โดยไม่มีความเสียหาย [34] โดยคำนวณได้จาก

$$\mathrm{Pf} = \frac{PS}{PR} \qquad (5.4)$$

จากสมการที่ 5.4 *Pf* คืออัตราส่วนการนำส่งข้อมูลหรือประสิทธิภาพของเครือข่าย, *PS* คือจำนวนข้อมูลที่มีการนำส่ง และ *PR* หรือจำนวนข้อมูลที่โหนดปลายทางได้รับ

5.2.4 โอเวอร์เฮดของระบบตรวจจับ

โอเวอร์เฮดหรือปริมาณข้อมูลที่เพิ่มสูงขึ้นในเครือข่ายเมื่อมีการใช้งานระบบตรวจจับ โดยทั่วไปมีสาเหตุจากกระบวนการแลกเปลี่ยนข้อมูลและรายงานผลระหว่างโมไบล์เอเจนต์ การประเมินโอเวอร์เฮดที่เพิ่มขึ้นสามารถคำนวณได้จาก

$$\mathrm{OH} = \frac{Pkt' - Pkt}{Pkt} * 100\% \qquad (5.5)$$

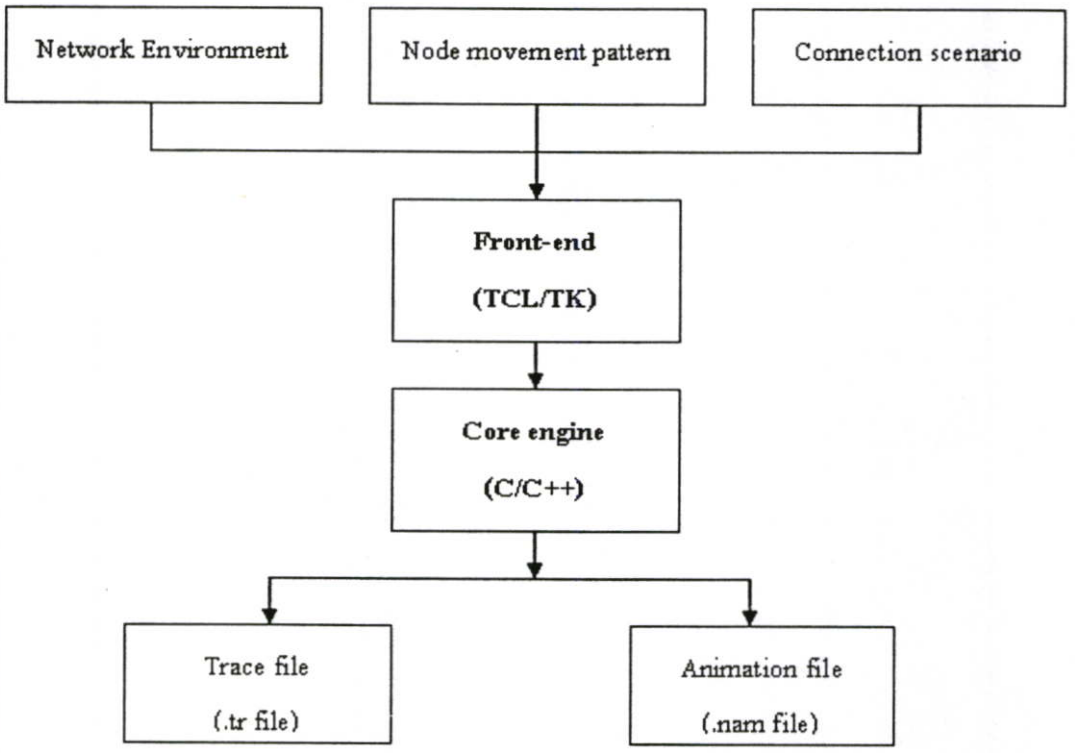
จากสมการที่ 5.5 *OH* คือโอเวอร์เฮดที่เพิ่มขึ้นในเครือข่าย *Pkt'* คือปริมาณข้อมูลในเครือข่ายเมื่อใช้งานระบบตรวจจับ และ *Pkt* คือปริมาณข้อมูลในเครือข่ายเมื่อไม่มีการใช้งานระบบตรวจจับ

5.3 การทดสอบระบบตรวจจับความผิดปกติ

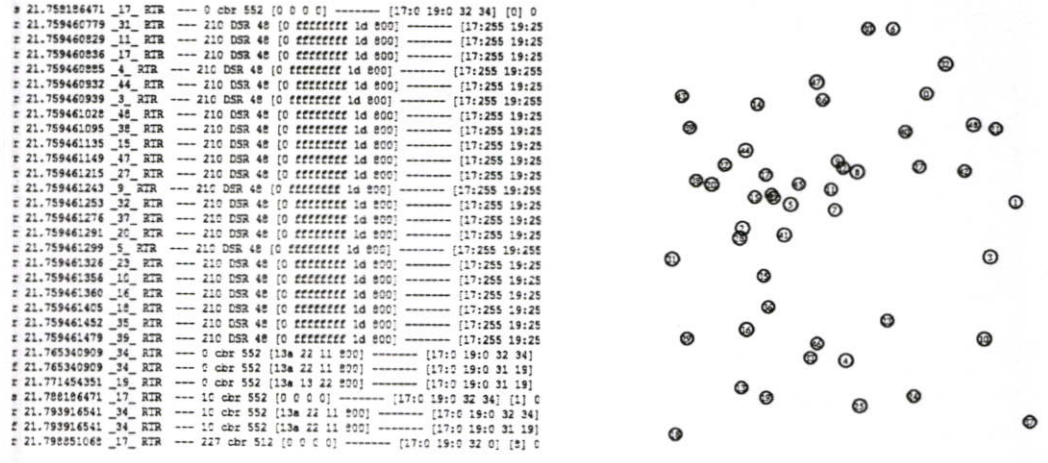
ในหัวข้อนี้จะเป็นการการทดสอบประสิทธิภาพการทำงานของระบบตรวจจับที่นำเสนอในวิทยานิพนธ์นี้ การทดลองทั้งหมดได้ใช้การจำลองสภาพแวดล้อมเครือข่ายที่ชื่อว่า Network Simulation NS-2 [31] ที่ได้รับการพัฒนาโดยมหาวิทยาลัย University of California-Berkely โปรแกรม NS-2 ได้รับความนิยมและยอมรับว่ามีความสามารถในการจำลองสภาพเครือข่ายได้ใกล้เคียงความจริง และเปิดโอกาสให้นักวิจัยได้พัฒนาและเพิ่มเติมความสามารถการทำงานของโหนดหรือเครือข่ายได้เอง

โครงสร้างภายในของ NS-2 [32] จะเป็นการทำงานร่วมกับระหว่างฟรอนเอนด์ที่พัฒนาจากภาษา TCL/TK สำหรับติดต่อกับผู้ใช้เพื่อทำการกำหนดสภาพแวดล้อมของเครือข่ายและรูปแบบการสื่อสาร และเอนจินหลักที่พัฒนาจากภาษา C/C++ สำหรับประมวลผลการทำงานทั้งหมด ผลที่ได้จากการทำงานของโปรแกรม NS-2 จะอยู่ในรูปข้อความในไฟล์เทรซ (Trace file) ที่จะแสดงพฤติกรรมการทำงานของโหนดในเวลาต่างๆ ซึ่งนักวิจัยจะใช้ข้อมูลในไฟล์ดังกล่าวเป็นหลัก นอกจากนี้โปรแกรม NS-2 ยังสามารถทำงานร่วมกับโปรแกรม NAM [32] เพื่อสร้างการแสดงผล

ในแบบกราฟิกได้อีกด้วย ขั้นตอนการทำงานของโปรแกรม NS-2 และผลที่ได้จากการทดลอง แสดงดังรูปที่ 5.1 และ 5.2 ตามลำดับ



รูปที่ 5.1 ขั้นตอนการทำงานของโปรแกรม NS-2



รูปที่ 5.2 ผลที่ได้หลังจากการทดลองผ่านโปรแกรม NS-2 จะอยู่ในรูปแบบข้อความและภาพ

5.3.1 การกำหนดสภาพแวดล้อมของเครือข่าย

การทดลองในวิทยานิพนธ์นี้จะใช้สภาพแวดล้อมเครือข่ายเดียวกันกับที่ทดลองในงานวิจัยระบบตรวจจับแบบวอชด็อกเพื่อให้ผลการทดลองสามารถเปรียบเทียบกันได้โดยยุติธรรม เหตุผลที่ใช้ระบบตรวจจับแบบวอชด็อกเป็นตัวเปรียบเทียบเนื่องจากเป็นงานวิจัยที่ได้การยอมรับและถือเป็นต้นแบบของการวิจัยระบบตรวจจับความผิดปกติบนเครือข่ายไร้สายแบบแอดฮอค

ในการทดลองได้มีการกำหนดสภาพแวดล้อมของเครือข่าย มีรายละเอียดดังนี้

- พื้นที่ของเครือข่ายถูกกำหนดให้มี 3 ขนาดคือ 670 * 670 ตารางเมตร
  - 670 * 670 ตารางเมตร
  - 1500 * 1500 ตารางเมตร
  - 2500 * 2500 ตารางเมตร
- มีจำนวนโหนดสื่อสารในเครือข่าย 50 โหนด
- มีจำนวนผู้บุกรุกไม่เกิน 40% ของโหนดทั้งหมด
- โหนดทั้งหมดที่ไม่ได้เป็นผู้บุกรุกจะมีหน้าที่เป็นโมไบล์เอเจนต์ โดยมีสมมติฐานว่าโหนดดังกล่าวไม่มีพฤติกรรมผิดปกติใดๆ
- โหนดมีลักษณะการเคลื่อนที่แบบ Random Way Point Model [33]
- โหนดมีความเร็วในการเคลื่อนที่ตั้งแต่ 0 ถึง 20 เมตรต่อวินาที และมีการสุ่มความเร็วในการเคลื่อนที่แต่ละครั้งแบบ Uniform Distribution Model [33]
- โหนดมีรัศมีการนำส่งข้อมูล 250 เมตร
- มีการใช้เสาอากาศแบบไม่มีทิศทาง (Omni-directional Antenna)
- ประเภทข้อมูลที่ใช้ทดสอบเป็นแบบ CBR (Constant bit rate) มีขนาดของข้อมูล 512 ไบต์ต่อแพ็กเก็ต แบ่งช่วงแบนด์วิดธ์ในการทดลองเป็น 4 ช่วงคือ
  - 2 กิโลไบต์ต่อวินาที
  - 20 กิโลไบต์ต่อวินาที
  - 100 กิโลไบต์ต่อวินาที
  - 500 กิโลไบต์ต่อวินาที

  การเชื่อมต่อมีจำนวนทั้งสิ้น 10 การเชื่อมต่อดังนี้
  - โหนดต้นทาง 4 โหนดรับผิดชอบการส่งข้อมูล 2 การเชื่อมต่อ
  - โหนดต้นทาง2 โหนดรับผิดชอบการส่งข้อมูล 1 การเชื่อมต่อ
  - มีโหนดปลายทางจำนวน 10 โหนดรับข้อมูลโหนดละ 1 การเชื่อมต่อ

- ความล่าช้า (Delay time) สำหรับการส่งข้อมูลแพ็กเก็ตแรกหลังจากกระบวนการค้นหาเส้นทาง และในการส่งแต่ละแพ็กเก็ต มีค่าไม่เกิน 10 วินาที [29]
- เทรชโฮลด์ในการตัดสินสภาพการเป็นผู้บุกรุกคือ 10 แพ็กเก็ต [29] โดยมีสมมติฐานว่าสภาพเครือข่ายที่กำหนดมีอัตราการความผิดพลาดในการนำส่งดีที่สุดคือไม่เกิน 5% ที่พื้นที่เครือข่าย 670 * 670 ตารางเมตร และแบนวิดธ์ 2 กิโลไบต์ต่อวินาที
- รูปแบบการโจมตีมีทั้งลดทิ้งข้อมูลเป็นแบบผู้บุกรุกโหนดเดียว และแบบร่วมกระทำโดยผู้บุกรุกทุกตัวมีฐานข้อมูลแสดงรายชื่อผู้บุรุกทั้งหมดอยู่ก่อนแล้ว
- กำหนดช่วงเวลาการหยุดรอการส่งครั้งต่อไป (Pause time) ไม่เกิน 1 วินาที
- เวลาที่ใช้ในการทดสอบไม่เกิน 800 วินาที

การกำหนดพารามิเตอร์ในการใช้งานโปรโตคอล DSR ของโปรแกรม NS-2 เพื่อให้มีการทำงานใกล้เคียงกับสภาพการใช้งานจริงและเหมาะสมกับการทดลอง ได้มีการกำหนดพารามิเตอร์ที่เกี่ยวข้องทั้งหมดดังนี้

- dsragent_snoop_source_routes กำหนดเพื่อให้กระบวนการส่งแพ็กเก็ตตอบกลับเส้นทางทำการส่งข้อมูลเส้นทางที่ถูกเลือกใช้เพียงเส้นทางเดียว
- dsragent_reply_only_to_first_rtreq เป็นพารามิเตอร์ที่ต้องกำหนดร่วมกับ dsragent_snoop_source_routes เพื่อให้ส่งข้อมูลเส้นทางที่ถูกเลือกใช้เพียงเส้นทางเดียว
- dsragent_use_tap กำหนดให้อินเตอร์เฟสที่ทำงานในระดับชั้นดาตาลิงค์มีการทำงานแบบโพรมิสคิวอัส เพื่อให้การเฝ้าฟังสามารถทำได้แม้ข้อมูลปลายทางไม่ได้ถูกกำหนดชื่อผู้รับเป็นโหนดผู้เฝ้าฟัง
- dsragent_reply_from_cache_on_propagating กำหนดให้ไม่มีการใช้แคชเพื่อบันทึกเส้นทางการสื่อสารสำหรับโหนดที่ไม่ได้ร้องขอเส้นทางเอง เพื่อกำหนดให้โหนดต้นทางต้องทำกระบวนการค้นหาเส้นทางการสื่อสารเองทุกครั้งเมื่อต้องการนำส่งข้อมูล

5.3.2 ผลการทดลอง

ในการทดลองส่วนนี้จะเป็นการเปรียบเทียบกับระบบตรวจจับแบบวอทช์ด็อก ผลที่ได้เกิดจากการจำลองรูปแบบการเคลื่อนที่ของโหนด 30 รูปแบบเพื่อนำมาหาค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน (Standard Derivation: SD) โดยจำนวนผู้บุกรุมีการกำหนดตั้งแต่ 5% ถึง 40% ของจำนวนโหนดทั้งหมดบนพื้นที่เครือข่ายที่แตกต่างกัน 3 รูปแบบมีแบนด์วิดธ์ที่แตกต่างกันทั้งหมด 4 ช่วง

ตารางที่ 5.1 แสดงความผิดพลาดแบบ True Positive

อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	1.40	0.28	0.21	0.04	0.30	0.06
10%	4.90	0.88	1.50	0.27	1.70	0.31
15%	6.80	1.02	1.60	0.24	1.90	0.29
20%	11.10	1.44	1.90	0.25	2.30	0.30
25%	19.10	2.48	2.60	0.34	3.30	0.43
30%	25.50	3.57	3.10	0.43	4.20	0.59
35%	34.70	2.78	3.50	0.28	4.70	0.38
40%	41.00	3.69	4.50	0.41	5.40	0.49
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	3.20	0.64	1.10	0.22	0.30	0.06
10%	6.40	1.34	2.00	0.42	1.70	0.36
15%	10.30	1.83	2.80	0.50	1.90	0.34
20%	14.20	2.17	3.20	0.49	3.20	0.49
25%	20.60	3.23	4.60	0.72	4.00	0.63
30%	30.30	4.67	6.20	0.95	5.00	0.77
35%	37.80	4.54	6.90	0.83	6.20	0.74
40%	44.20	4.33	9.20	0.90	7.60	0.74
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	3.90	1.09	2.70	0.76	1.10	0.76
10%	6.00	1.44	3.90	0.94	1.80	0.94
15%	10.70	2.02	5.70	1.08	2.30	1.08
20%	13.50	2.48	6.60	1.21	2.70	1.21
25%	21.00	3.49	8.20	1.36	4.30	1.36
30%	32.40	5.41	10.30	1.72	5.50	1.72
35%	39.70	5.32	12.80	1.72	6.80	1.72
40%	47.50	5.80	17.60	2.15	8.70	2.15

ตารางที่ 5.1 (ต่อ)

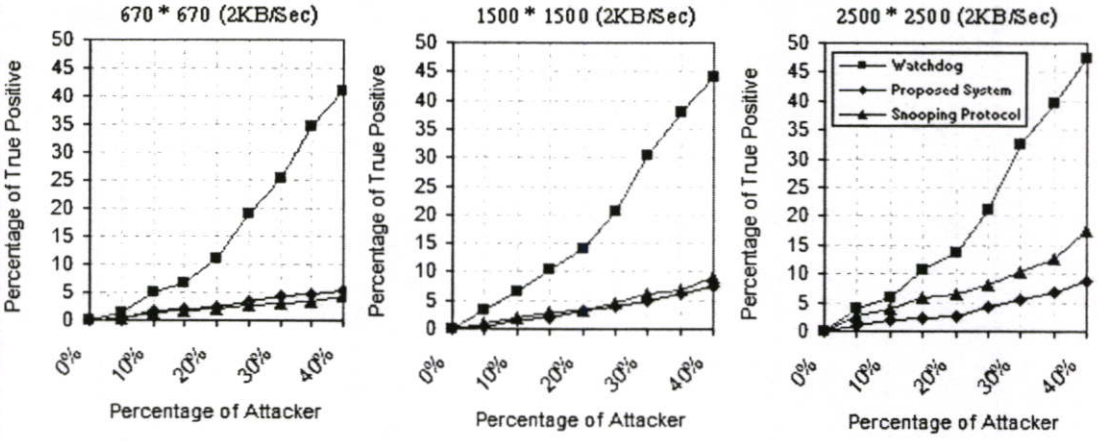
อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 20 KB/Sec						
0%	0.00	0.25	0.00	0.00	0.00	0.00
5%	1.40	0.66	0.19	0.03	0.28	0.05
10%	4.10	0.84	1.45	0.23	1.65	0.26
15%	6.00	1.10	1.55	0.22	1.88	0.26
20%	10.00	1.78	1.92	0.21	2.31	0.25
25%	17.80	2.42	2.54	0.25	3.25	0.33
30%	24.20	3.20	3.12	0.31	4.21	0.42
35%	32.00	3.63	3.28	0.33	4.35	0.44
40%	36.30	0.25	4.35	0.44	4.89	0.49
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 20 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	3.15	0.60	1.25	0.24	0.31	0.06
10%	6.50	1.11	2.10	0.36	1.69	0.29
15%	8.60	1.38	2.88	0.46	1.84	0.29
20%	13.50	1.62	3.33	0.40	2.80	0.34
25%	18.60	2.05	3.98	0.44	4.10	0.45
30%	24.60	2.71	5.89	0.65	5.25	0.58
35%	32.80	3.28	6.88	0.69	5.70	0.57
40%	39.10	3.91	9.01	0.90	6.30	0.63
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 20 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	3.76	0.79	1.35	0.28	0.56	0.12
10%	6.65	1.20	2.55	0.46	1.76	0.32
15%	11.11	2.00	3.20	0.58	2.11	0.38
20%	15.80	2.53	4.80	0.77	2.82	0.45
25%	21.22	3.18	5.60	0.84	4.25	0.64
30%	28.50	4.13	6.88	1.00	6.20	0.90
35%	34.60	5.02	8.45	1.23	6.35	0.92
40%	42.10	5.05	12.65	1.52	6.97	0.84

ตารางที่ 5.1 (ต่อ)

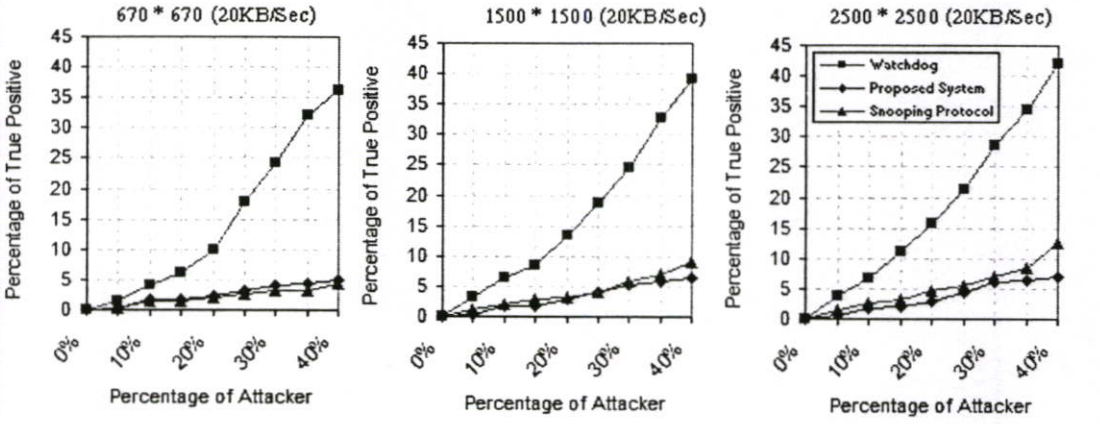
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 100 KB/Sec						
อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
0%	0.00	0.25	0.00	0.00	0.00	0.00
5%	1.35	0.20	1.19	0.18	0.26	0.04
10%	3.87	0.50	1.42	0.18	1.59	0.21
15%	5.80	0.75	1.49	0.19	1.90	0.25
20%	9.80	1.18	1.87	0.22	2.25	0.27
25%	16.40	1.64	2.34	0.23	3.14	0.31
30%	23.47	1.88	3.25	0.26	4.30	0.34
35%	27.65	2.21	3.17	0.25	4.15	0.33
40%	32.57	2.54	4.00	0.31	4.77	0.37
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 100 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	1.42	0.23	1.10	0.18	0.31	0.05
10%	3.90	0.53	1.68	0.23	1.78	0.24
15%	6.10	0.84	2.24	0.31	2.11	0.29
20%	10.50	1.30	2.80	0.35	2.38	0.30
25%	15.40	1.69	3.50	0.39	3.34	0.37
30%	22.80	2.28	4.60	0.46	4.35	0.44
35%	27.77	3.05	6.40	0.70	4.46	0.49
40%	33.20	3.25	8.90	0.87	6.24	0.61
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 100 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	1.98	0.35	1.25	0.22	0.42	0.07
10%	4.20	0.58	2.20	0.31	1.98	0.28
15%	5.89	0.84	2.84	0.40	2.45	0.35
20%	10.50	1.34	4.20	0.54	2.66	0.34
25%	14.99	1.89	4.30	0.54	3.45	0.43
30%	22.78	2.51	5.55	0.61	4.65	0.51
35%	29.48	3.24	7.45	0.82	4.89	0.54
40%	35.40	3.54	10.59	1.06	6.54	0.65

ตารางที่ 5.1 (ต่อ)

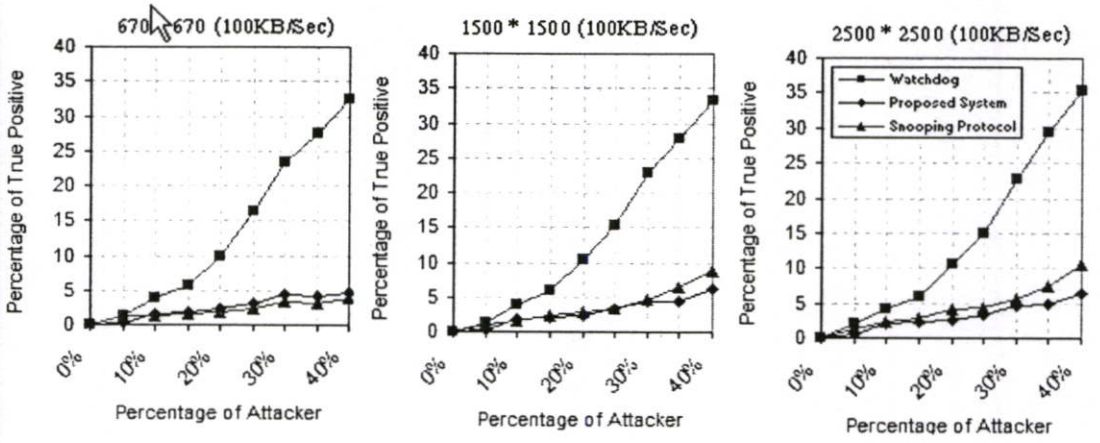
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 500 KB/Sec						
อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
0%	0.00	0.25	0.00	0.00	0.00	0.00
5%	1.29	0.17	1.18	0.15	0.26	0.03
10%	3.70	0.41	1.33	0.15	1.59	0.17
15%	5.48	0.60	1.45	0.16	1.90	0.21
20%	9.60	1.06	1.95	0.21	2.25	0.25
25%	15.45	1.51	2.33	0.23	3.14	0.31
30%	21.90	1.75	3.27	0.26	4.30	0.34
35%	24.65	1.97	3.25	0.26	4.15	0.33
40%	30.10	2.35	4.02	0.31	4.77	0.37
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 500 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	1.38	0.20	1.07	0.16	0.29	0.04
10%	3.84	0.47	1.64	0.20	1.65	0.20
15%	6.00	0.74	2.18	0.27	2.01	0.25
20%	9.40	1.05	2.60	0.29	2.20	0.25
25%	16.00	1.76	3.25	0.36	3.28	0.36
30%	20.90	2.30	4.14	0.46	4.24	0.47
35%	24.50	2.18	4.80	0.43	4.29	0.38
40%	32.10	2.09	5.90	0.38	5.80	0.38
พื้นที่เครือข่าย 2500 * /500 ตารางเมตร แบนวิดธ์ 500 KB/Sec						
0%	0.00	0.00	0.00	0.00	0.00	0.00
5%	1.88	0.29	1.23	0.19	0.34	0.05
10%	3.98	0.57	1.78	0.25	1.75	0.25
15%	6.10	0.79	2.78	0.36	2.22	0.29
20%	9.70	1.26	3.90	0.51	2.40	0.31
25%	16.10	1.96	4.70	0.57	3.39	0.41
30%	20.17	2.44	5.27	0.64	4.12	0.50
35%	24.68	2.47	6.89	0.69	4.57	0.46
40%	33.10	3.97	8.78	1.05	5.98	0.72



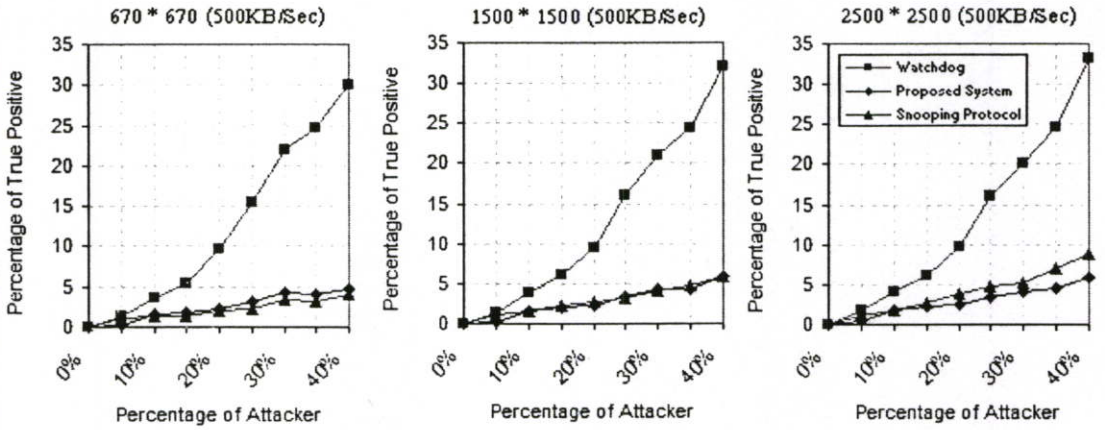
รูปที่ 5.3 กราฟความผิดพลาดแบบ True Positive เมื่อใช้แบนด์วิดธ์ 2 กิโลไบต์ต่อวินาที



รูปที่ 5.4 กราฟความผิดพลาดแบบ True Positive เมื่อใช้แบนด์วิดธ์ 20 กิโลไบต์ต่อวินาที



รูปที่ 5.5 กราฟความผิดพลาดแบบ True Positive เมื่อใช้แบนด์วิดธ์ 100 กิโลไบต์ต่อวินาที



รูปที่ 5.6 กราฟความผิดพลาดแบบ True Positive เมื่อใช้แบนด์วิดธ์ 500 กิโลไบต์ต่อวินาที

จากผลการทดลองพบว่าระบบตรวจจับแบบ Snooping Protocol และระบบตรวจจับที่นำเสนอมีจุดเด่นที่แตกต่างกันอย่างชัดเจน โดยระบบตรวจจับแบบ Snooping Protocol จะทำงานได้ดีบนเครือข่ายที่มีพื้นที่ไม่กว้างมากนัก ซึ่งโหนดเฝ้าฟังยังคงเก็บข้อมูลการสื่อสารได้ครบถ้วน แต่เมื่อพื้นที่กว้างมากขึ้น (ในการทดลองคือ 2500 * 2500 ตารางเมตร) ทำให้การเฝ้าฟังแบบ Snooping Protocol ลดประสิทธิภาพลง เนื่องจากไม่สามารถเก็บข้อมูลได้อย่างครบถ้วน

สำหรับระบบตรวจจับที่นำเสนอ พบว่ายังคงประสิทธิภาพในการตรวจจับได้อย่างคงที่แม้พื้นที่เครือข่ายจะกว้างมากขึ้น อันเนื่องมากจากการเฝ้าฟังที่อาศัยเพียงโหนดเดียวก็เพียงพอต่อตรวจสอบพฤติกรรมการสื่อสาร

ในเครือข่ายที่มีการเพิ่มแบนด์วิดธ์ที่สูงขึ้น พบว่ามีส่วนช่วยให้ความสามารถในการตรวจจับถูกต้องมากขึ้นเล็กน้อย อันเนื่องจากรูปแบบการทำงานของระบบตรวจจับทั้งหมดเป็นแบบพาสซีฟ (Passive monitoring) ที่ต้องอาศัยการนำส่งข้อมูลปกติบนเครือข่าย ทำให้เครือข่ายที่มีปริมาณการนำส่งข้อมูลกระจายกันอย่างหนาแน่นจะช่วยให้การตรวจจับทำได้รวดเร็วและมีความถูกต้องสูงกว่าเครือข่ายที่มีความหนาแน่นของการนำส่งข้อมูลน้อย

ตารางที่ 5.2 แสดงความผิดพลาดแบบ False Positive

อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	16.80	3.36	9.50	1.90	1.29	0.26
5%	16.83	3.37	9.80	1.96	1.52	0.30
10%	17.21	3.10	10.60	1.91	1.50	0.27
15%	17.49	2.62	10.00	1.50	1.80	0.27
20%	17.49	2.27	10.90	1.42	1.83	0.24
25%	17.95	2.33	10.50	1.37	1.80	0.23
30%	18.40	2.58	10.70	1.50	1.75	0.25
35%	18.00	1.44	11.60	0.93	2.05	0.16
40%	18.73	1.69	12.40	1.12	2.00	0.18
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	17.20	3.78	13.79	3.03	2.47	0.54
5%	17.20	3.61	14.00	2.94	2.47	0.52
10%	17.60	3.70	14.25	2.99	2.65	0.56
15%	18.00	2.88	13.88	2.22	3.47	0.56
20%	18.08	2.89	14.40	2.30	3.29	0.53
25%	18.45	2.84	14.98	2.31	3.60	0.55
30%	18.63	2.79	14.61	2.19	3.29	0.49
35%	18.72	2.25	14.70	1.76	3.38	0.41
40%	19.00	2.09	15.71	1.73	4.75	0.52
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	19.40	4.75	18.80	4.61	3.40	0.83
5%	19.70	4.73	18.40	4.42	3.80	0.91
10%	21.50	4.95	18.80	4.32	4.50	1.04
15%	22.10	4.86	19.00	4.18	4.80	1.06
20%	22.80	5.02	18.80	4.14	5.50	1.21
25%	24.00	4.80	18.40	3.68	6.00	1.20
30%	24.00	4.32	19.50	3.51	5.70	1.03
35%	23.60	4.46	20.00	3.78	5.60	1.06
40%	24.50	4.17	20.20	3.43	6.50	1.11

ตารางที่ 5.2 (ต่อ)

อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	16.80	3.36	9.50	1.90	1.29	0.26
5%	16.83	3.37	9.80	1.96	1.52	0.30
10%	17.21	3.10	10.60	1.91	1.50	0.27
15%	17.49	2.62	10.00	1.50	1.80	0.27
20%	17.49	2.27	10.90	1.42	1.83	0.24
25%	17.95	2.33	10.50	1.37	1.80	0.23
30%	18.40	2.58	10.70	1.50	1.75	0.25
35%	18.00	1.44	11.60	0.93	2.05	0.16
40%	18.73	1.69	12.40	1.12	2.00	0.18
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	17.20	3.78	13.79	3.03	2.47	0.54
5%	17.20	3.61	14.00	2.94	2.47	0.52
10%	17.60	3.70	14.25	2.99	2.65	0.56
15%	18.00	2.88	13.88	2.22	3.47	0.56
20%	18.08	2.89	14.40	2.30	3.29	0.53
25%	18.45	2.84	14.98	2.31	3.60	0.55
30%	18.63	2.79	14.61	2.19	3.29	0.49
35%	18.72	2.25	14.70	1.76	3.38	0.41
40%	19.00	2.09	15.71	1.73	4.75	0.52
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 2 KB/Sec						
0%	19.40	4.75	18.80	4.61	3.40	0.83
5%	19.70	4.73	18.40	4.42	3.80	0.91
10%	21.50	4.95	18.80	4.32	4.50	1.04
15%	22.10	4.86	19.00	4.18	4.80	1.06
20%	22.80	5.02	18.80	4.14	5.50	1.21
25%	24.00	4.80	18.40	3.68	6.00	1.20
30%	24.00	4.32	19.50	3.51	5.70	1.03
35%	23.60	4.46	20.00	3.78	5.60	1.06
40%	24.50	4.17	20.20	3.43	6.50	1.11

ตารางที่ 5.2 (ต่อ)

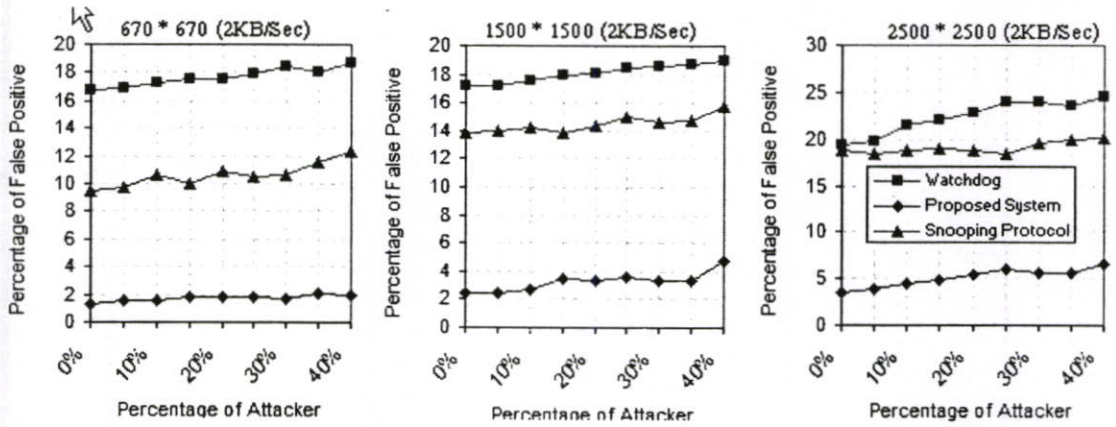
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 20 KB/Sec						
อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
0%	17.01	3.06	9.86	0.40	2.24	0.40
5%	17.10	3.08	9.80	0.36	2.00	0.36
10%	17.60	2.99	9.95	0.40	2.35	0.40
15%	17.74	2.48	10.68	0.33	2.35	0.33
20%	17.65	2.12	10.32	0.30	2.53	0.30
25%	18.28	2.19	11.13	0.30	2.53	0.30
30%	18.64	2.42	11.60	0.26	2.00	0.26
35%	18.64	1.86	11.95	0.25	2.53	0.25
40%	18.19	1.46	12.58	0.22	2.80	0.22
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 20 KB/Sec						
0%	17.39	3.48	13.40	2.68	3.00	0.60
5%	17.60	3.34	14.30	2.72	3.30	0.63
10%	17.93	3.41	14.90	2.83	3.60	0.68
15%	18.40	2.76	14.80	2.22	3.70	0.56
20%	19.01	3.04	15.20	2.43	3.90	0.62
25%	19.20	2.88	15.80	2.37	3.80	0.57
30%	19.50	2.54	15.50	2.02	3.00	0.39
35%	19.60	2.35	15.20	1.82	4.30	0.52
40%	20.30	2.23	14.80	1.63	5.70	0.63
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 20 KB/Sec						
0%	21.10	4.64	17.80	3.92	3.40	0.75
5%	21.40	4.49	19.10	4.01	3.80	0.80
10%	22.20	4.66	19.80	4.16	4.50	0.95
15%	23.30	3.96	18.30	3.11	4.80	0.82
20%	24.80	4.22	20.00	3.40	5.50	0.94
25%	24.10	3.62	19.60	2.94	6.00	0.90
30%	25.20	3.78	20.40	3.06	5.70	0.86
35%	25.00	3.50	21.40	3.00	5.60	0.78
40%	24.50	2.94	21.40	2.57	6.50	0.78

ตารางที่ 5.2 (ต่อ)

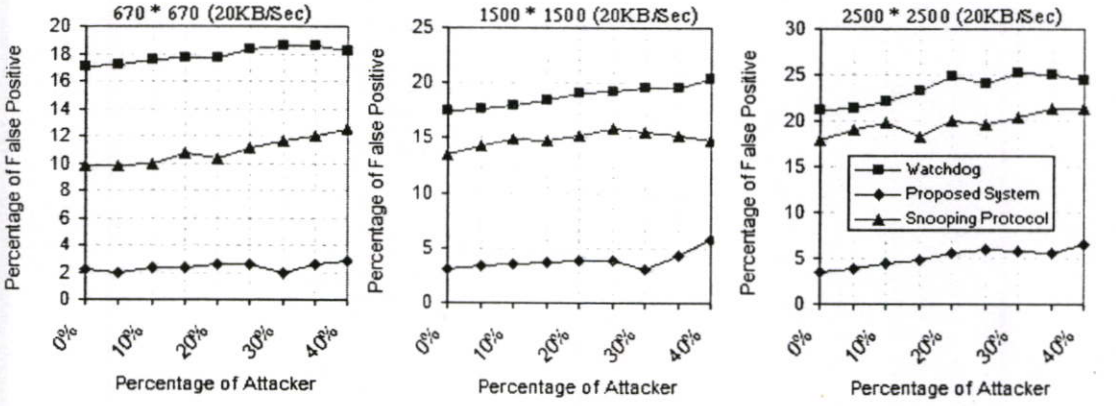
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 100 KB/Sec						
อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
0%	17.50	2.80	11.56	1.85	4.50	0.72
5%	17.77	2.84	12.87	2.06	4.10	0.66
10%	18.21	2.73	11.50	1.73	3.90	0.59
15%	18.40	2.76	12.20	1.83	3.70	0.56
20%	18.57	2.23	12.80	1.54	3.70	0.44
25%	18.21	2.19	13.10	1.57	3.20	0.38
30%	19.20	2.11	12.30	1.35	2.90	0.32
35%	19.60	2.16	13.20	1.45	3.30	0.36
40%	19.50	1.56	12.40	0.99	3.20	0.26
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 100 KB/Sec						
0%	18.80	3.38	15.10	2.72	5.20	0.94
5%	19.30	3.47	15.70	2.83	5.00	0.90
10%	18.90	3.02	15.30	2.45	4.90	0.78
15%	19.20	3.07	16.20	2.59	4.80	0.77
20%	20.40	2.47	16.70	2.02	3.99	0.48
25%	21.20	2.57	15.00	1.82	4.25	0.51
30%	20.80	2.29	16.40	1.80	4.60	0.51
35%	21.30	2.56	16.40	1.97	4.60	0.55
40%	21.40	2.14	16.60	1.66	4.60	0.46
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 100 KB/Sec						
0%	23.60	5.19	22.10	4.86	4.80	1.06
5%	24.00	5.04	21.50	4.52	5.60	1.18
10%	23.40	4.68	21.60	4.32	6.20	1.24
15%	23.90	4.78	20.00	4.00	5.40	1.08
20%	24.20	4.60	21.00	3.99	5.60	1.06
25%	25.00	4.50	21.20	3.82	6.66	1.20
30%	25.90	4.66	22.20	4.00	5.78	1.04
35%	26.00	4.16	23.00	3.68	6.45	1.03
40%	25.90	4.14	22.70	3.63	7.13	1.14

ตารางที่ 5.2 (ต่อ)

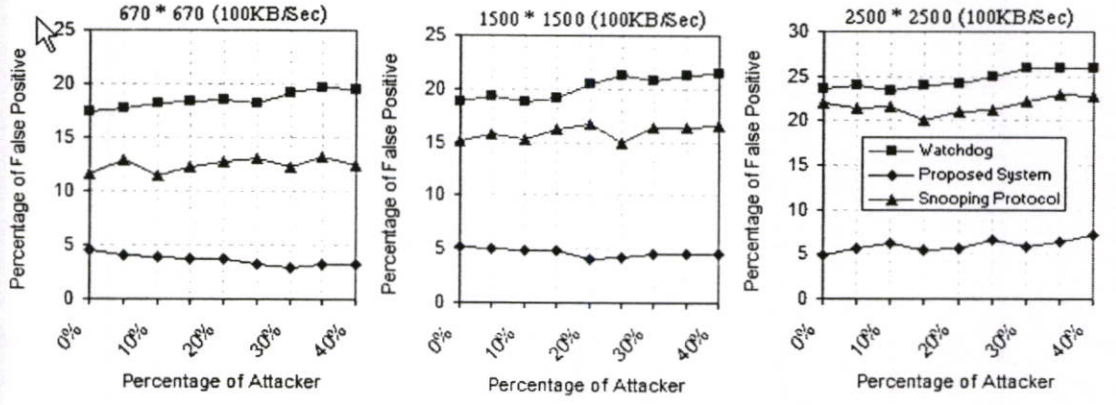
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 500 KB/Sec						
อัตราส่วนผู้บุกรุก	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
0%	18.20	2.18	12.80	1.54	4.00	0.48
5%	18.40	2.21	12.40	1.49	4.50	0.54
10%	19.00	2.09	12.40	1.36	4.40	0.48
15%	17.80	1.78	12.60	1.26	4.60	0.46
20%	18.40	1.84	12.00	1.20	4.50	0.45
25%	19.70	1.97	13.50	1.35	3.60	0.36
30%	19.90	1.99	14.00	1.40	3.60	0.36
35%	20.30	1.62	13.20	1.06	4.00	0.32
40%	20.30	1.62	12.40	0.99	4.20	0.34
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 500 KB/Sec						
0%	20.00	2.80	17.50	2.45	6.40	0.90
5%	20.00	2.80	17.10	2.39	6.40	0.90
10%	19.40	2.52	17.50	2.28	6.30	0.82
15%	19.70	2.36	16.80	2.02	6.00	0.72
20%	19.40	2.33	17.70	2.12	5.40	0.65
25%	20.10	2.61	18.30	2.38	6.10	0.79
30%	19.70	2.96	18.00	2.70	5.70	0.86
35%	20.00	2.00	17.30	1.73	5.60	0.56
40%	20.10	2.01	18.10	1.81	5.60	0.56
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 500 KB/Sec						
0%	24.20	2.90	23.30	2.80	7.00	0.84
5%	24.00	3.84	23.20	3.71	7.70	1.23
10%	24.50	3.68	23.60	3.54	7.10	1.07
15%	24.20	3.39	23.40	3.28	7.70	1.08
20%	24.00	3.12	24.40	3.17	7.20	0.94
25%	25.50	2.81	24.00	2.64	8.60	0.95
30%	25.40	3.81	25.20	3.78	7.90	1.19
35%	26.60	3.72	24.60	3.44	8.10	1.13
40%	25.30	3.04	24.90	2.99	8.40	1.01



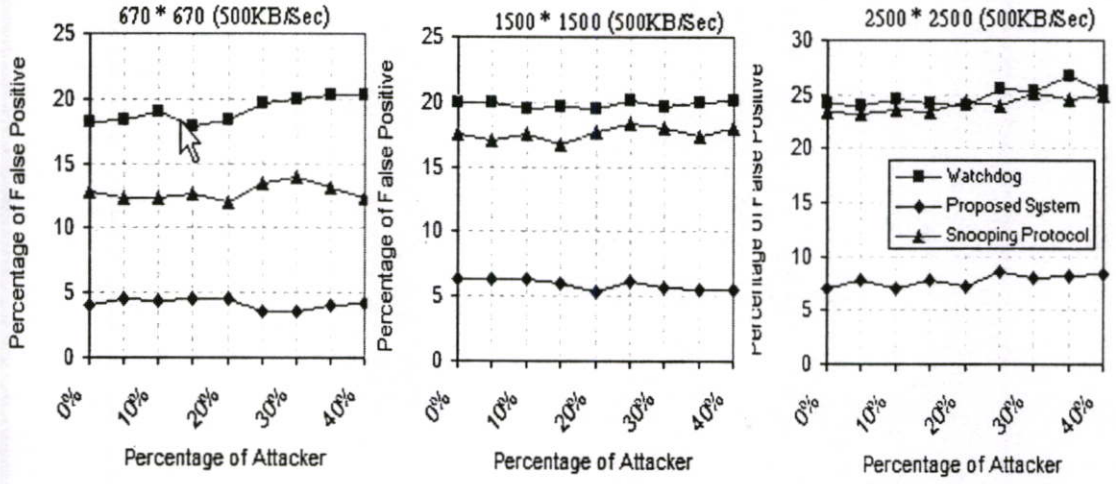
รูปที่ 5.7 กราฟความผิดพลาดแบบ False Positive เมื่อใช้แบนด์วิดธ์ 2 กิโลไบต์ต่อวินาที



รูปที่ 5.8 กราฟความผิดพลาดแบบ False Positive เมื่อใช้แบนด์วิดธ์ 20 กิโลไบต์ต่อวินาที



รูปที่ 5.8 กราฟความผิดพลาดแบบ False Positive เมื่อใช้แบนด์วิดธ์ 100 กิโลไบต์ต่อวินาที



รูปที่ 5.9 กราฟความผิดพลาดแบบ False Positive เมื่อใช้แบนด์วิดธ์ 500 กิโลไบต์ต่อวินาที

จากผลการทดลองพบว่ากระบวนการตรวจสอบและยืนยันผลการเฝ้าฟังที่ทำงานบนระบบตรวจจับที่นำเสนอได้ช่วยลดความผิดพลาดแบบ False Positive ลงได้เป็นอย่างมากเมื่อเทียบกับระบบตรวจจับแบบอื่น ปัจจัยที่มีผลต่อระดับความผิดพลาดแบบ False Positive นอกจากความเร็วในการเคลื่อนที่แล้ว จากผลการทดลองพบว่าพื้นที่การสื่อสารนับเป็นปัจจัยหนึ่งที่มีผลเช่นเดียวกัน โดยเฉพาะอย่างยิ่งระบบตรวจจับแบบ Snooping Protocol ที่มีอัตราการเพิ่มของความผิดพลาดแบบ False Positive สูงมากบนพื้นที่เครือข่ายที่กว้างที่สุด (2500 * 2500 ตารางเมตร) ซึ่งเป็นผลจากการเฝ้าฟังที่ไม่สามารถเก็บข้อมูลได้ครบถ้วนนั่นเอง

ตารางที่ 5.3 แสดงอัตราการนำส่งข้อมูล

อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 2 KB/Sec								
0%	98.78	11.85	98.73	11.72	98.32	11.23	98.30	11.62
5%	90.90	10.91	96.51	11.58	97.00	11.64	96.66	11.60
10%	87.30	10.48	95.69	11.48	96.15	11.54	96.20	11.54
15%	82.30	9.88	94.25	11.31	95.90	11.51	95.61	11.47
20%	76.40	9.93	92.89	12.08	95.00	12.35	94.87	12.33
25%	72.30	9.40	91.18	11.85	94.90	12.34	94.09	12.23
30%	66.40	9.30	88.53	12.39	94.20	13.19	93.48	13.09
35%	57.30	6.88	84.34	10.12	93.78	11.25	92.42	11.09
40%	52.30	5.23	81.40	8.14	93.54	9.35	91.02	9.10
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 2 KB/Sec								
0%	93.80	11.26	93.740	11.14	93.62	11.35	93.21	11.01
5%	88.40	10.61	93.10	18.98	92.50	11.10	91.50	10.98
10%	84.50	10.14	93.20	11.18	92.10	11.05	92.10	11.05
15%	79.50	9.54	91.10	10.93	91.10	10.93	89.40	10.73
20%	73.60	9.57	90.50	11.77	92.10	11.97	88.40	11.49
25%	69.10	8.98	88.90	11.56	92.00	11.96	87.30	11.35
30%	60.50	9.08	86.20	12.93	90.50	13.58	86.30	12.95
35%	53.20	7.98	82.90	12.44	89.50	13.43	82.40	12.36
40%	46.40	7.42	79.10	12.66	88.00	14.08	81.60	13.06
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 2 KB/Sec								
0%	88.40	10.61	88.38	10.61	88.36	10.61	88.36	10.61
5%	83.10	9.97	87.60	10.51	88.20	10.58	86.40	10.37
10%	81.00	9.72	85.45	10.25	85.10	10.21	86.20	10.34
15%	78.00	9.36	82.50	9.90	82.40	9.89	86.00	10.32
20%	73.60	9.57	79.60	10.35	79.60	10.35	85.10	11.06
25%	66.00	8.58	77.40	10.06	75.60	9.83	83.70	10.88
30%	58.40	10.51	76.00	13.68	73.80	13.28	82.00	14.76
35%	49.10	8.35	74.56	12.68	70.60	12.00	80.50	13.69
40%	36.00	6.12	71.50	12.16	66.00	11.22	78.70	13.38

ตารางที่ 5.3 (ต่อ)

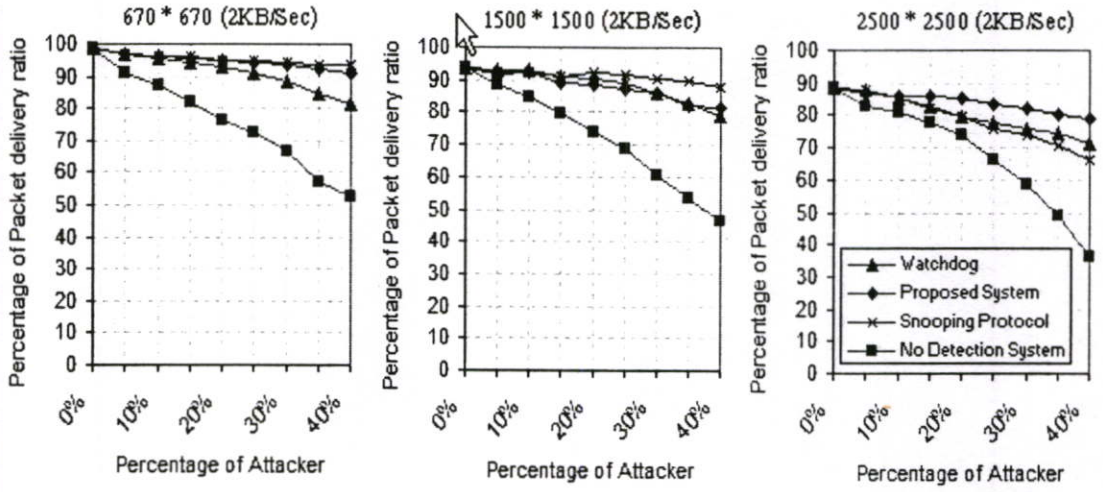
อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 20 KB/Sec								
0%	98.21	11.79	98.21	11.73	98.21	11.74	98.21	11.65
5%	89.10	10.69	95.40	11.45	96.40	11.57	95.40	11.45
10%	83.20	9.98	95.20	11.42	96.12	11.53	95.10	11.41
15%	79.50	9.54	94.00	11.28	95.10	11.41	94.54	11.34
20%	75.70	9.84	93.20	12.12	94.10	12.23	94.00	12.22
25%	70.80	9.20	90.30	11.74	93.30	12.13	93.25	12.12
30%	64.00	8.96	88.30	12.36	93.60	13.10	93.56	13.10
35%	57.30	6.88	84.30	10.12	92.50	11.10	91.40	10.97
40%	52.10	5.21	80.00	8.00	91.23	9.12	89.20	8.92
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 20 KB/Sec								
0%	91.10	10.93	91.07	10.90	91.07	10.91	90.75	10.88
5%	86.50	10.38	90.20	10.82	90.10	10.81	90.00	10.80
10%	84.00	10.08	89.50	10.74	89.60	10.75	88.60	10.63
15%	76.70	9.20	86.50	10.38	88.40	10.61	86.50	10.38
20%	71.70	9.32	85.20	11.08	89.00	11.57	86.20	11.21
25%	66.80	8.68	82.50	10.73	88.80	11.54	84.80	11.02
30%	59.20	8.88	81.20	12.18	88.00	13.20	84.30	12.65
35%	50.70	7.61	79.40	11.91	86.50	12.98	82.40	12.36
40%	45.30	7.25	76.70	12.27	85.70	13.71	80.00	12.80
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 20 KB/Sec								
0%	86.40	10.37	86.35	10.31	86.33	10.11	86.30	9.36
5%	83.10	9.97	87.25	10.47	84.00	10.08	86.20	10.34
10%	79.00	9.48	85.12	10.21	82.30	9.88	84.50	10.14
15%	76.80	9.22	82.00	9.84	81.40	9.77	84.80	10.18
20%	72.80	9.46	79.00	10.27	80.10	10.41	83.50	10.86
25%	64.70	8.41	76.90	10.00	76.20	9.91	81.30	10.57
30%	57.60	10.37	75.40	13.57	72.10	12.98	82.00	14.76
35%	47.30	8.04	74.30	12.63	70.00	11.90	80.50	13.69
40%	33.50	5.70	72.00	12.24	67.10	11.41	78.70	13.38

ตารางที่ 5.3 (ต่อ)

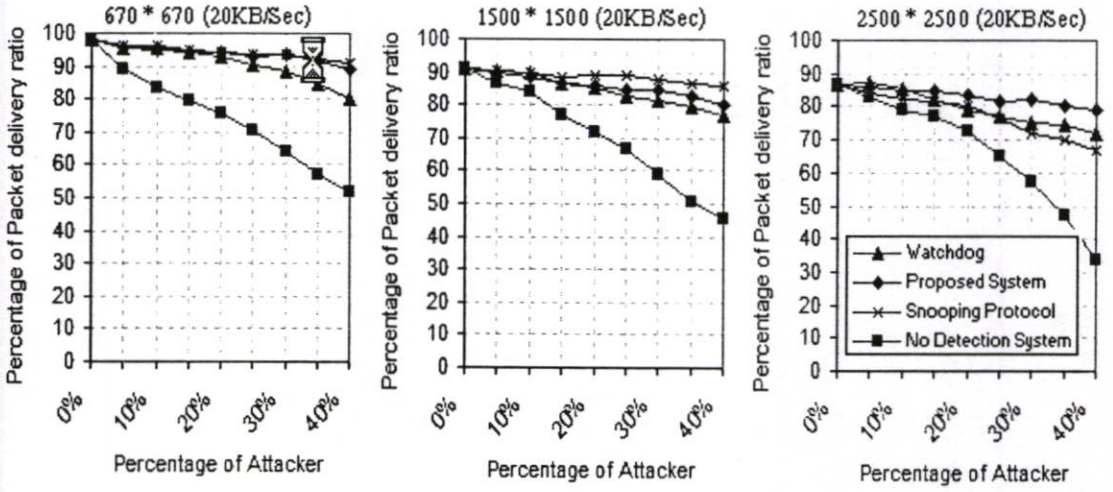
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 100 KB/Sec								
อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
0%	96.80	8.99	96.35	12.47	96.18	8.98	96.00	9.68
5%	86.00	10.32	95.20	11.42	95.90	11.51	95.10	11.41
10%	79.60	9.55	94.80	11.38	95.60	11.47	94.50	11.34
15%	73.80	8.86	93.60	11.23	94.80	11.38	93.89	11.27
20%	69.30	9.01	93.20	12.12	93.60	12.17	93.12	12.11
25%	65.30	8.49	92.10	11.97	92.70	12.05	92.10	11.97
30%	61.80	8.65	87.60	12.26	93.00	13.02	92.00	12.88
35%	55.60	6.67	84.30	10.12	91.78	11.01	89.45	10.73
40%	48.40	4.84	77.40	7.74	90.20	9.02	86.78	8.68
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 100 KB/Sec								
0%	88.70	8.65	88.55	7.60	88.48	8.97	88.41	7.65
5%	86.50	10.38	88.40	10.61	88.50	10.62	88.00	10.56
10%	84.00	10.08	88.10	10.57	88.50	10.62	87.60	10.51
15%	76.70	9.20	85.40	10.25	87.20	10.46	85.40	10.25
20%	71.70	9.32	82.30	10.70	87.60	11.39	84.00	10.92
25%	66.80	8.68	79.20	10.30	86.70	11.27	82.30	10.70
30%	59.20	8.88	78.30	11.75	85.40	12.81	82.00	12.30
35%	50.70	7.61	75.70	11.36	83.60	12.54	79.60	11.94
40%	45.30	7.25	72.40	11.58	80.10	12.82	74.60	11.94
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 100 KB/Sec								
0%	81.10	9.65	81.88	9.01	81.86	8.87	81.88	7.89
5%	75.20	9.02	81.00	9.72	79.10	9.49	80.20	9.62
10%	71.70	8.60	79.60	9.55	77.20	9.26	78.40	9.41
15%	68.60	8.23	79.20	9.50	78.00	9.36	78.30	9.40
20%	65.00	8.45	78.80	10.24	77.40	10.06	79.20	10.30
25%	58.00	7.54	77.40	10.06	74.00	9.62	78.80	10.24
30%	51.80	9.32	73.50	13.23	70.00	12.60	76.50	13.77
35%	43.40	7.38	72.00	12.24	67.30	11.44	76.00	12.92
40%	33.50	5.70	68.00	11.56	62.30	10.59	74.00	12.58

ตารางที่ 5.3 (ต่อ)

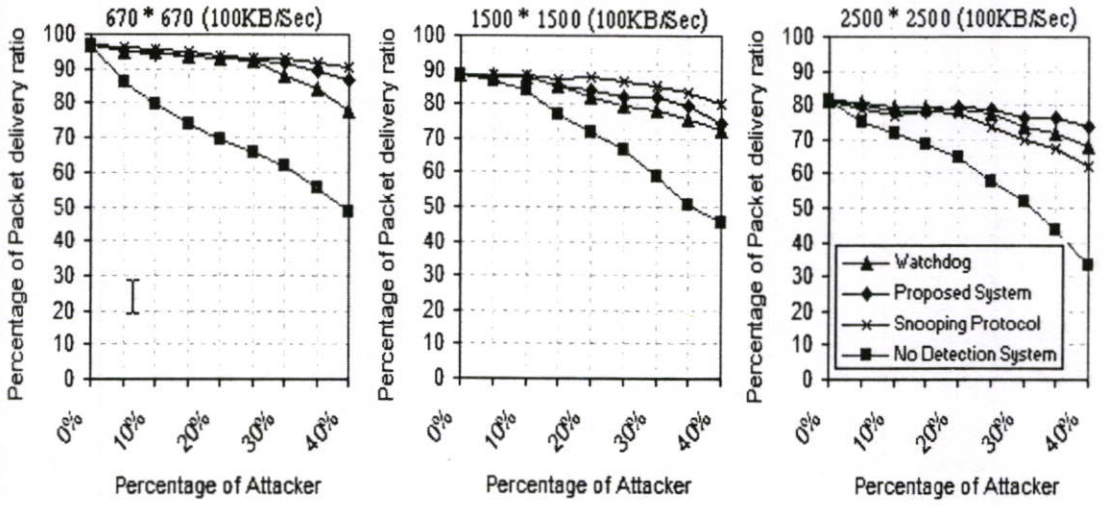
อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 500 KB/Sec								
0%	92.30	9.63	92.28	8.72	92.27	8.64	92.28	9.32
5%	85.00	10.20	89.40	10.73	90.70	10.88	88.10	10.57
10%	78.00	9.36	83.30	10.00	88.50	10.62	85.10	10.21
15%	74.40	8.93	80.00	9.60	86.00	10.32	81.50	9.78
20%	68.30	8.88	78.90	10.26	86.00	11.18	80.00	10.40
25%	61.70	8.02	76.70	9.97	83.30	10.83	79.30	10.31
30%	59.00	8.26	74.00	10.36	82.40	11.54	78.40	10.98
35%	51.50	6.18	74.00	8.88	82.00	9.84	77.50	9.30
40%	41.30	4.13	69.10	6.91	79.30	7.93	75.30	7.53
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 500 KB/Sec								
0%	82.30	8.64	82.30	8.47	82.28	9.74	82.27	8.98
5%	72.80	8.74	78.50	9.42	82.00	9.84	78.50	9.42
10%	67.50	8.10	74.60	8.95	80.30	9.64	76.00	9.12
15%	66.00	7.92	72.80	8.74	78.00	9.36	75.40	9.05
20%	63.20	8.22	72.40	9.41	79.40	10.32	74.00	9.62
25%	58.80	7.64	72.80	9.46	78.90	10.26	74.00	9.62
30%	54.00	8.10	71.50	10.73	77.20	11.58	74.60	11.19
35%	48.70	7.31	70.00	10.50	75.40	11.31	74.00	11.10
40%	41.56	6.65	69.10	11.06	75.80	12.13	72.40	11.58
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 500 KB/Sec								
0%	76.20	7.86	76.18	9.32	76.17	8.97	76.18	8.37
5%	72.50	8.70	76.00	9.12	76.00	9.12	75.80	9.10
10%	66.00	7.92	74.60	8.95	72.50	8.70	75.00	9.00
15%	63.30	7.60	71.20	8.54	71.20	8.54	74.70	8.96
20%	60.70	7.89	71.20	9.26	69.40	9.02	74.00	9.62
25%	56.30	7.32	71.20	9.26	67.20	8.74	72.90	9.48
30%	52.00	9.36	70.30	12.65	65.10	11.72	73.40	13.21
35%	45.40	7.72	68.00	11.56	64.60	10.98	72.50	12.33
40%	35.60	6.05	66.00	11.22	58.00	9.86	70.00	11.90



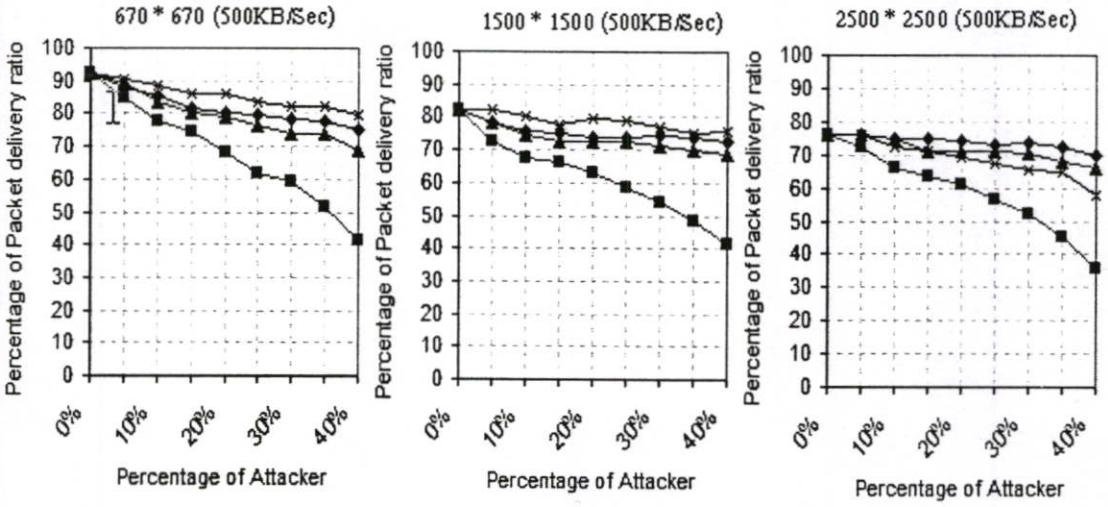
รูปที่ 5.10 กราฟอัตราการนำส่งข้อมูลเมื่อใช้แบนด์วิดธ์ 2 กิโลไบต์ต่อวินาที



รูปที่ 5.11 กราฟอัตราการนำส่งข้อมูลเมื่อใช้แบนด์วิดธ์ 20 กิโลไบต์ต่อวินาที



รูปที่ 5.12 กราฟอัตราการนำส่งข้อมูลเมื่อใช้แบนด์วิดธ์ 100 กิโลไบต์ต่อวินาที



รูปที่ 5.13 กราฟอัตราการนำส่งข้อมูลเมื่อใช้แบนด์วิดธ์ 500 กิโลไบต์ต่อวินาที

ตารางที่ 5.4 แสดงโอเวอร์เฮดจากการทำงานของระบบตรวจจับ

อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 2 KB/Sec								
0%	14.35	1.44	22.30	2.23	28.00	2.80	33.90	3.39
5%	15.10	1.51	24.21	2.42	30.30	3.03	38.70	3.87
10%	15.28	1.99	25.20	3.28	34.40	4.47	47.60	6.19
15%	15.55	2.02	26.80	3.48	37.60	4.89	56.90	7.40
20%	18.00	2.34	29.10	3.78	45.00	5.85	77.30	10.05
25%	18.80	2.44	30.30	3.94	52.00	6.76	92.30	12.00
30%	18.80	2.63	32.00	4.48	63.00	8.82	117.80	16.49
35%	20.50	2.77	35.70	4.82	70.40	9.50	136.50	18.43
40%	22.90	3.09	40.40	5.45	81.80	11.04	165.90	22.40
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 2 KB/Sec								
0%	17.10	1.88	26.10	2.87	32.10	3.53	33.90	3.73
5%	15.50	1.71	26.10	2.87	33.40	3.67	45.60	5.02
10%	17.10	2.10	28.00	3.44	36.70	4.51	55.40	6.81
15%	14.70	1.81	29.30	3.60	41.50	5.10	63.50	7.81
20%	17.10	2.26	31.00	4.09	48.00	6.34	82.30	10.86
25%	14.70	1.94	33.40	4.41	57.80	7.63	108.00	14.26
30%	17.90	2.58	35.00	5.04	70.90	10.21	137.00	19.73
35%	15.50	2.20	39.10	5.55	85.50	12.14	161.00	22.86
40%	23.50	3.36	50.50	7.22	105.90	15.14	200.00	28.60
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 2 KB/Sec								
0%	15.20	1.82	26.10	3.13	32.10	3.85	46.00	5.52
5%	16.00	1.92	28.00	3.36	36.50	4.38	53.00	6.36
10%	15.90	1.94	30.00	3.66	42.20	5.15	61.00	7.44
15%	16.00	1.95	33.20	4.05	48.60	5.93	75.00	9.15
20%	15.70	1.95	37.30	4.63	57.70	7.15	91.00	11.28
25%	15.30	1.90	38.90	4.82	72.00	8.93	109.00	13.52
30%	17.10	2.31	41.40	5.59	88.00	11.88	133.30	18.00
35%	21.90	2.96	43.00	5.81	125.20	16.90	155.00	20.93
40%	24.00	3.31	53.50	7.38	180.00	24.84	202.00	27.88

ตารางที่ 5.4 (ต่อ)

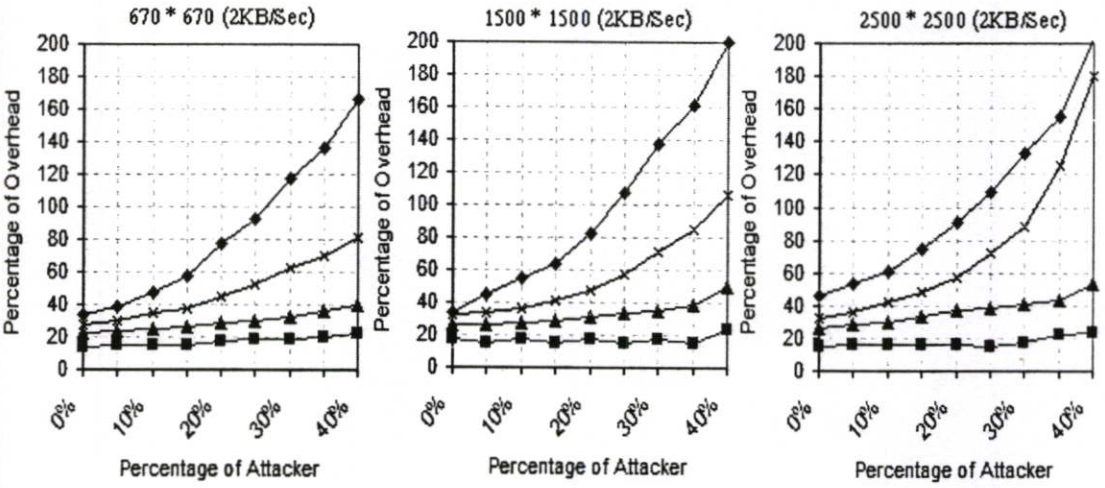
อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 20 KB/Sec								
0%	8.70	0.87	18.70	1.87	28.00	2.80	25.70	2.57
5%	9.40	0.94	17.80	1.78	30.30	3.03	30.60	3.06
10%	8.70	1.13	20.70	2.69	34.40	4.47	38.50	5.01
15%	10.80	1.40	21.70	2.82	37.60	4.89	45.10	5.86
20%	12.00	1.56	22.70	2.95	39.50	5.14	54.50	7.09
25%	12.80	1.66	21.70	2.82	44.40	5.77	61.90	8.05
30%	13.50	1.89	25.70	3.60	50.00	7.00	71.30	9.98
35%	16.00	2.16	27.60	3.73	58.20	7.86	84.80	11.45
40%	18.20	2.46	32.60	4.40	68.10	9.19	96.00	12.96
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 20 KB/Sec								
0%	10.00	1.10	18.70	2.06	32.10	3.53	33.90	3.73
5%	10.00	1.10	23.60	2.60	33.40	3.67	36.30	3.99
10%	11.80	1.45	24.60	3.03	36.70	4.51	43.20	5.31
15%	11.80	1.45	24.60	3.03	38.30	4.71	55.00	6.77
20%	11.80	1.56	25.50	3.37	43.20	5.70	68.80	9.08
25%	14.70	1.94	29.50	3.89	51.10	6.75	93.30	12.32
30%	17.90	2.58	31.40	4.52	61.90	8.91	118.80	17.11
35%	20.00	2.84	36.30	5.15	73.70	10.47	143.40	20.36
40%	28.50	4.08	45.20	6.46	87.40	12.50	166.00	23.74
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 20 KB/Sec								
0%	10.80	1.30	26.10	3.13	32.10	3.85	46.00	5.52
5%	11.70	1.40	28.00	3.36	34.20	4.10	53.00	6.36
10%	12.70	1.55	30.00	3.66	38.10	4.65	61.00	7.44
15%	16.00	1.95	33.20	4.05	44.00	5.37	75.00	9.15
20%	18.60	2.31	37.30	4.63	52.80	6.55	88.00	10.91
25%	21.50	2.67	38.90	4.82	64.50	8.00	109.00	13.52
30%	20.50	2.77	41.40	5.59	83.10	11.22	122.20	16.50
35%	24.40	3.29	43.00	5.81	114.40	15.44	140.80	19.01
40%	29.30	4.04	53.50	7.38	158.40	21.86	174.00	24.01

ตารางที่ 5.4 (ต่อ)

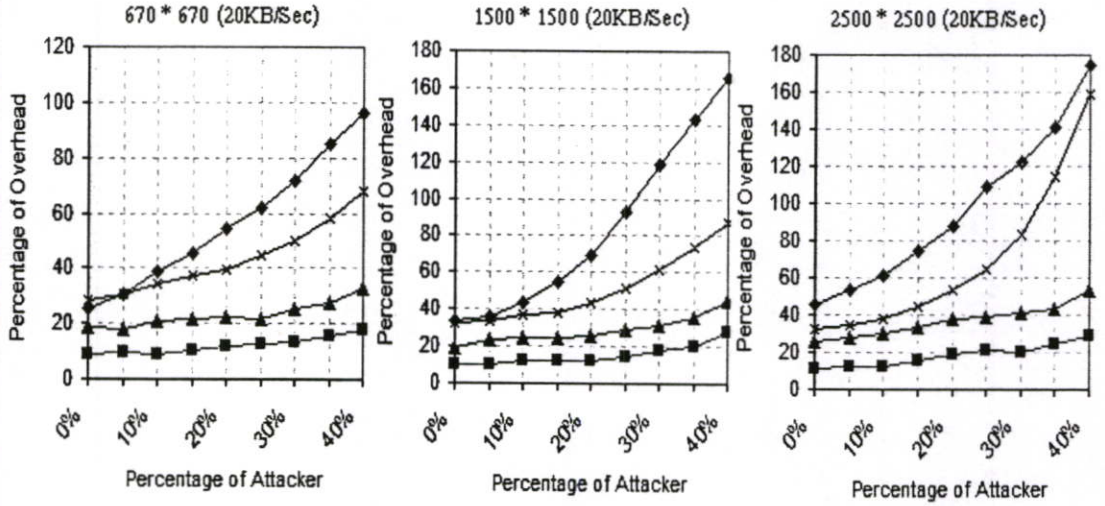
อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 100 KB/Sec								
0%	5.30	0.53	10.10	1.01	8.50	0.85	19.60	1.96
5%	5.80	0.58	11.20	1.12	13.30	1.33	21.80	2.18
10%	6.40	0.83	12.00	1.56	16.50	2.15	24.00	3.12
15%	8.00	1.04	15.40	2.00	20.00	2.60	26.50	3.45
20%	8.50	1.11	13.80	1.79	21.20	2.76	30.30	3.94
25%	11.20	1.46	16.00	2.08	25.00	3.25	37.70	4.90
30%	13.50	1.89	21.20	2.97	32.90	4.61	48.30	6.76
35%	16.00	2.16	24.40	3.29	41.40	5.59	61.60	8.32
40%	18.20	2.46	30.30	4.09	48.00	6.48	68.50	9.25
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 100 KB/Sec								
0%	5.80	0.64	18.70	2.06	26.30	2.89	30.00	3.30
5%	4.90	0.54	23.60	2.60	27.30	3.00	33.10	3.64
10%	5.80	0.71	24.60	3.03	29.20	3.59	35.00	4.31
15%	4.90	0.60	24.60	3.03	33.10	4.07	44.80	5.51
20%	7.80	1.03	25.50	3.37	38.00	5.02	62.30	8.22
25%	7.80	1.03	29.50	3.89	42.80	5.65	82.70	10.92
30%	11.70	1.68	31.40	4.52	54.50	7.85	103.20	14.86
35%	14.60	2.07	36.30	5.15	63.30	8.99	120.00	17.04
40%	18.50	2.65	45.20	6.46	71.10	10.17	131.40	18.79
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 100 KB/Sec								
0%	7.80	0.94	16.50	1.98	24.20	2.90	37.80	4.54
5%	7.80	0.94	12.60	1.51	30.00	3.60	42.60	5.11
10%	7.80	0.95	17.40	2.12	38.10	4.65	48.50	5.92
15%	10.00	1.22	22.30	2.72	41.70	5.09	55.20	6.73
20%	10.70	1.33	25.20	3.12	50.00	6.20	65.90	8.17
25%	14.50	1.80	31.00	3.84	61.10	7.58	78.90	9.78
30%	17.40	2.35	33.00	4.46	74.60	10.07	96.90	13.08
35%	21.30	2.88	37.80	5.10	100.80	13.61	123.10	16.62
40%	24.20	3.34	53.50	7.38	129.00	17.80	142.50	19.67

ตารางที่ 5.4 (ต่อ)

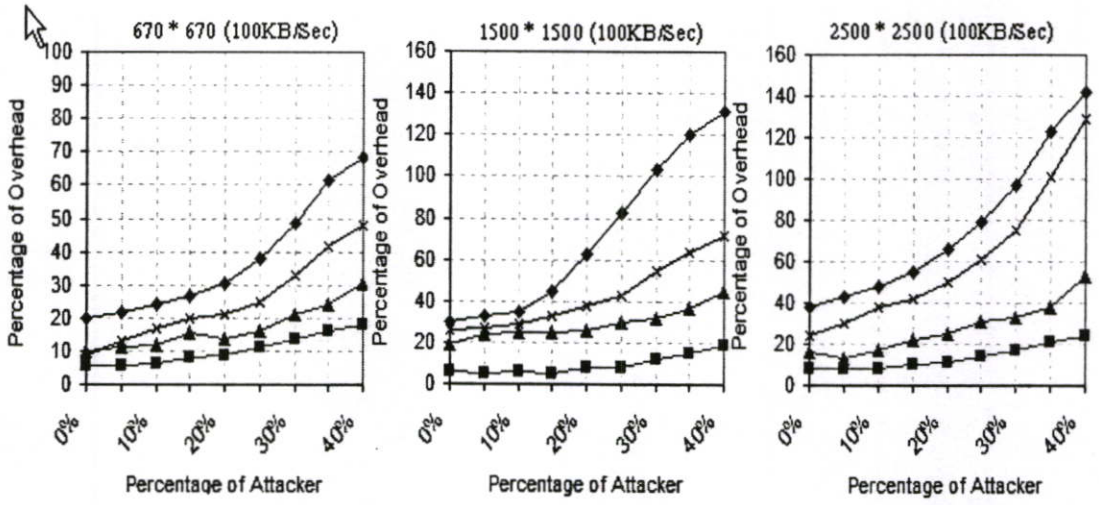
พื้นที่เครือข่าย 670 * 670 ตารางเมตร แบนวิดธ์ 500 KB/Sec								
อัตราส่วนผู้บุกรุก	No IDS	Standard Derivation	Watchdog	Standard Derivation	Snooping Protocol	Standard Derivation	Proposed System	Standard Derivation
0%	1.80	0.78	4.60	1.65	8.50	2.42	13.30	3.78
5%	2.80	0.78	4.90	1.26	7.00	3.00	14.00	4.26
10%	3.20	1.01	6.00	2.26	9.10	4.95	16.00	6.31
15%	4.60	1.30	6.70	2.90	9.80	5.42	18.00	7.18
20%	3.20	1.39	6.70	3.28	13.00	6.50	18.90	8.57
25%	4.90	1.89	8.00	4.03	15.10	7.94	22.50	10.26
30%	6.30	2.44	10.00	4.62	19.60	10.44	29.50	13.57
35%	8.00	2.88	14.40	5.10	24.00	13.61	35.40	16.62
40%	10.00	3.27	20.00	7.22	27.70	17.42	41.40	19.24
พื้นที่เครือข่าย 1500 * 1500 ตารางเมตร แบนวิดธ์ 500 KB/Sec								
0%	3.80	0.42	6.70	0.74	19.20	2.11	30.00	3.30
5%	4.90	0.54	11.50	1.27	20.00	2.20	28.80	3.17
10%	3.80	0.47	12.50	1.54	23.10	2.84	35.00	4.31
15%	4.90	0.60	14.40	1.77	26.90	3.31	41.30	5.08
20%	7.70	1.02	13.40	1.77	32.70	4.32	50.90	6.72
25%	6.70	0.88	15.40	2.03	34.60	4.57	64.40	8.50
30%	11.70	1.68	24.00	3.46	48.00	6.91	78.80	11.35
35%	10.00	1.42	30.00	4.26	54.80	7.78	85.90	12.20
40%	13.40	1.92	37.50	5.36	60.00	8.58	92.00	13.16
พื้นที่เครือข่าย 2500 * 2500 ตารางเมตร แบนวิดธ์ 500 KB/Sec								
0%	5.60	0.67	12.50	1.50	20.90	2.51	32.70	3.92
5%	4.90	0.59	12.60	1.51	31.30	3.76	34.80	4.18
10%	5.60	0.68	13.90	1.70	38.10	4.65	39.00	4.76
15%	7.70	0.94	16.70	2.04	44.50	5.43	48.00	5.86
20%	7.70	0.95	19.50	2.42	52.90	6.56	57.00	7.07
25%	9.70	1.20	22.30	2.77	64.70	8.02	68.00	8.43
30%	12.50	1.69	24.00	3.24	80.70	10.89	81.40	10.99
35%	16.00	2.16	29.90	4.04	96.00	12.96	98.80	13.34
40%	24.20	3.34	43.10	5.95	114.10	15.75	121.00	16.70



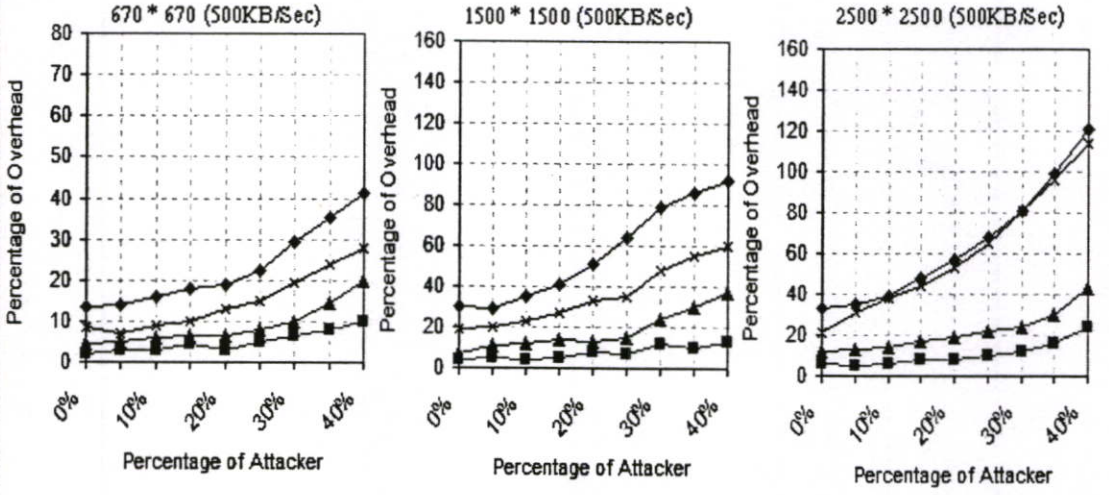
รูปที่ 5.14 กราฟโอเวอร์เฮดของระบบตรวจจับเมื่อใช้แบนด์วิดธ์ 2 กิโลไบต์ต่อวินาที



รูปที่ 5.15 กราฟโอเวอร์เฮดของระบบตรวจจับเมื่อใช้แบนด์วิดธ์ 10 กิโลไบต์ต่อวินาที



รูปที่ 5.16 กราฟโอเวอร์เฮดของระบบตรวจจับเมื่อใช้แบนด์วิดธ์ 100 กิโลไบต์ต่อวินาที



รูปที่ 5.17 กราฟโอเวอร์เฮดของระบบตรวจจับเมื่อใช้แบนด์วิดธ์ 500 กิโลไบต์ต่อวินาที

5.4 วิเคราะห์ผลการทดลอง

จากผลการทดลองระบบตรวจจับความผิดปกติแบบลดทิ้งข้อมูลโดยใช้โมไบล์เอเจนต์ ที่นำเสนอในวิทยานิพนธ์นี้ จะเห็นว่ามีความสามารถในการตรวจจับสูงกว่าการใช้ระบบตรวจจับแบบ วือชด็อกทั้งในด้านปริมาณการโจมตีที่ตรวจจับได้ และมีความผิดพลาดทั้งแบบ True Positive และ False Positive ที่น้อยลง ส่งผลให้อัตราส่วนการนำส่งข้อมูลของเครือข่ายมีค่าสูงขึ้น แต่การทำงานของระบบตรวจจับแบบโมไบล์เอเจนต์ได้ทำให้เกิดโอเวอร์เฮดแก่เครือข่ายสูงกว่าระบบตรวจจับแบบวอชด็อก เนื่องจากต้องมีการแลกเปลี่ยนข้อมูลระหว่างโมไบล์เอเจนต์ที่กระจายอยู่ทั่วไปเครือข่าย โดยอัตราการเพิ่มขึ้นของโอเวอร์เฮดจะขึ้นอยู่กับจำนวนผู้บุกรุกในเครือข่าย เนื่องจากจำนวนผู้บุกรุกจำนวนที่มากขึ้นนั้น ทำให้ระบบตรวจจับต้องทำการรายงานผลและแลกเปลี่ยนข้อมูลความผิดปกติของผู้บุกรุกดังกล่าวทุกครั้งเมื่อพฤติกรรมผิดปกติถูกตรวจจับได้

ในส่วนของการทดลองเกี่ยวกับความหนาแน่นของโหนดในเครือข่าย พบว่าจำนวนที่เพิ่มขึ้นหรือลดลงของโหนดหรือโมไบล์เอเจนต์มีผลเพียงเล็กน้อยต่อความถูกต้องในการตรวจจับ แต่มีผลอย่างมากต่อโอเวอร์เฮดของเครือข่าย เนื่องจากการแลกเปลี่ยนข้อมูลต้องทำงานร่วมกับโหนดที่มีจำนวนมากขึ้น

ในส่วนการทดลองการหาเส้นทางโดยพิจารณาจากความถี่พฤติกรรมสะสม พบว่าอัตราส่วนการนำส่งข้อมูลที่ได้สูงกว่าการพิจารณาหาเส้นทางจากค่าเทรชโฮลด์หรือสภาพความเป็นผู้บุกรุกของโหนด เนื่องจากเส้นทางที่เลือกมีความโอกาสน้อยที่จะมีผู้บุกรุกอยู่ในเส้นทาง ทำให้การนำส่งข้อมูลมีความสำเร็จสูง แต่วิธีการพิจารณาเส้นจากความถี่พฤติกรรมสะสมมักทำให้ได้เส้นทางที่มีจำนวนโหนดตัวกลางสูงกว่าปกติ

5.5 ลักษณะของโครงสร้างเครือข่ายและการโจมตีที่เป็นอุปสรรคในการตรวจจับ

เมื่อพิจารณาการทำงานและผลการทดลองของระบบตรวจจับที่นำเสนอ พบว่ามีเงื่อนไขทางเครือข่ายและรูปแบบการโจมตีบางประการที่ส่งผลให้ระบบตรวจจับไม่สามารถทำงานได้อย่างมีประสิทธิภาพ ดังนี้

1. การชนกันของข้อมูล หากเกิดขึ้นในระหว่างที่โมไบล์เอเจนต์ทำการเฝ้าฟังอยู่ จะทำให้การเฝ้าฟังไม่สามารถทำงานได้ และโดยทั่วไปแล้วเครือข่ายไร้สายแบบแอดฮอคมักมีปริมาณการชนกันของข้อมูลสูงกว่าเครือข่ายแบบอื่น [1] การชนกันของข้อมูลในเครือข่ายที่มีผลต่อการทำงานของระบบตรวจจับแบ่งเป็นสองลักษณะตามสถานะการทำงานของโมไบล์เอเจนต์ ดังนี้

- เกิดการชนกันของข้อมูลในขณะเฝ้าฟังแพ็กเก็ตตอบกลับข้อมูลเส้นทาง ส่งผลให้โมไบล์เอเจนต์จะไม่เข้าสู่สถานะเฝ้าฟังพฤติกรรมการนำส่งข้อมูล ผลที่เกิดขึ้นทำให้ความผิดพลาดแบบ True Positive สูงขึ้น
- เกิดการชนกันของข้อมูลในขณะเฝ้าฟังข้อมูล ทำให้โมไบล์เอเจนต์ตัดสินว่าโหนดต้องสงสัยมีพฤติกรรมผิดปกติในการนำส่งและรายงานไปยังโหนดปลายทางของเส้นทาง

2. เครือข่ายที่โหนดมีความเร็วในการเคลื่อนที่สูง จะมีผลต่ออัตราการนำส่งข้อมูลลดลง เนื่องจากมีปริมาณข้อมูลที่ไม่สามารถนำส่งได้สำเร็จเพิ่มสูงขึ้น เมื่อกระบวนการเฝ้าฟังที่นำเสนอทุงานในเครือข่ายดังกล่าว จะทำให้เกิดความผิดพลาดในการเฝ้าฟังแบบ False Positive ต่อโหนดสูง ส่งผลให้การตัดสินว่าโหนดมีสภาพการเป็นผู้บุกรุกทำได้ผิดพลาด

3. เครือข่ายมีปริมาณข้อมูลสำหรับนำส่งน้อย เนื่องจากการเก็บข้อมูลความผิดปกติของระบบตรวจจับเป็นลักษณะพาสซีฟ หากเครือข่ายมีปริมาณข้อมูลน้อยจะส่งผลให้ความถี่พฤติกรรมผิดปกติสะสมของต่ำไปด้วย ซึ่งจะมีผลทำให้ระบบตรวจจับไม่สามารถแยกแยะได้ว่าโหนดใดทีสภาพเป็นผู้บุกรุก

4. การปลอมแปลงและแก้ไขข้อมูลความถี่พฤติกรรมผิดปกติสะสม แม้ว่าในการทดลองได้กำหนดสมมติฐานว่าโมไบล์เอเจนต์จะต้องเป็นโหนดที่ปราศจากพฤติกรรมผิดปกติใดๆ แต่ในความเป็นจริงแล้วโมไบล์เอเจนต์อาจถูกควบคุมการทำงานจากผู้บุกรุก หรือผู้บุกรุกอาจมีความสามารถในการปลอมแปลงข้อมูลให้เหมือนกับการส่งจากโมไบล์เอเจนต์ได้ ในกรณีที่ข้อมูลความถี่พฤติกรรมผิดปกติสะสมถูกปลอมแปลงหรือแก้ไขจากผู้บุกรุก จะทำให้การตัดสินสภาพการเป็นผู้บุกรุกมีความผิดพลาด แนวทางการป้องกันในกรณีที่ผู้บุกรุกทำการปลอมแปลงข้อมูลสามารถใช้การพิสูจน์ตนจากการเข้ารหัสแบบคีย์คู่ แต่ในกรณีที่โมไบล์เอเจนต์ถูกควบคุมการทำงานจากผู้บุกรุก ระบบตรวจจับจะไม่สามารถตรวจสอบได้

5. ผู้บุกรุกมีการลดทิ้งข้อมูลแบบมีการสุ่มหรือเลือกข้อมูล เป็นรูปแบบการโจมตีได้รับการพัฒนาเพื่อควบคุมความถี่พฤติกรรมผิดปกติสะสมของตนเอง มีผลทำให้โหนดดังกล่าวไม่ถูกตัดสินสภาพการเป็นผู้บุกรุก การโจมตีรูปแบบนี้ยังไม่สามารถตรวจจับได้บนระบบตรวจจับใดที่ทำงานแบบ Abnormally detection เพราะไม่สามารถแยกแยะความเสียหายที่เกิดขึ้นได้ว่ามีสาเหตุจากการโจมตีหรือเกิดขึ้นจากการทำงานตามปกติ

บทที่ 6
สรุปการวิจัยและข้อเสนอแนะ

6.1 บทนำ

การโจมตีแบบลดทิ้งข้อมูล มีจุดประสงค์เพื่อทำให้เครือข่ายมีอัตราการนำส่งข้อมูลลดลง นอกจากจะมีผลโดยตรงต่อประสิทธิภาพของเครือข่ายแล้ว ยังทำให้ความน่าเชื่อถือของเครือข่ายต่ำลงด้วย วิทยานิพนธ์นี้ได้เสนอโครงสร้างระบบตรวจจับความผิดปกติในเครือข่ายผ่านการใช้โมไบล์เอเจนต์ โดยมีเป้าหมายเพื่อเพิ่มจำนวนโหนดที่ทำหน้าที่เฝ้าฟังการสื่อสาร ซึ่งจะช่วยให้การตรวจจับความผิดปกติของโหนดต้องสงสัยทำให้ครอบคลุมและถูกต้องมากขึ้นกว่าระบบตรวจจับที่ได้มีการนำเสนอก่อนหน้า

6.2 สรุปการวิจัย

การใช้งานโมไบล์เอเจนต์เพื่อทำการเฝ้าฟังโหนดต้องสงสัยในเครือข่าย มีจุดมุ่งหมายในการเพิ่มจำนวนโหนดเฝ้าฟังในเครือข่ายให้สามารถตรวจจับการโจมตีที่มีความซับซ้อน และการเฝ้าฟังโดยอาศัยโหนดเดียวดังเช่นวิธีการของระบบตรวจจับแบบวอชด็อกไม่ทำการตรวจจับได้ เช่น การโจมตีลดทิ้งข้อมูลแบบร่วมกระทำ เนื่องจากรูปแบบการโจมตีสามารถทำการปิดบังพฤติกรรมที่ผิดปกติจากกระบวนการเฝ้าฟังจากโหนดเพียงตัวเดียวได้ ซึ่งเมื่อทำการทดลองแล้วทำให้พบถึงข้อดีข้อเสียในหลายประเด็นที่แตกต่างกัน

เมื่อนำโมไบล์เอเจนต์จำนวนมากมาทำหน้าที่เฝ้าฟังพฤติกรรมความผิดปกติในการนำส่งข้อมูลของโหนดบนเครือข่าย ได้ส่งผลให้ความถูกต้องและจำนวนความผิดปกติที่ตรวจจับได้มีค่าสูงขึ้นเมื่อเปรียบเทียบกับการทำงานของระบบตรวจจับแบบวอชด็อก โดยเฉพาะในเครือข่ายที่มีการโจมตีแบบร่วมกระทำ อันเป็นผลจากการเฝ้าฟังแบบหลายโหนดที่ทำได้ครอบคลุมพื้นที่การสื่อสาร สำหรับความผิดพลาดในการเฝ้าฟังแบบ False Positive ที่เกิดขึ้นจากการเฝ้าฟังข้อมูลในหลายตำแหน่งได้ถูกควบคุมให้น้อยลงโดยกระบวนการยืนยันความถูกต้องของข้อมูล และเมื่อโปรโตคอลค้นหาเส้นทางได้นำสภาพการเป็นผู้บุกรุกมาพิจารณาหาเส้นทางการสื่อสาร ทำให้เส้นทางที่ได้นั้นมีความเสี่ยงที่จะถูกโจมตีลดลง ส่งผลทำให้อัตรานำส่งข้อมูลในเครือข่ายสูงขึ้น

เนื่องจากโมไบล์เอเจนต์ในเครือข่ายมีเป็นจำนวนมากและมีการเก็บข้อมูลความผิดปกติของโหนดแบบกระจาย กระบวนการแลกเปลี่ยนและรายงานข้อมูลของระบบตรวจจับจึงได้สร้างโอเวอร์เฮดให้แก่เครือข่ายในปริมาณที่ค่อนข้างสูง โดยเฉพาะอย่างยิ่งเครือข่ายที่มีปริมาณผู้บุกรุก

จำนวนมากที่ต้องมีการแลกเปลี่ยนข้อมูลอยู่บ่อยครั้ง โดยในการทดลองเกี่ยวกับหนาแน่นของโหนดในเครือข่าย ทำให้พบข้อมูลที่สำคัญอย่างหนึ่งว่าจำนวนโมไบล์เอเจนต์ที่ทำการเฝ้าฟังมีผลต่อความถูกต้องในการตรวจจับเพียงเล็กน้อยเท่านั้น แต่ในเครือข่ายที่มีโมไบล์เอเจนต์จำนวนมากได้ทำให้เกิดโอเวอร์เฮดมากขึ้นตามลำดับ ซึ่งในเครือข่ายจริงที่จะประยุกต์ใช้ระบบตรวจจับที่นำเสนอในวิทยานิพนธ์นี้จำเป็นต้องพิจารณาความคุ้มค่าในจุดนี้

การพิจารณาเส้นทางการสื่อสารจากความถี่พฤติกรรมผิดปกติสะสมของโหนดในเส้นทางมีผลทำให้อัตราส่วนการนำส่งข้อมูลของเครือข่ายสูงขึ้น เมื่อเปรียบเทียบกับวิธีการพิจารณาเส้นทางจากสภาพความผิดปกติ เนื่องจากเส้นทางที่ได้มีความเสี่ยงต่ำสุดที่จะถูกโจมตีจากผู้บุกรุก แต่วิธีการดังกล่าวมีผลทำให้ได้การนำส่งข้อมูลต้องผ่านเส้นทางที่มีจำนวนโหนดตัวกลางขึ้น ซึ่งอาจส่งผลเสียในด้านคุณภาพการให้บริการและการใช้พลังงาน

6.3 ปัญหาและอุปสรรค

ในการทดลองสำหรับงานวิจัยนี้ได้ทำบนระบบเครือข่ายแบบจำลองเท่านั้น เนื่องจากการทดลองบนระบบเครือข่ายจริงต้องใช้ทั้งจำนวนคนและค่าใช้จ่ายจำนวนมาก แม้ว่าผลที่ได้จะพบว่าระบบตรวจจับที่นำเสนอช่วยค้นหาโหนดผู้บุกรุกและเพิ่มอัตราส่วนการนำส่งข้อมูลได้จริง แต่ในการใช้งานจริงอาจมีปัจจัยเกี่ยวข้องที่ไม่สามารถพบได้ในระบบจำลอง โดยเฉพาะความแตกต่างกันของอุปกรณ์เครือข่ายที่ใช้, ความสามารถในการรับส่งสัญญาณของเสาอากาศและความแตกต่างกันของแหล่งพลังงาน ที่อาจทำให้รัศมีการนำส่งข้อมูลของแต่ละโหนดไม่เท่ากัน เมื่อนำผลที่ได้จากการทดลองมาเปรียบเทียบกับการทำงานระบบเครือข่ายจริงจึงอาจมีความแตกต่างกัน

งานวิจัยด้านความปลอดภัยบนระบบเครือข่ายไร้สายแบบแอดฮอค โดยเฉพาะการโจมตีแบบ Abnormally นั้นยังไม่เป็นที่แพร่หลายนัก การวิจัยจึงยังอยู่ในกลุ่มที่จำกัด สภาพแวดล้อมของเครือข่ายที่เป็นมาตรฐานสำหรับทำการทดลองยังไม่มีการกำหนดให้ชัดเจน สภาพแวดล้อมครือข่ายที่ใช้จึงอาศัยจากข้อมูลงานวิจัยที่มีการอ้างอิงเท่านั้น

6.4 แนวทางการพัฒนาต่อ

โอเวอร์เฮดของเครือข่ายที่เกิดจากการแลกเปลี่ยนข้อมูลระหว่างโมไบล์เอเจนต์ นับว่าเป็นประเด็นหลักที่ควรมีการศึกษาและวิจัยเพิ่มเติม ผลจากการทดลองได้แสดงให้เห็นว่าจำนวนโมไบล์เอเจนต์ที่ทำหน้าที่เฝ้าฟังไม่มีผลมากนักต่อความถูกต้องในการตรวจจับ แต่มีผลอย่างมากกับปริมาณโอเวอร์เฮดของระบบตรวจจับ การจำกัดจำนวนโมไบล์เอเจนต์เพื่อให้ลดโอเวอร์เฮดจึงเป็นแนวทางที่จะทำให้ระบบตรวจจับมีประสิทธิภาพและมีความคุ้มค่ามากขึ้น

การเก็บข้อมูลแบบกระจายเป็นอีกตัวแปรหนึ่งที่ทำให้โอเวอร์เฮดในเครือข่ายสูง จึงทำให้การเก็บข้อมูลมาแบบรวมศูนย์เป็นอีกแนวทางหนึ่งที่สามารถลดปริมาณโอเวอร์เฮดในเครือข่ายได้ แต่ในขณะเดียวกันต้องมีการศึกษาประเด็นด้านความปลอดภัยให้ด้วย เนื่องจากข้อมูลที่ถูกจัดเก็บไว้เพียงแห่งเดียวย่อมมีความเสี่ยงที่จะเสียหาย หรือโดนโจมตีแบบ Denial of Service ได้

เอกสารอ้างอิง

[1] C. Siva Ram Murthy and B.S. Manoj. 2004. "Machine Ad Hoc Wireless Networks: Architectures and Protocols." Prentice Hall.

[2] Charles E. Perkins. 2000. " Ad Hoc Networking." Addison Wesley.

[3] C.K. Toh. 2002. "The Wireless Network Evolution." Prentice Hall.

[4] Dana M. and John H. 2001. " Peer-to-Peer: Building Secure, Scalable, and Manageable Networks." McGraw-Hill.

[5] Shafinaz B. 2002. " Overview of Ad Hoc Routing Protocols." Networking and Performance Engineering Group, Informatics, Bradford University

[6] Thomas E and Ulrich S. 2004. "Highly Dynamic Destination-Sequenced Distance-Vector Routing." SECAN-Lab at the University of Luxembourg.

[7] Madhusudhan N. 2000. "How Bellman-Ford algorithm works." [Online]. Avaliable : www.laynetworks.com/Bellman20Ford%20Algorithm.htm

[8] Douglas E. Comer. 2000. "Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture (4th Edition)." Prentice Hall.

[9] Thomas E and Ulrich S. 2004. "Ad Hoc On-Demand Distance Vector Routing Protocol." SECAN-Lab at the University of Luxembourg.

[10] David B. Johnson. 1999. "The Rice University Monarch Project: Mobile Networking Architectures"

[11] David B. Johnson, David A. and Maltz Josh Broch. 1999. "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks." Computer Science Department Carnegie Mellon University.

[12] Matt Welsh. 2000. "NIST DSR Model." [Online]. Avaliable : http://www.antd.nist.gov/wctg/DSRreadme.pdf

[13] David B. Johnson, David A. Maltz and Yih-Chun Hu. 1993. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) ." IETF MANET Working Group.

[14] Andrew S. Tanenbaum. 1996. "Computer Networks." Prentice Hall.

[15] Pejman Roshan and Jonathan Leary. 2004. "802.11 Wireless LAN Fundamentals." Cisco Press

[16] Adam Burg. 2003 "Ad hoc network specific attacks" Seminar Ad hoc networking: concepts, applications, and security, Technische Universität München

[17] Bruce Schneier. 1995. "Applied Cryptography: Protocols, Algorithms, and Source Code in C". John Wiley & Sons Inc.

[18] Stuart McClure, Joel Scambray, George Kurtz. 2000. "Network Security Secrets and Solutions (Hacking Exposed)." McGraw-Hill.

[19] Yih-Chun Hu, Adrian Perrig and David B. Johnson. 2000. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" in The 8th ACM International Conference on Mobile Computing and Networking,

[20] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. 2002. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless AdHoc Networks." In Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002).

[21] William Stallings. 2002. "Cryptography and Network Security: Principles and Practice (3rd Edition)." Prentice Hall.

[22] Yih-Chun Hu, Adrian Perrig and David B. Johnson. 2003. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks.

[23] Lingxuan Hu and David Evans. 2004. "Using Directional Antennas to Prevent Wormhole Attacks." Proceedings of the Network and Distributed System Security Symposium.

[24] Stephen Northcutt, Judy Novak. 2000. "Network Intrusion Detection: An Analyst's Handbook (2nd Edition)." New Riders Publishing.

[25] Zhang, Y. and Lee, W.. 2000. "Intrusion Detection in Wireless Ad-Hoc Networks." In Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking.

[26] Zhang, Y., Lee, W. and Huang Y. A. 2003. "Intrusion detection techniques for mobile wireless networks." Wireless Networks, Volume 9 Issue 5, September 2003.

[27] Sergio Marti, T. J. Giuli, Kevin Lai and Mary Baker. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks." Mobile Computing and Networking.

[28] Chawedee Baramee, Sakchai Thipchaksurat and Ruttikorn Varakulsiripunth. 2004. "A Mechanism of Detecting Misbehavior Nodes in Ad-Hoc Wireless Networks." The Second ECTI Annual Conference (ECTI-CON-2005).

[29] Jim Parker, Jeffrey L Undercoffer, John Pinkston, and Anupam Joshi. 2004. "On Intrusion Detection and Response for Mobile Ad Hoc Networks." 23rd IEEE International Performance Computing and Communications Conference.

[30] ชาวดี บารมี, ศักดิ์ชัย ทิพย์จักษุรัตน์. 2003 "การตรวจจับโหนดที่มีพฤติกรรมผิดปกติด้วยโมไบล์เอเจนต์ ในเครือข่ายไร้สายแบบแอดฮอค" วิศวสารลาดกระบัง ฉบับที่ 4 ปีที่ 21 ธันวาคม 2547

[31] NS-2. "NS by Example." [Online]. Available : http://nile.wpi.edu/NS

[32] NS-2. "NS-2 architecture." [Online]. Available : http://nsnam.isi.edu/nsnam/index.php/Main_Page

[33] Josh Broch, David A Maltz, David B, Johnson and Yih-Chun Hu. 1998. "A performance comparison of multi-hop wireless ad hoc network routing protocols." International Conference on Mobile Computing and Networking archive Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking

[34] Mike Just and, Evangelos Kranakis and and Tao Wan. 2003. "Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks." Ad-Hoc, Mobile, and Wireless Networks, Second International Conference, ADHOC-NOW 2003

ภาคผนวก

งานวิจัยที่ได้รับการตีพิมพ์

[1] ชาวดี บารมี, ศักดิ์ชัย ทิพย์จักษุรัตน์, "การตรวจจับโหนดที่มีพฤติกรรมผิดปกติด้วยโมไบล์เอเจนต์ในเครือข่ายไร้สายแบบแอดฮอค", วิศวสารลาดกระบัง ปีที่ 21 ฉบับที่ 4, ธันวาคม 2547

[2] Chawedee Baramee, Sakchai Thipchaksurat and Ruttikorn Varakulsiripunth. "A Mechanism of Detecting Misbehavior Nodes in Ad-Hoc Wireless Networks." Proceedings of The 2005 Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI 2005) International Conference, Asia Pattaya Beach Hotel, Pattaya, Cholburi, Thailand

ISSN 0125-1724

วิศวสาร

ลาดกระบัง

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

LADKRABANG ENGINEERING JOURNAL

ปีที่ 21 ฉบับที่ 4 ธันวาคม 2547

การตรวจจับโหนดที่มีพฤติกรรมผิดปกติด้วยโมไบล์เอเจนต์ในเครือข่ายไร้สายแบบแอดฮอค

Misbehavior Node Detection with Mobile Agent in Ad Hoc Wireless Network

ชาวดี บารมี ศักดิ์ชัย ทิพย์จักมุรัตน์

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

บทคัดย่อ

งานวิจัยฉบับนี้ได้เสนอวิธีการตรวจจับโหนดที่มีพฤติกรรมผิดปกติในขณะที่มีการรับส่งข้อมูล สำหรับเครือข่ายไร้สายแบบแอดฮอคที่ใช้โปรโตคอลการสื่อสารแบบดีเอสอาร์ โดยการใช้โหนดสื่อสารที่อยู่ในเครือข่ายทำหน้าที่เป็นโมไบล์เอเจนต์คอยเฝ้าฟังข้อมูลที่มีการรับส่งบนเครือข่ายไร้สาย ซึ่งมีจุดเด่นที่ช่วยให้ระบบตรวจจับในงานวิจัยนี้สามารถตรวจสอบความผิดปกติของโหนดในพื้นที่การสื่อสารได้ครอบคลุมมากกว่าระบบตรวจจับที่เคยมีการนำเสนอ เนื่องจากโหนดสื่อสารมักมีการกระจายตัวกันอย่างทั่วถึงบนเครือข่ายอยู่แล้ว สำหรับวิธีตรวจจับพฤติกรรมความผิดปกติของโหนดสื่อสารในงานวิจัยนี้ เป็นการวิเคราะห์ความสัมพันธ์ระหว่างข้อมูลที่ถูกส่งออกมาจากโหนดสื่อสาร และข้อมูลเส้นทางการสื่อสารจากโหนดต้นทางไปยังโหนดปลายทาง ความผิดปกติของโหนดใดๆ สามารถตรวจจับหากโหนดดังกล่าวไม่มีการส่งข้อมูลออกจากตัวเองไปยังโหนดตัวถัดไปตามเส้นทางและเวลาที่กำหนด ผลที่ได้จากระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติจะช่วยให้เครือข่ายสามารถหลีกเลี่ยงการใช้โหนดดังกล่าวในแต่ละเส้นทาง ส่งผลให้เครือข่ายมีประสิทธิภาพและความน่าเชื่อถือสูงขึ้น

Abstract

This research proposes the methodology to detect misbehavior nodes in ad-hoc wireless networks that uses Dynamic Source Routing (DSR) Algorithm for communicating. Besides intermediate nodes in transmission path, other nodes are going to be the mobile agents. These agents are going to monitor the communication of data at each intermediate node. Because nodes distribute all over network space, in this way, the detection of misbehavior nodes can cover more area than other previous researches. The detection technique in our research is the analyzing on outgoing packets from intermediate node and the route path of packet. Any misbehavior nodes will be detected, if there is no packet sending out from intermediate node to the next hop in the route path and in the appropriate time. Consequently, network communications avoid using route path which has misbehavior node. Thus, the network has high efficiency and high reliability.

1. บทนำ

แนวคิดของเครือข่ายไร้สายแบบแอดฮอค คือ การสื่อสารระหว่างโหนดต้นทางและปลายทาง โดยไม่ต้องใช้อุปกรณ์กระจายสัญญาณ (แอกเซสพอยต์) ในกรณีที่โหนดต้นทางและปลายทาง ไม่สามารถสื่อสารกันได้โดยตรง (เนื่องจากอุปสรรคด้านระยะทางการสื่อสาร) โหนดที่อยู่ระหว่างต้นทางและปลายทาง จะทำหน้าที่รับและส่งต่อ (Store and Forward) แพ็กเก็ตข้อมูลเพื่อทดแทนการใช้อุปกรณ์กระจายสัญญาณ กระบวนการค้นหาเส้นทางการสื่อสาร ที่เหมาะสมต่อการสื่อสารในเครือข่ายแต่ละครั้งนั้น จะกระทำโดยโปรโตคอลค้นหาเส้นทาง (Routing Protocol) เช่น AODV[2], DSR[1] และ ZRP[3] วิธีการทำงานในแต่ละโปรโตคอลอาจแตกต่างกัน จากความต้องการที่แตกต่างกันในแต่ละสภาพแวดล้อมการสื่อสาร

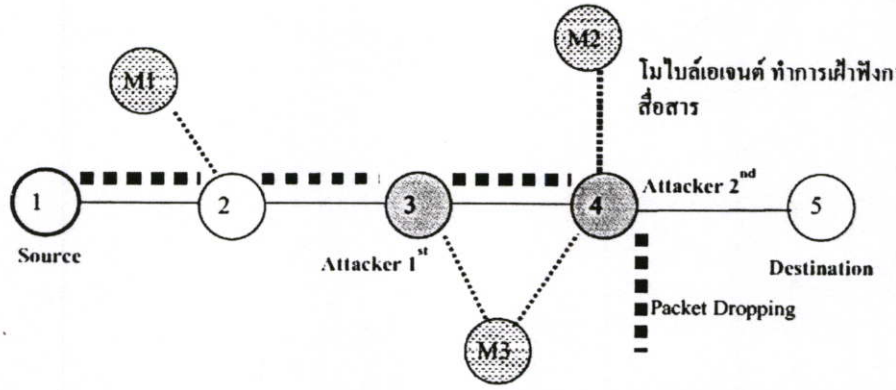
เนื่องจากเครือข่ายไร้สายแบบแอดฮอค มักจะมีโครงสร้างการสื่อสารเปลี่ยนแปลงอยู่ตลอดเวลา เมื่อโครงสร้างการสื่อสารมีการเปลี่ยนแปลง ย่อมส่งผลกระทบต่อเส้นทางการสื่อสารที่กำลังมีการใช้งานอยู่ เช่น กรณีที่โหนดในเส้นทางการสื่อสารมีการเคลื่อนที่ออกนอกรัศมีการสื่อสาร ความเสียหายลักษณะนี้เป็นสิ่งที่มีโอกาสเกิดขึ้นได้ตามปกติสำหรับเครือข่ายไร้สายแบบแอดฮอค โดยโปรโตคอลการสื่อสารจะทำหน้าที่ตรวจสอบความผิดพลาดในการสื่อสาร และทำการแก้ไขต่อไป แต่หากความเสียหายของเส้นทางการสื่อสารเกิดจากการโจมตีของผู้บุกรุกทางเครือข่าย ซึ่งมักมีรูปแบบที่ซับซ้อน ความสามารถในการตรวจสอบและแก้ไขจากโปรโตคอลการสื่อสาร อาจไม่เพียงพอที่จะควบคุมความเสียหายที่เกิดขึ้นกับระบบเครือข่ายได้

งานวิจัยนี้ได้เสนอวิธีการตรวจจับพฤติกรรมที่ผิดปกติจากการไม่นำส่งแพ็กเก็ต (Packet Dropping) โดยมีรูปแบบพฤติกรรมคือไม่มีการนำส่งแพ็กเก็ตหลังจากที่ได้รับแพ็กเก็ตนั้น (Store but not Forward) ซึ่งเกิดจากโหนดดังกล่าวเป็นผู้บุกรุกทางเครือข่าย (Network Intrusion) โดยมีโมไบล์เอเจนต์ทำการเฝ้าฟังแพ็กเก็ตข้อมูล ที่มีการรับส่งกันในเครือข่าย กระบวนการเฝ้าฟังจะเริ่มตั้งแต่โหนดสื่อสารในเส้นทางทำการส่ง "แพ็กเก็ตตอบกลับเส้นทาง" (Route Reply Packet) ข้อมูลที่บรรจุอยู่ในแพ็กเก็ตตอบกลับเส้นทาง จะช่วยให้โมไบล์เอเจนต์ทราบว่าโหนดสื่อสารที่ถูกเฝ้าฟังอยู่ จะมีการส่งแพ็กเก็ตข้อมูลไปยังโหนดใดเป็นตัวต่อไป และหากโหนดสื่อสารไม่มีการส่งแพ็กเก็ตข้อมูลออกมาภายในเวลาที่กำหนดไว้ จะถือได้ว่าโหนดสื่อสารดังกล่าว มีพฤติกรรมที่ผิดปกติไปจากข้อกำหนดในโปรโตคอลการสื่อสาร

2. งานวิจัยที่เกี่ยวข้อง

ปัจจุบันได้มีระบบตรวจจับความผิดปกติของโหนดสื่อสารในเครือข่ายไร้สายแบบแอดฮอค อยู่หลายงานวิจัย เช่น Watchdog[4] เป็นงานวิจัยแรกที่มีการนำเทคนิคเฝ้าฟัง (Sniffing) การส่งแพ็กเก็ตข้อมูลของโหนดมาเป็นส่วนประกอบสำคัญของระบบตรวจจับ แนวคิดของ Watchdog คือการให้โหนดที่ทำการส่งแพ็กเก็ตทำการเฝ้าฟังว่าโหนดผู้รับนั้น มีการส่งแพ็กเก็ตออกมาอีกครั้งหลังจากได้รับแพ็กเก็ตที่ตัวเองส่งไปให้หรือไม่ (จากกระบวนการรับและส่งต่อ) จุดอ่อนของ Watchdog คือไม่สามารถตรวจจับความผิดปกติจากการโจมตีที่มีความซับซ้อนได้ ตัวอย่างเช่นการโจมตีที่มีผู้บุกรุกทำงานร่วมกันหลายโหนด (Collusion Attack)

Snooping Protocol[5] เป็นอีกงานวิจัยที่มีการนำเทคนิคการเฝ้าฟังมาใช้ วิธีการของงานวิจัยนี้คือการเฝ้าฟังการรับแพ็กเก็ตเข้า (Inbound Packet) และการส่งแพ็กเก็ตออก (Outbound Packet) ของโหนดสื่อสาร โดยการใช้โหนดข้างเคียง (Neighbor Node) ทำหน้าที่เฝ้าฟังพฤติกรรมการรับส่งดังกล่าว การเฝ้าฟังวิธีดังกล่าวทำให้ระบบตรวจจับนี้ สามารถทำงานได้กับโปรโตคอลการสื่อสารทุกหลายแบบ แต่ความจำเป็นที่ต้องเฝ้าฟังแพ็กเก็ตทั้งเข้าและออกของโหนดสื่อสารแต่ละตัว ทำให้ไม่สามารถทำงานได้บนเครือข่ายไร้สายที่โหนดแต่ละตัวอยู่ห่างกันมากๆ ได้



รูปที่ 1 โครงสร้างเครือข่ายที่ประกอบด้วยโหนดสื่อสารและโมไบล์เอเจนต์ที่กำลังทำหน้าที่เฝ้าฟัง

จุดเด่นของงานวิจัยฉบับนี้ เมื่อเปรียบเทียบกับงานวิจัยทั้งสอง คือความสามารถตรวจจับความผิดปกติของโหนดได้ครอบคลุมพื้นที่มากขึ้น เนื่องจากโหนดสื่อสารที่เป็นโมไบล์เอเจนต์มักจะมีการกระจายตัวกันในเครือข่ายอยู่แล้ว นอกจากนี้ยังสามารถตรวจจับการโจมตีที่มีความซับซ้อนสูง เช่นการโจมตีแบบร่วมกระทำได้ เนื่องจากโหนดผู้โจมตีไม่สามารถปิดบังการเฝ้าฟังจากโมไบล์เอเจนต์ที่อยู่โดยรอบได้ทุกตัว

3. การตรวจจับโหนดที่มีพฤติกรรมผิดปกติด้วยโมไบล์เอเจนต์

รูปที่ 1 แสดงโครงสร้างของเครือข่ายไร้สายแอดฮอค ที่ประกอบด้วย เส้นทางการสื่อสารระหว่างโหนดต้นทางและปลายทาง โหนดผู้บุกรุก และโมไบล์เอเจนต์ โดยโหนดผู้บุกรุกและโมไบล์เอเจนต์มีนิยามดังนี้

- โหนดผู้บุกรุก คือโหนดสื่อสารที่มีพฤติกรรมผิดปกติ ไม่มีการรับส่งข้อมูลตามโปรโตคอลการสื่อสารที่กำหนดไว้ ซึ่งอาจเกิดจากโหนดดังกล่าวติดไวรัสคอมพิวเตอร์ หรือโปรแกรมใดๆ จากบุคคลที่ต้องการทำลายการสื่อสารของเครือข่าย
- โมไบล์เอเจนต์ คือโหนดสื่อสารที่ได้รับการติดตั้งระบบตรวจจับความผิดปกติของโหนดสื่อสาร โดยในอุดมคติแล้ว โหนดสื่อสารที่ไม่เป็นผู้บุกรุกจะเป็นโมไบล์เอนต์ทุกตัว

นอกจากโครงสร้างเครือข่ายที่เหมาะสม เพื่อให้การเฝ้าฟังทำได้ครอบคลุมเครือข่ายแล้ว โหนดสื่อสารในเครือข่ายยังต้องมีคุณสมบัติพื้นฐานดังต่อไปนี้

- โหนดมีการสื่อสารแบบ Bi-Direction[1]
- สายอากาศของอุปกรณ์มีการส่งสัญญาณแบบ Omni-Direction เพื่อให้ไม่มีข้อจำกัดการทิศทางของการรับส่ง
- อินเตอร์เฟสของโหนดทำงานแบบโพรมิสคิวอัสโหมด (Promiscuous Mode) ซึ่งเป็นการทำงานที่ไม่มีการตรวจสอบ MAC แอดเดรสของแต่ละแพ็กเก็ตที่เข้ามายังอินเตอร์เฟส
- โหนดแต่ละตัวไม่มีความแตกต่างกันในด้านพลังงาน

การทำงานของระบบตรวจจับประกอบด้วย 2 ขั้นตอน คือการเฝ้าฟังเพื่อเก็บข้อมูล และการวิเคราะห์ผลที่ได้จากการเฝ้าฟัง โดยมีการทำงานแต่ละขั้นตอนโดยละเอียดดังนี้

3.1 กระบวนการเฝ้าฟังการสื่อสาร

อินเตอร์เฟสของโมไบล์เอเจนต์ทุกตัวจะทำงานในโหมดที่เรียกว่าโพรมิสคิวอัส เพื่อทำการเฝ้าฟังทุกแพ็กเก็ตที่มีการส่งออกมาจากโหนดสื่อสาร ดังตัวอย่างรูปที่ 1 โมไบล์เอเจนต์ M2 จะสามารถทำการเฝ้าฟังโหนดหมายเลข 4 (เนื่องจากอยู่ในรัศมีการรับส่ง) โดยโมไบล์เอเจนต์จะบันทึกข้อมูลการสื่อสาร เพื่อใช้ในการวิเคราะห์ผล โดยมีเงื่อนไขและขั้นตอนดังนี้

1. โมไบล์เอเจนต์จะเลือกบันทึกข้อมูลเฉพาะแพ็กเก็ตตอบกลับเส้นทาง ที่ถูกส่งออกมาจากโหนดที่เป็นตัวกลางในการสื่อสาร ตัวอย่างเช่น หลังจากที่โหนดหมายเลข 4 ได้รับจากโหนดหมายเลข 5 แล้ว โหนดหมายเลข 4 จะมีการส่งแพ็กเก็ตตอบกลับเส้นทางไปยังโหนดหมายเลข 3 ซึ่งเอเจนต์ M2 และ M3 จะต้องทำการบันทึกข้อมูลเกี่ยวกับแพ็กเก็ตตอบกลับ ที่ถูกส่งออกมาจากโหนดหมายเลข 4 ลงในตารางการเฝ้าฟัง ดังข้อมูลที่แสดงในตารางที่ 1
2. โมไบล์เอเจนต์ จะคอยเฝ้าฟังการส่งแพ็กเก็ตข้อมูล (Data Packet) ที่ถูกส่งออกมาจากโหนดในตารางการเฝ้าฟัง เนื่องจากจากข้อกำหนดของโปรโตคอลการสื่อสาร DSR โหนดตัวกลางจะทำการรับข้อมูลจากโหนดก่อนหน้า และส่งข้อมูลต่อไปยังโหนดตัวกลางตัวถัดไป ตามเส้นทางที่ระบุไว้ในแพ็กเก็ตตอบกลับเส้นทาง เช่นจากรูปที่ 1 โหนดหมายเลข 4 จะต้องมีการรับแพ็กเก็ตจากโหนดหมายเลข 3 และส่งต่อแพ็กเก็ตดังกล่าวไปยังโหนดถัดไป (โหนดหมายเลข 5) หากโหนดหมายเลข 4 ไม่ทำการส่งแพ็กเก็ตข้อมูลที่ได้รับออกมา ถือว่าโหนดดังกล่าวมีพฤติกรรมที่ผิดปกติในการสื่อสารครั้งนี้

ตารางที่ 1 ตารางบันทึกข้อมูลที่ได้จากการเฝ้าฟังการส่งแพ็กเก็ตตอบกลับเส้นทาง

ตารางการเฝ้าฟังบนโมไบล์เอเจนต์ M2	
ชื่อข้อมูล	ข้อมูลที่ถูกจัดเก็บ
Sender	4
Path	1,2,3,4,5
TimeStamp	0.123456789 Sec

3. โมไบล์เอเจนต์ทำการแจ้งความผิดปกติ ของโหนดแต่ละตัวหลังจากการเฝ้าฟังออกไปยังเครือข่าย ผ่านกระบวนการส่งแบบบรอดแคสต์ เพื่อให้โมไบล์เอเจนต์ตัวอื่นทำการเพิ่มข้อมูลความผิดปกติ ลงสู่ฐานข้อมูลของตัวเอง

3.2 กระบวนการวิเคราะห์โหนดที่มีพฤติกรรมผิดปกติ

การตัดสินพฤติกรรมที่ผิดปกติของโหนด จะใช้วิธีการให้คะแนนจากพฤติกรรมการสื่อสาร ที่เกิดขึ้นบนเส้นทางการสื่อสารที่โหนดดังกล่าวทำหน้าที่เป็นตัวกลางในการสื่อสาร โดยมีเงื่อนไขการให้คะแนนดังนี้

- ทุกโหนดที่ถูกเฝ้าฟังมีคะแนนความผิดปกติเริ่มต้นเป็น 0.0
- หากพฤติกรรมการสื่อสารของโหนดมีความผิดปกติ ระบบตรวจจับจะเพิ่มคะแนนครั้งละ 0.05
- หากโหนดมีการรับและส่งแพ็กเก็ตตามปกติ ระบบตรวจจับจะลดคะแนนลงครั้งละ 0.01
- เมื่อโหนดมีคะแนนเกิน 1.0 ระบบถือว่าโหนดดังกล่าวมีพฤติกรรมที่ผิดปกติ

โมไบล์เอเจนต์ทุกตัวจะมีตารางเก็บคะแนนความผิดปกติของโหนดในเครือข่าย โดยคะแนนดังกล่าวอาจได้มาจากการเฝ้าฟังโดยโมไบล์เอเจนต์เอง หรือได้รับการบรอดแคสต์ข้อมูลพฤติกรรม จากโมไบล์เอเจนต์ตัวอื่นก็ได้

ตารางที่ 2 ตารางบันทึกคะแนนแต่ละโหนดบนโมไบล์เอเจนต์

ตารางคะแนนบนโมไบล์เอเจนต์ M2	
ชื่อข้อมูล	ข้อมูลที่ถูกจัดเก็บ
Node	4
Point	0.10
LastUpdated	5.345874532 Sec

4. การทดลอง

งานวิจัยฉบับนี้ได้ทำการใช้ Network Simulator 2 (NS-2) เวอร์ชัน 2.27 สำหรับจำลองสภาพแวดล้อมการสื่อสารของเครือข่าย โดยระบบคอมพิวเตอร์ที่ใช้ทดสอบมีรายละเอียดดังนี้

- หน่วยประมวลผล Pentium 4 1.8 GHz
- หน่วยความจำ 512 MB
- ระบบปฏิบัติการ Linux RedHat 9.0 (Kernel Version 2.4.24)

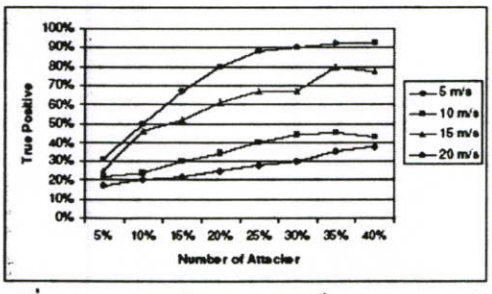
4.1 สภาพแวดล้อมของเครือข่าย

- พื้นที่ของเครือข่าย 1500 * 1500 ตารางเมตร
- จำนวนโหนดสื่อสาร 50 โหนด
- รัศมีการสื่อสารของโหนด 250 เมตร
- จำนวนการสื่อสารแบบ CBR (Constant Bit Rate) ทั้งหมด 15 ครั้ง
- โหนดมีการเคลื่อนที่แบบ Random Way Point Model มีความเร็วการเคลื่อนที่ 5, 10, 15 และ 20 เมตรต่อวินาที
- โหนดผู้บุกรุกมีไม่เกิน 40% ของโหนดสื่อสารทั้งหมด
- เวลาในการทดสอบ 1000 วินาที

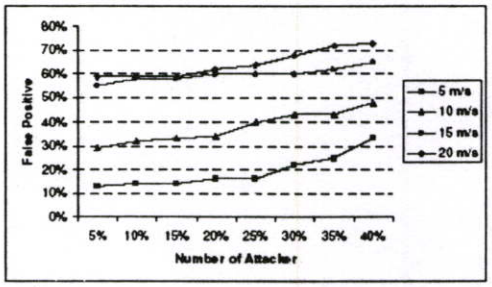
4.2 ผลการทดลอง

การทดลองได้ทำการสร้างสภาพแวดล้อมของเครือข่าย ที่มีความแตกต่างกันของความเร็วการเคลื่อนที่และจำนวนของโหนดผู้บุกรุกจำนวนทั้งหมด 16 รูปแบบ รูปที่ 2 คือกราฟ True Positive คือค่าความผิดพลาดในการตรวจจับซึ่งระบบไม่สามารถตรวจจับความผิดปกติที่เกิดขึ้นได้

ในรูปที่ 3 คือกราฟแสดงความผิดพลาดแบบ False Positive[6] (ความผิดพลาดที่ระบบทำการแจ้งเตือนว่าโหนดมีพฤติกรรมที่ผิดปกติ แต่ในความเป็นจริงโหนดดังกล่าวไม่ได้เป็นผู้บุกรุก) การทดลองในส่วนนี้ทำโดยกำหนดให้ในระบบเครือข่าย มีเพียงโหนดสื่อสารทำงานอยู่ (ไม่มีผู้บุกรุกในเครือข่าย) และให้ไมโบล์เอเจนต์ทำการเก็บข้อมูลเพื่อวิเคราะห์ผลที่ได้จากการเฝ้าฟัง



รูปที่ 2 กราฟแสดงความถูกต้องของการตรวจจับเปรียบเทียบกับความเร็วการเคลื่อนที่และจำนวนโหนดผู้บุกรุก



รูปที่ 3 กราฟแสดงความความผิดพลาดแบบ False Positive เปรียบเทียบกับความเร็วในการเคลื่อนที่

4.3 วิเคราะห์ผลที่ได้จากการทดลอง

จากผลการทดลองพบว่า ความถูกต้องของการระบุพฤติกรรมของโหนดว่ามีความผิดปกติหรือไม่ จะแปรผันเป็นอย่างมากกับความเร็วในการเคลื่อนที่ และจำนวนของโหนดผู้บุกรุก ซึ่งผลที่ได้สามารถวิเคราะห์เป็นสองประเด็นคือ

1. ในเครือข่ายที่มีความเร็วของการเคลื่อนที่สูง และมีปริมาณความเสียหายของเส้นทางการสื่อสารมาก จะมีแพ็กเก็ตปริมาณแพ็กเก็ตในเครือข่ายมากกว่าเครือข่ายที่มีความเสียหายเกิดขึ้นน้อย ปริมาณแพ็กเก็ตที่ถูกส่งออกมามากนั้น ส่งผลให้ความสามารถในการเฝ้าฟังลดลงเนื่องจากแพ็กเก็ตอาจเสียหายจากการชนกัน (Collision[1]) ที่เกิดขึ้น ทำให้ค่า True Positive มีค่าสูง
2. หากโหนดมีความเร็วในการเคลื่อนที่สูงขึ้น ปริมาณความเสียหายของเส้นทางการสื่อสาร จะมีมากขึ้นจากการเปลี่ยนแปลงโครงสร้างเครือข่าย ส่งผลให้ระบบตรวจจับมีการรายงานผิดพลาดแบบ False Positive สูงขึ้นตามลำดับ เพราะการโจมตีแบบ Packet Dropping[7] นั้น ก่อให้เกิดความเสียหายรูปแบบเดียวกันกับการที่โหนดตัวกลางมีเคลื่อนที่ออกจากเส้นทางการสื่อสาร

5. บทสรุปและแนวทางการวิจัยต่อ

ระบบตรวจจับผู้บุกรุกบนเครือข่ายไร้สายแบบแอดฮอก เป็นสิ่งจำเป็นสำหรับเครือข่ายที่ต้องการความน่าเชื่อถือและประสิทธิภาพในการสื่อสารสูง เนื่องจาก

โครงสร้างเครือข่ายที่เปลี่ยนแปลงอยู่ตลอดเวลา ทำให้การโจมตีจากผู้บุกรุกทำได้หลากหลายช่องทาง และยากที่จะตรวจสอบและควบคุมจากความสามารถเดิม ที่มีอยู่ในโปรโตคอลการสื่อสาร งานวิจัยฉบับนี้ได้เสนอวิธีการตรวจจับผู้บุกรุก สำหรับเครือข่ายไร้สายแบบแอดฮอคที่ใช้โปรโตคอลการสื่อสารแบบ DSR โดยการให้โมไบล์เอเจนต์ทำการเฝ้าฟังการสื่อสาร และวิเคราะห์ความผิดปกติโดยอ้างอิงจากพฤติกรรมปกติของโหนด ตามที่โปรโตคอลการสื่อสารระบุไว้

ผลที่ได้จากงานวิจัยนี้พบว่า ระบบตรวจจับโหนดที่มีพฤติกรรมผิดปกติ ที่ใช้วิธีการตรวจสอบความสัมพันธ์ระหว่างแพ็กเก็ตที่ถูกส่งออกจากโหนด และข้อมูลเส้นทางการสื่อสาร ที่ได้จากขั้นตอนค้นหาเส้นทาง สามารถระบุได้ว่าโหนดสื่อสารใดมีพฤติกรรมผิดปกติได้อย่างถูกต้อง และสามารถนำมาใช้จริงในเครือข่ายได้

งานวิจัยต่อไปที่กำลังดำเนินการ คือการลดความผิดพลาดแบบ False Positive ให้น้อยลง โดยเราจะพิจารณาการใช้ข้อมูลสภาพเครือข่าย เช่น ความเร็วการเคลื่อนที่และจำนวนการสื่อสารที่เกิดขึ้น เพื่อใช้ในการกำหนดค่าที่เหมาะสมของการให้คะแนนความผิดพลาดแต่ละครั้ง

6. เอกสารอ้างอิง

[1] David B., Johnson David A .and Maltz Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Computer Science Department Carnegie Mellon University Pittsburgh.

[2] Charles E. Perkins and Elizabeth M. Royer. "Ad hoc On-Demand Distance Vector Routing." Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[3] Z.J. Haas and M.R. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," Internet Draft, draft-ietf-manet-zone-zrp-02.txt, June 1999

[4] Sergio Marti, T.J. Giuli, Kevin Lai and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. Mobicom 2000, August 2000

[5] James Parker, Jeffrey Undercoffer, John Pinkston and Anupam Joshi "On Intrusion Detection and Response for Mobile Ad Hoc Networks"

[6] M. Just, E. Kranikis and T. Wan, "Resisting Malicious Packet Dropping in Wireless AdHoc networks", ADHOC-NOW 2003, LNCS 2865, pp. 151-163, 2003.

[7] Adam Burg. "Ad hoc network specific attacks", Technische Universität München, 2003.


ECTI-CON 2005
The 2005 ECTI International Conference
1 00 10 101 01000 1000 101110 10101010 101
ECTI
Association
May 12-13, 2005
Asia Pattaya Beach Hotel, Pattaya, Cholburi, THAILAND
NECTEC
PES

A Mechanism of Detecting Misbehavior Nodes in Ad-Hoc wireless networks

Chawedee Baramee Sakchai Thipchaksurat Ruttikorn Varakulsiripunth

Faculty of Engineering and Research Center for Communications and Information Technology (ReCCIT),
King Mongkut's Institute of Technology Ladkrabang,
Chalongkrung Road, Ladkrabang, Bangkok, Thailand 10520
E-mail: chawdeeb@hotmail.com , {ktsakcha and kvruttik}@kmitl.ac.th

ABSTRACT

This research proposes the methodology to detect misbehavior nodes in ad-hoc wireless networks that use Dynamic Source Routing (DSR) Algorithm for transferring data. The mobile agents are applied in the network for monitoring the communication of data at each intermediate node on the transmission path. The misbehavior nodes, detected by the mobile agents, are going to be verified by the destination node to confirm and to decrease the error of monitoring. For final data analysis, destination nodes are going to exchange the information of misbehavior nodes with other nodes in network. This information is compared with the highest acceptable failure of network to decide that the intermediate nodes are misbehavior or not.

Keywords: Ad-hoc wireless networks, Attacker, Intrusion Detection

1. INTRODUCTION

There are many differences between Ad-hoc wireless network and Wired Network. First, in ad-hoc wireless network, nodes can communicate between each other by using routing protocol, no need to use the access point. The routing protocols utilized in ad-hoc wireless network are dependent on each node serving as router. For examples of these protocols including DSR [1], AODV [2] and ZRP [3]. Moreover, the nodes of Ad-hoc Wireless Network are computationally constrained and have limited power.

The ad-hoc wireless networks is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line to defense. For a clear example, Ad-hoc wireless networks provide no fixed infrastructure, for the reason that nodes can move all over network space. While Ad-Hoc network is changing, it may cause the damage for route being used at that time. Likewise, network is vulnerable and may also be attacked. How to detect nodes that are misbehaviors, e.g. failing to forward data following criteria of protocol, is a challenge of research problem. Thus, in this research, we propose the mechanism to detect misbehavior node, especially packet dropping attack [9], in ad-hoc wireless networks which use Dynamic Source Routing Algorithm (DSR [1]). Mobile Agents in network are used to monitor storing-forwarding behavior of intermediate nodes. The mobile agents are nodes in network topology that are not part of route in current communication. The strategy monitor route reply packet. [1]. Thus, mobile agents know next destination of packets. If the communication node does not response in limit time, it can be said that this node is a misbehavior node.

The rest of this paper is organized as follows. Section 2 refers to some previous related works. Section 3 describes The Packet Flow Monitoring (PFM) machine. Section 4 describes the methodology in our research. Section 5 shows the simulation results. Finally, the conclusion and future works are given in Section 6.

2. RELATED WORKS

Watchdog, introduced by Marti et al. was the first snooping protocol for Mobile Ad-Hoc Networks (MANETs). Watchdog relies upon DSR and each node participates by "watching" its downstream node, on the route from source to destination, to ensure that it has retransmitted the packet without modification. Marti et al. hold that not only if source routing is not used then a misbehaving node could simply broadcast to a non-existent node, but Watchdog also is not capable to detect the complicated attacking, for example, collusion attack, multiple can mount a more sophisticated attack.

Buchegger and Le boudec [4] built upon Marti et al.'s work by replacing Watchdog with Neighborhood Watch, which is also dependent upon DSR, and snoops its downstream neighbor. They introduced a Trust Manager, Reputation System, and a Path Manager. Essentially each node is required to run a finite state machine to calculate trust, which in turn is used to rank the other node's reputation and then determine routes with the highest security metric. Buchegger and Le boudec [4] seemingly did not consider the resource constraints imposed upon most mobile ad-hoc devices, nor did they provide analysis of their protocol with respect to network performance.

Snooping Protocol [10] is the other monitoring technique to watch the inbound and outbound packet of each neighbor node, assumption is that, if any intermediate node receives the packet in, called

inbound, this node is going to send the packet out, called outbound. Mobile agents in Snooping try to monitor both of those packets. The weakness is that in unsuitable network topology, i.e. very wide network space, mobile agents are not able to monitor both inbound and outbound packet.

3. PACKET FLOW MONITORING (PFM)

In this paper, we present the "Packet Flow Monitoring" (PFM) mechanism in order to detect the node which has not retransmitted the packet properly. The basic assumption of our proposed PFM mechanism is that all nodes use omni- directional antenna and node can hear the packet that just has been sent out from intermediate node by using promiscuous mode on interface. The PFM mechanism composes of 3 sub-systems working together as shown in Fig.1.

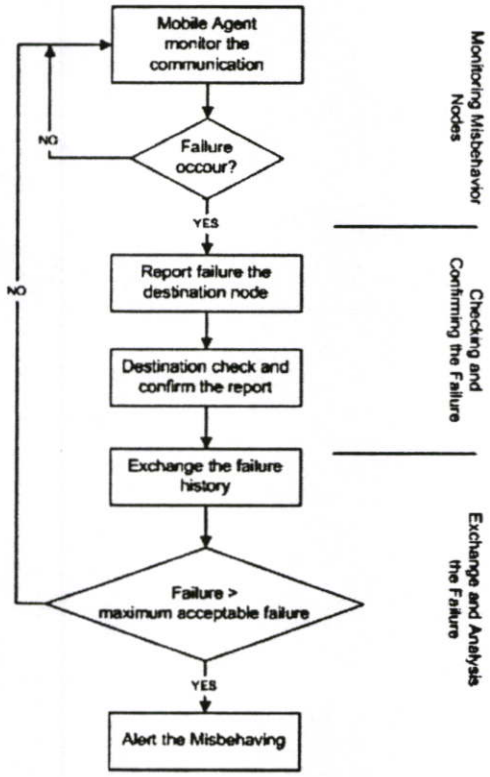


Fig.1 The entire process of PFM mechanism

3.1 Monitoring Misbehavior Nodes

This sub-system is to observe the flow of packet transferring in the path that its behavior is whether follow the DSR protocol or not. Our assumption use the basic concept of On-Demand routing protocol [4], when source has the data, sent to destination. Before packet of data will be sent, source has to use routing protocol (such as DSR) to find the reachable path from itself to the destination, this process is called *route discovery* [4]. In DSR, source use *route request packet* to discover the available path and *Route Reply Packets* is used by destination to inform the path information back to source.

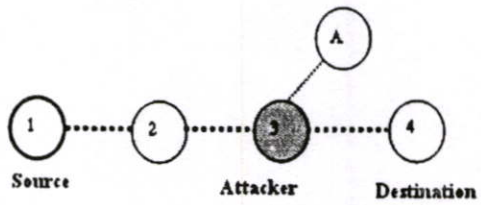


Fig. 2 Example of Network Topology

From Fig 2, source can communicate to destination by intermediate node [node: 2, 3]. Node *A*, not on the path from source to destination, is mobile agent hearing every packet in its boundary. The step to monitor misbehavior node in the path are as below:

1. When source want to communicate to the destination, source is going to send *route request packet* to destination. Then, the destination will send *Route Reply Packet* back to the source.
2. While *Route Reply Packets* is being sent out from the intermediate node, node *A* (or any agent) is monitoring these packets and records this transferring information, data being recorded are *sender node*, *path* and *timestamp*.
3. Node *A* will monitoring data packet sent out from the node *3* (which has been recorded previously), so if there are no data packet sent out from node *3*, node *A* keep the record that node *3* shows the misbehavior on this connection. Misbehavior record on node *A* will be checked and confirmed in the next sub-system.

3.2 Checking and Confirming the Failure

An ad-hoc wireless network consists of a collection of "peer" mobile nodes that are capable of communicating each other without help from a fixed infrastructure. Therefore, it could be very hard to decide the misbehavior nodes, detected by Monitoring Misbehavior nodes sub-system. As the intermediate nodes and the mobile agent may move away from each other, the error of misbehavior analysis may be easy to occur. One of the risky failures is called *False Positive*, which report that some nodes are misbehavior nodes but, in the right way, they are not misbehaviors.

To check and confirm the failure, system needs some reliability to check and confirm this. In this research, we use the destination of the transmission for the reasons that first; destination is the most reliability in communication path because almost attacking the intermediate node can be attacked by packet dropping attack. Second, destination can confirm the failure of the communication by checking with the transferring

protocol e.g. using sequence number of protocol to check the completion of data. Finally, since the transmission path from the monitoring of mobile agent can be used as a path to destination, mobile agent can send data to destination immediately and it does not have to search for a new transmission path. Checking and confirming processes are as below:

1. While destination is working, mobile agents of destination check all packets sent from source all the time by using information from transferring protocol such as sequence numbers and flags.
2. When all mobile agents find the misbehavior nodes, they are going to report to destination by using path from the monitoring. If they can not send data using that path, they will try to find new path.
3. Destination receives all the information of misbehavior nodes from mobile agents. Then, it compares this received data with the actual data, received from source. If destination does not receive the actual data from source as checking in 1, then, it can confirm which nodes in path do not send packets and are misbehaviors.

3.3 Exchange and Analysis the Failure

At this state, the last sub-system will analyze and confirm the correctness of the information from monitoring and identify misbehavior nodes in transferring path. After destination of each path has the misbehavior information, they have to exchange this information to other nodes in network.

Since information of misbehavior nodes may disperse on many destinations of each path in network and any node can be the intermediate node on many communication paths, this research propose the exchange and analysis the failure to occur on the last destination as following steps:

1. The last destination sends request for the history of misbehavior nodes by broadcast to its neighborhood nodes. This request from destination also identify the under suspicion nodes for the reason that all mobile agents can send the information of these misbehavior nodes back. And each neighborhood node re-broadcast this request all over network. For no repeated broadcasting of the request, we have to limit the hop of broadcasting as below:

$$\text{Hop Broadcasting} = \frac{\text{Longest Side of Network Area}}{\text{Radius of Transmission}}$$

For example, network space is 500 X 500 m^2 and the radius of broadcasting is 250 m. then, the hop to re-broadcast is $500/250 = 2$. This means that for all the network space, there are 2 hops to broadcast the request.

2. When each node receives the request for the history of misbehavior nodes, it is going to do a self-checking to find the requested information. If there is the information at this node, it is going to send the information back immediately.
3. When the destination receive the requested information, it keeps continue to the analysis process.

3.4 Analysis Misbehavior Nodes Information

Since the abnormal behavior of node may cause by its movement, this is acceptable for Ad-Hoc Wireless Network. Thus, the misbehavior analysis needs to adjust that the causes of the damage that occurred and have been detected are truly from attackers or from the movement of nodes.

We analyze this abnormality by comparing the number of misbehaviors, happened in network, with the *maximum acceptable failure* in the simulated network with no attacker as in section 4.

4. METHODOLY

In this section we describe our simulator, simulation parameters, and measured metrics.

We use the *Network Simulator 2* (NS-2) version 2.27 with the detail as below:

- Processor: Pentium4 1.8 GHz.
- Memory : 512 MB
- Operating System: Linux Redhat 9.0 (Kernel Version 2.4.24)

Our simulations take place in a 1,500 X 1,500 m^2 flat space filled with a scattering of 50 wireless nodes. The radius of each node is 250 m. The nodes communicate using 50 constant bit rate (CBR) node-to-node connections.

In all of our node movement scenarios, the nodes choose a destination and move in a straight line towards the destination at a speed uniformly distributed at 5, 10, 15 and 20 meters/second (m/s). This is called the random waypoint model [8].There are 10%, 20%, 30% and 40% of attackers which will act the misbehavior while transferring data packet. The run-time of the simulations is set to 1,000 seconds. The *maximum acceptable failure* is the average of the failure from the scenarios that no attacker in the network.

5. SIMULATION RESULTS

The simulation had been done with 16 different speeds of movement and number of attackers. The simulation has been done on Network Simulator 2 (NS-2). The results of the experiment are shown as graphs in the Fig. 2 and Fig. 3

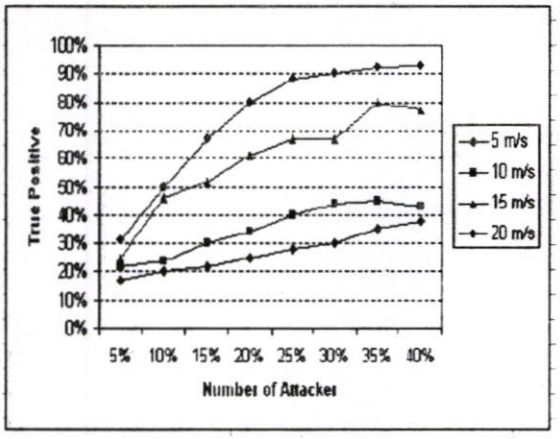


Fig.2: The comparative graph between the True Positive and the number of attackers

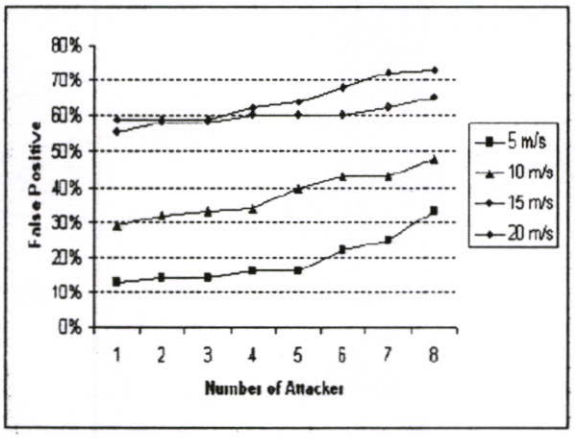


Fig. 3: The comparative graph between the False Positive and the number of attackers

6. CONCLUSION AND FUTURE WORKS

From our experiment, we can make the conclusion in according to the results of our simulation as follow. If mobility in network has high speed, then, the network topologies usually change. This bring about first, the routing paths have high risk of damage. And last, the failures from five simulations may have high difference, thus, the *maximum acceptable failure*, found from this simulations, may not trend to close to the reality.

Through our continuing investigation, we have shown that architecture with better intrusion detection in Ad-hoc wireless networks should be distributed and cooperative. A statistical anomaly detection approach should be used. The trace analysis and anomaly detection should be done locally in each node and possibly through cooperation with all nodes at the network. Furthermore, intrusion detection should take place at all networking layers in an integrated cross-layer manner.

7. REFERENCES

[1] David B., Johnson David A .and Maltz Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad-hoc Networks", Computer Science Department Carnegie Mellon University Pittsburgh

[2] Charles E. Perkins and Elizabeth M. Royer. "Ad-hoc On-Demand Distance Vector Routing." Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[3] Z.J. Haas and M.R. Pearlman, "The Zone Routing Protocol (ZRP) for Ad-hoc Networks," Internet Draft, draft-ietf-manet-zone-zrp-02.txt, June 1999

[4] Sergio Marti, T.J. Giuli, Kevin Lai and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", Proc. Mobicom 2000, August 2000

[5] James Parker, Jeffrey Undercoffer, John Pinkston and Anupam Joshi "On Intrusion Detection and Response for Mobile Ad-hoc Networks"

[6] M. Just, E. Kranikis and T. Wan, "Resisting Malicious Packet Dropping in Wireless AdHoc networks", ADHOC-NOW 2003, LNCS 2865, pp. 151-163, 2003.

[7] Adam Burg. "Ad-hoc network specific attacks", Technische Universität München, 2003.

[8] J. Broch, D. A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jectcheva. "A Performance Comparison of Multi-Hop Wireless Ad-hoc Network Routing Protocols.", In proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM '99), August 1999.

[9] Yongguang Zhang and Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", In Proceedings of the six Annual International Conference on Mobile Computing and Networking (MobiCom2000), Aug. 6-11,2000. Boston, Massachusetts.

[10] James Parker, Jeffrey Undercoffer, John Pinkston, and Anupam Joshi, "On intrusion Detection in Mobile Ad-hoc Networks". In Proceedings, 23rd IEEE International performance Computating and Communications Conference- Workshop on Information Assurance, April 2004.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายชาวดี บารมี
วันเดือนปีเกิด	วันที่ 11 มีนาคม 2522 ที่จังหวัดเชียงใหม่
ที่อยู่	95/360 หมู่บ้านชวนชื่นนีโอเฮาส์ ซ.คู้บอน 6 ถนนรามอินทรา แขวงคันนายาว เขตคันนายาว จังหวัดกรุงเทพมหานคร
ประวัติการศึกษา	2545 จบการศึกษาคณะวิศวกรรมศาสตร์สาขาวิชาคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง