โพรโทคอลเอโอดีวีแบบใช้เครดิตเพื่อป้องกันการโจมตีแบบหลุมดำ

Credit based AODV Protocol for Preventing Blackhole Attack

วัชระ แซ่ตั้ง

Watchara Saetang

วิทยานิพนธ์นี้สำหรับการศึกษาตามหลักสูตรปริญญา

วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

มหาวิทยาลัยสงขลานครินทร์

A Thesis Submitted in Fulfillment of the Requirements for the Degree of

Master of Engineering in Computer Engineering

Prince of Songkla University

2555

โพรโทคอลเอโอดีวีแบบใช้เครดิตเพื่อป้องกันการโจมตีแบบหลุมดำ

Credit based AODV Protocol for Preventing Blackhole Attack

วัชระ แซ่ตั้ง

Watchara Saetang

วิทยานิพนธ์นี้สำหรับการศึกษาตามหลักสูตรปริญญา

วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

มหาวิทยาลัยสงขลานครินทร์

A Thesis Submitted in Fulfillment of the Requirements for the Degree of

Master of Engineering in Computer Engineering

Prince of Songkla University

2555

ชื่อวิทยานิพนธ์ โพรโทคอลเอโอดีวีแบบใช้เครดิตเพื่อป้องกันการโจมตีแบบหลุมดำ
ผู้เขียน นายวัชระ แซ่ตั้ง
สาขาวิชา วิศวกรรมคอมพิวเตอร์

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

.....

(ดร.สกุณา เจริญปัญญาศักดิ์)

คณะกรรมการสอบ

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.วรรณรัช สันติอมรทัต)

.....กรรมการ

(ดร.กมล เขมะรังษี)

.....กรรมการ

(ดร.สกุณา เจริญปัญญาศักดิ์)

บัณฑิตวิทยาลัย มหาวิทยาลัยสงขลานครินทร์ อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษา ตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์

.....

(รองศาสตราจารย์ ดร.ธีระพล ศรีชนะ)

คณบดีบัณฑิตวิทยาลัย

ขอรับรองว่า ผลงานวิจัยนี้เป็นผลมาจากการศึกษาวิจัยของนักศึกษาเอง และขอขอบคุณผู้ที่มีส่วนเกี่ยวข้องทุกท่านไว้ ณ ที่นี้

ลงชื่อ_____

(ดร.สกุณา เจริญปัญญาศักดิ์)

อาจารย์ที่ปรึกษาวิทยานิพนธ์

ลงชื่อ_____

(นายวัชระ แซ่ตั้ง)

นักศึกษา

ข้าพเจ้าขอรับรองว่า ผลงานวิจัยนี้ไม่เคยเป็นส่วนหนึ่งในการอนุมัติปริญญาในระดับใดมาก่อน และไม่ได้ถูกใช้ในการยื่นขออนุมัติปริญญาในขณะนี้

ลงชื่อ_____

(นายวัชระ แซ่ตั้ง)

นักศึกษา

ชื่อวิทยานิพนธ์ โพรโทคอลเอโอดีวีแบบใช้เครดิตเพื่อป้องกันการโจมตีแบบหลุมดำ
ผู้เขียน นายวัชระ แซ่ตั้ง
สาขาวิชา วิศวกรรมคอมพิวเตอร์
ปีการศึกษา 2555

บทคัดย่อ

เครือข่ายไร้สายแบบ Ad hoc เป็นเครือข่ายที่ไม่จำเป็นต้องใช้สถานีฐานในการจัดการเส้นทางการสื่อสาร โหนดที่อยู่ในระยะทางการติดต่อสื่อสารสามารถติดต่อถึงกันได้โดยตรง แต่ในกรณีที่โหนดอยู่นอกระยะการติดต่อสื่อสาร โหนดจำเป็นต้องค้นหาเส้นทางการสื่อสารด้วยโพรโทคอลการค้นหาเส้นทาง ยกตัวอย่างเช่น Ad hoc On-demand Distance Vector (AODV) ที่มีประสิทธิภาพในการจัดการเส้นทางการสื่อสาร แต่การจัดการด้านการรักษาความปลอดภัยยังคงมีช่องโหว่ ส่งผลทำให้ง่ายต่อการโจมตีในระดับชั้นเครือข่าย โดยเฉพาะอย่างยิ่งการโจมตีแบบหลุมดำ

การโจมตีแบบหลุมดำจะทำการโจมตี โดยการส่งข้อความควบคุมที่มีข้อมูลเท็จไปยังโหนดต้นทางที่ต้องการส่งข้อมูล จึงส่งผลทำให้โหนดต้นทางไม่สามารถส่งข้อมูลไปยังโหนดปลายทางได้ ดังนั้นงานวิทยานิพนธ์นี้จึงนำเสนอโพรโทคอลการค้นหาเส้นทาง Credit based Ad hoc On-demand Distance Vector (CAODV) ซึ่งใช้ระบบของความน่าเชื่อถือ (Credits) เพื่อตรวจสอบและจัดการกับการโจมตีแบบหลุมดำ โดยทำการทดสอบด้วยโปรแกรมจำลองเครือข่าย Network simulator 2 (NS-2) เปรียบเทียบสมรรถนะการทำงานระหว่างโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV เพื่อแสดงให้เห็นถึงผลกระทบของการโจมตีแบบหลุมดำ และผลการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV ที่สามารถลดผลกระทบจากการโจมตีแบบหลุมดำได้ถึงร้อยละ 92

Thesis Title Credit based AODV Protocol for Preventing Blackhole Attack

Author Mr. Watchara Saetang

Major Program Computer Engineering

Academic Year 2012

ABSTRACT

Ad hoc networks are the network that having no infrastructure or base station. Node can either communicate directly to each other or via the intermediate nod. The well-known routing protocol used in ad hoc network is Ad hoc On-demand Distance Vector (AODV). However, the lack of security in AODV is it weakness. In this thesis, the blackhole attack is focused in order to minimize the significant effect of the attack.

In blackhole attack, the malicious node will send a false reply message to the source node. Thus the source node cannot transmit the data to the destination node. In this thesis, we proposed Credit based Ad hoc On-demand Distance Vector (CAODV) to detect and handle the effect of blackhole attack. The Network Simulator 2 (NS-2) has been used to analyze and compare the performance between the original AODV and CAODV. The result shows that CAODV is able to reduce the effect of blackhole attack about 92 percentages

กิตติกรรมประกาศ

ขอขอบพระคุณ ดร.สกุณา เจริญปัญญาศักดิ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้เสียสละเวลาในการให้คำปรึกษา พร้อมทั้งแนะนำแนวคิดในการทำวิทยานิพนธ์รวมถึงแนะนำวิธีการแก้ไขปัญหาที่เกี่ยวกับการทำวิทยานิพนธ์ ตลอดจนตรวจสอบและแก้ไขวิทยานิพนธ์ให้ดำเนินไปอย่างลุล่วงสมบูรณ์

ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.วรรณรัช สันติอมรทัต ที่กรุณาเสียสละเวลาเป็นกรรมการสอบวิทยานิพนธ์ อีกทั้งตรวจทานและแก้ไขวิทยานิพนธ์ให้มีความสมบูรณ์ยิ่งขึ้น

ขอขอบพระคุณ ดร.กมล เขมะรังษี ที่กรุณาเสียสละเวลาเป็นกรรมการสอบวิทยานิพนธ์ อีกทั้งตรวจทานและแก้ไขวิทยานิพนธ์ให้มีความสมบูรณ์ยิ่งขึ้น

ขอขอบพระคุณ บัณฑิตวิทยาลัย มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ ที่ให้การสนับสนุนทุนในการทำวิจัย และให้ความช่วยเหลือในการประสานงานด้านต่างๆ

ขอขอบพระคุณ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์ ที่ให้การสนับสนุนเงินทุนเพื่อใช้ในการประชุมวิชาการ

ขอขอบพระคุณ คณาจารย์ บุคลากร นักศึกษาปริญญาเอก และนักศึกษาปริญญาโท ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกคนที่ได้ให้คำปรึกษา และเป็นกำลังใจในการทำงานเป็นอย่างดีเสมอมา

และท้ายที่สุดนี้ ข้าพเจ้าขอน้อมรำลึกถึงพระคุณของบิดามารดา และครอบครัวที่ส่งเสริม และสนับสนุนข้าพเจ้าในทุกๆ เรื่องจนกระทั่งข้าพเจ้าสำเร็จการศึกษา

วัชระ แซ่ตั้ง

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

รายการตาราง

หน้า

รายการภาพประกอบ

หน้า

รายการภาพประกอบ (ต่อ)

หน้า

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของวิทยานิพนธ์

เครือข่ายการสื่อสารไร้สาย (Wireless networks) ได้รับความนิยมอย่างแพร่หลายในปัจจุบัน เนื่องจากอุปกรณ์สื่อสารไร้สายได้ใช้อากาศเป็นสื่อกลางในการสื่อสาร จึงสะดวกในการติดตั้ง โดยที่สามารถแบ่งระบบการสื่อสารไร้สายได้ 2 ลักษณะคือ เครือข่ายไร้สายแบบใช้สถานีฐาน (Base station) เพื่อกระจายสัญญาณในการติดต่อสื่อสาร และจัดการข้อมูลของเครือข่าย ซึ่งการใช้สถานีฐานนั้นทำให้ง่ายต่อการควบคุมและจัดการมากกว่าเครือข่ายไร้สายอีกประเภทนั้นก็คือ เครือข่ายไร้สายแบบ Ad hoc (Ad hoc networks) [1] ซึ่งไม่จำเป็นต้องใช้สถานีฐาน ดังนั้นเมื่ออุปกรณ์สื่อสารไร้สาย ในวิทยานิพนธ์ฉบับนี้เรียกว่า โหนด อยู่ในระยะการสื่อสาร โหนดสามารถติดต่อกันได้โดยตรง (Peer to Peer) แต่ในกรณีที่โหนดต้นทาง (Source node) ต้องการส่งข้อมูล แต่ไม่สามารถติดต่อโหนดปลายทาง (Destination node)ได้โดยตรง โหนดต้นทางจำเป็นต้องส่งข้อมูลไปยังโหนดอื่นๆในเครือข่าย เพื่อใช้เป็นเส้นทางในการสื่อสาร โดยจัดการเส้นทางการสื่อสารด้วยโพรโทคอลการค้นหาเส้นทาง (Routing Protocol) [2]

การสร้างเส้นทางสื่อสารในเครือข่ายไร้สายแบบ Ad hoc จำเป็นต้องใช้โพรโทคอลการค้นหาเส้นทาง โดยสามารถแบ่งได้ตามวิธีการในการสร้างและจัดการเส้นทางการสื่อสารได้ 3 ลักษณะ [2] คือ โพรโทคอลการค้นหาเส้นทางแบบ (1) Proactive (2) Reactive และ (3) Hybrid ซึ่งโพรโทคอลการค้นหาเส้นทางแบบ Hybrid เป็นโพรโทคอลที่รวมคุณลักษณะของโพรโทคอล Proactive และ Reactive ส่วนการจัดการเส้นทางโดยโพรโทคอลการค้นหาเส้นทางแบบ Proactive จะทำการตรวจสอบเส้นทางสื่อสารอยู่ตลอดเวลา ยกตัวอย่างเช่นโพรโทคอลการค้นหาเส้นทางที่ชื่อว่า Destination Sequence Distance Vector (DSDV) [3] มีลักษณะการทำงานโดยสร้างเส้นทางสื่อสารทั้งเครือข่าย และตรวจสอบข้อมูลเส้นทางสื่อสารอยู่ตลอดเวลา ในขณะที่โพรโทคอลอีกตัวหนึ่งได้แก่ โพรโทคอลการค้นหาเส้นทางแบบ Reactive ซึ่งเป็นที่นิยมและนำมาใช้อย่างกว้างขวาง ยกตัวอย่างเช่น โพรโทคอลการค้นหาเส้นทาง Ad hoc On-demand Distant Vector (AODV) [4] ทำการจัดการเส้นทางเมื่อโหนดมีการร้องขอ ดังนั้นจึงส่งผลทำให้เป็นโพรโทคอลที่มีภาระงาน (Overhead) ต่ำกว่าโพรโทคอลการค้นหาเส้นทางแบบ DSDV อย่างไรก็ตาม โพรโทคอลการค้นหาเส้นทาง AODV ยังคงมีจุดอ่อนในเรื่องของการรักษาความปลอดภัยโดยเฉพาะอย่างยิ่งการโจมตีแบบหลุมดำ [5]

การจัดการเส้นทางเป็นส่วนที่สำคัญที่ส่งผลกระทบต่อค่าสมรรถนะของเครือข่าย (Throughput) โดยเฉพาะอย่างยิ่งในกรณีที่เครือข่ายถูกโจมตีจะยิ่งส่งผลกระทบต่อค่าสมรรถนะการทำงานเป็นอย่างมาก สำหรับการโจมตีในระดับชั้นเครือข่าย เป็นการขัดขวางการสร้างเส้นทางการสื่อสาร โดยทำให้โหนดต้นทางไม่สามารถส่งข้อมูลไปยังโหนดปลายทางได้ จึงส่งผลทำให้เครือข่ายไร้สายแบบ Ad hoc ไม่สามารถให้บริการได้ จากการศึกษาผลกระทบของการโจมตีแบบต่างๆ พบว่าการโจมตีแบบหลุมดำเป็นรูปแบบหนึ่งที่ส่งผลกระทบกับเครือข่ายไร้สาย โดยที่สามารถทำให้ค่าสมรรถนะการทำงานลดลงไปถึงร้อยละ 90 [6] และการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV ก็ไม่สามารถตรวจสอบและจัดการกับการโจมตีแบบหลุมดำได้ ดังนั้นวิทยานิพนธ์นี้จึงเสนอโพรโทคอลการค้นหาเส้นทาง Credits based Ad hoc On-demand Distance Vector (CAODV) เพื่อใช้ตรวจสอบและจัดการกับการโจมตีแบบหลุมดำ

โพรโทคอลการค้นหาเส้นทาง CAODV พัฒนาจากโพรโทคอลการค้นหาเส้นทาง AODV ซึ่งยังคงกระบวนการจัดการเส้นทางไว้ดังเดิม แต่เพิ่มกระบวนการจัดการการโจมตีแบบหลุมดำ โดยการใช้ระบบความน่าเชื่อถือ (Credits) ให้แก่โหนดถัดไปในเส้นทางการสื่อสารเพื่อเป็นการกำหนดจำนวนข้อมูลที่ส่ง โดยมีกระบวนการที่เพิ่มขึ้นจากโพรโทคอล AODV คือ กระบวนการกำหนดค่าความน่าเชื่อถือ กระบวนการจัดการค่าความน่าเชื่อถือ และกระบวนการจัดการกับโหนดหลุมดำ ซึ่งโพรโทคอลการค้นหาเส้นทาง CAODV สามารถลดผลกระทบจากการโจมตีแบบหลุมดำ และทำให้สมรรถนะการทำงานของเครือข่ายยังคงเดิม

1.2 การตรวจเอกสาร

งานวิจัยที่เกี่ยวกับการจัดการกับการโจมตีแบบหลุมดำในเครือข่ายไร้สายแบบ Ad hoc อยู่หลายงานวิจัย ซึ่งในแต่ละกระบวนการมีข้อดี และข้อเสียแตกต่างกันไป สามารถสรุปได้ดังนี้

1.2.1 การใช้ศูนย์กลางในการจัดการความน่าเชื่อถือ

โดยปกติเครือข่ายไร้สายแบบ Ad hoc ไม่จำเป็นต้องมีศูนย์กลางในการจัดการข้อมูลในเครือข่าย ซึ่งเป็นคุณลักษณะที่ทำให้เครือข่ายไร้สาย Ad hoc แตกต่างกับเครือข่ายในลักษณะอื่นๆ แต่อย่างไรก็ตามมีงานวิจัยที่ได้นำเสนอเกี่ยวกับการใช้ศูนย์กลางมาจัดการกับระบบความปลอดภัยในเครือข่ายไร้สายแบบ Ad hoc จึงส่งผลทำให้โหนดในเครือข่ายสามารถจัดการกับเส้นทางการสื่อสารได้ดียิ่งขึ้น อย่างเช่น M. Raza และ S. I. Hyder ได้นำเสนอ Forced Routing Information Modification Model (FRIMM) [7] โดยมีการใช้ 2 ช่องสัญญาณที่แตกต่างกันในการ

จัดการข้อมูลเส้นทาง โดยมีการใช้มาตรฐานของ Wimax (IEEE 802.16) [8] เป็นช่องสัญญาณระหว่างศูนย์กลางกับสถานีฐาน และการใช้มาตรฐานของ Wifi (IEEE 802.11g) [9] กับโหนดติดต่อสื่อสารกับสถานีฐาน กระบวนตรวจสอบความถูกต้องของเส้นทาง โหนดจะทำการติดต่อไปยังสถานีฐาน จากนั้นสถานีฐานจะทำการติดต่อไปยังศูนย์กลางเพื่อตรวจสอบความถูกต้อง โดยกระบวนการตรวจสอบต่างๆ จะมีสถานีฐานเป็นตัวในการจัดการข้อมูลในตารางเส้นทาง จึงส่งผลทำให้ทุกโหนดในเครือข่ายมีข้อมูลเส้นทางที่ถูกต้องและมีความน่าเชื่อถือ แต่อย่างไรก็ตามการใช้สถานีฐานในการจัดการข้อมูลจะทำให้คุณสมบัติของเครือข่ายไร้สาย Ad hoc เปลี่ยนไป

1.2.2 การใช้กระบวนการด้านการเข้ารหัส

การเข้ารหัสถือเป็นเรื่องที่สำคัญอย่างหนึ่งในด้านความปลอดภัยโดยเฉพาะอย่างยิ่งการรักษาความลับ แต่อย่างไรก็ตามยังคงสามารถนำมาประยุกต์ใช้ในการยืนยันตัวบุคคลและความถูกต้องของข้อมูล ซึ่งโดยปกติแล้วการจัดการในการเข้ารหัสนั้นจำเป็นต้องมี กุญแจ หรือ สิ่งที่เชื่อได้ว่ามีความถูกต้อง ยกตัวอย่างเช่น ใบรับรอง (Certificated) ซึ่งการจัดการในเรื่องดังกล่าวมักมีความยุ่งยากและซับซ้อน โดยเฉพาะอย่างยิ่งเครือข่ายไร้สายแบบ Ad hoc ที่ไม่มีศูนย์กลางในการจัดการด้านความน่าเชื่อถือ ดังนั้นการจัดการในการกระจายกุญแจหรือการแลกกุญแจ เพื่อใช้ในการเข้ารหัสจึงเป็นไปได้ยาก แต่อย่างไรก็ตามมีหลายงานวิจัยที่มีการนำการใช้การเข้ารหัสในเครือข่ายไร้สายแบบ Ad hoc

โพรโทคอลการค้นหาเส้นทาง Secure AODV (SAODV) [10] ได้เพิ่มส่วนข้อมูลในข้อความควบคุมต่างๆ ในโพรโทคอลการค้นหาเส้นทาง AODV โดยการใช้หลักการของการใช้กุญแจ โดยถือว่าทุกโหนดมีการยืนยันตัวตนและมีกุญแจอย่างถูกต้อง โดยจะทำการสร้างสัญลักษณ์จากกุญแจ (Signature) และตารางเปรียบเทียบ (Hash Chain) เพื่อเป็นการยืนยันตัวตนและความถูกต้องของข้อมูล จึงส่งผลทำให้สามารถมั่นใจได้ว่าข้อความควบคุม RREP ที่ได้รับมาจากโหนดปลายทางอย่างถูกต้อง แต่อย่างไรก็ตามหลักการทำงานในการเข้ารหัสและถอดรหัสด้วยกุญแจจำเป็นต้องใช้การคำนวณที่สูง ประกอบกับต้องมีการจัดการกุญแจที่มีความน่าเชื่อถือจึงสามารถทำให้เชื่อถือในการเข้ารหัสได้

1.2.3 การตรวจสอบการส่งข้อมูลต่อของโหนดเพื่อนบ้าน

K.Lakhani และคณะได้เสนอกระบวนการ Watchdog [11] ใช้ในเครือข่ายแบบไร้สายแบบ Ad hoc ที่มีการใช้โพรโทคอลการค้นหาเส้นทาง AODV ซึ่งกำหนดให้โหนดฟังการติดต่อสื่อสารของโหนดเพื่อนบ้านอยู่เสมอ ส่งผลทำให้โหนดสามารถตรวจสอบได้ว่าโหนดเพื่อน

บ้านมีการส่งข้อมูลต่อไปหรือไม่ แต่ยังคงมีข้อจำกัดที่ไม่สามารถตรวจสอบ การความถูกต้องของการส่งข้อมูลได้ในกรณีที่มีการชนกันของข้อมูล เนื่องจากข้อจำกัดของโหนดที่มองไม่เห็น (Hidden Terminal) ซึ่งเป็นปัญหาที่เกิดขึ้นเมื่อโหนด 2 โหนดทำการส่งข้อมูลไปหาอีกโหนดในช่วงเวลาเดียวกัน จึงเป็นสาเหตุทำให้เกิดการชนกันของข้อมูลส่งผลทำให้โหนดไม่สามารถตรวจสอบช่องสัญญาณของโหนดถัดไปได้ แต่การทำงานของ Watchdog สามารถเพิ่มค่าสมรรถนะของเครือข่ายไร้สายแบบ Ad hoc เมื่อถูกโจมตีแบบหลุมดำร้อยละ 10 ถึงร้อยละ 18 แต่อย่างไรก็ตามการใช้กระบวนการ Watchdog ภาระงานของโหนดจะเพิ่มขึ้น โดยโหนดอยู่ในสภาวะตื่น (Wake up) อยู่ตลอดเวลาเพื่อทำการตรวจสอบโหนดเพื่อนบ้าน ซึ่งส่งผลทำให้โหนดสิ้นเปลืองพลังงานเป็นอย่างมาก และมีข้อจำกัดที่ไม่สามารถตรวจสอบเมื่อมีการชนกันของข้อมูล ดังนั้นจึงไม่เหมาะสมกับเครือข่ายที่มีความหนาแน่นสูง

P. K. Singh และ G. Sharma [12] ได้นำเสนอวิธีการที่ใกล้เคียงกับกระบวนการ Watchdog แต่กระบวนการนี้จะเริ่มใช้ในกรณีที่โหนดได้รับข้อความควบคุม RREP จากโหนดอื่นๆ นอกเหนือจากโหนดปลายทาง โดยโหนดต้นทางจะทำการส่งข้อความควบคุม Hello ไปยังโหนดปลายทาง และใช้วิธีการเดียวกับ Watchdog ในการติดตามผลการส่งข้อความ Hello โดยโหนดจะทำการตรวจสอบโหนดเพื่อนบ้านในการส่งต่อข้อความ ในกรณีที่พบว่าโหนดไหนไม่ทำการส่งข้อความ Hello จะถือว่าโหนดดังกล่าวมีการทำการโจมตีแบบหลุมดำ ซึ่งกระบวนการดังกล่าวนี้สามารถจัดการกับการโจมตีแบบหลุมดำได้ แต่อย่างไรก็ตามการสื่อสารของเครือข่ายนี้จะมีเวลาหน่วง (Delay) เนื่องจากจำเป็นต้องตรวจสอบเสร็จทางก่อนส่งข้อมูล

การตรวจสอบโหนดเพื่อนบ้านโดยการตรวจสอบการส่งต่อของข้อมูลมีจุดอ่อนที่สำคัญอย่างยิ่งโดยเฉพาะโหนดจะไม่มีข้อมูลของโหนดในเส้นทางสื่อสาร จึงไม่สามารถตรวจสอบได้ว่าข้อมูลได้ส่งไปยังโหนดที่มีอยู่จริงหรือไม่ ในกรณีที่โหนดทำการส่งต่อข้อมูลไปยังโหนดถัดไปที่ไม่มีอยู่จริง กระบวนการตรวจสอบโหนดเพื่อนบ้านจะไม่สามารถตรวจสอบได้ จึงส่งผลทำให้เกิดการโจมตีได้

1.2.4 การตรวจนับและตรวจสอบจำนวนการส่งข้อมูล

G. S. Mamatha และ S.C. Sharma ได้นำเสนอโพรโทคอล Highly Secured Approach against attacks in MANETs (HSAM) [13] โหนดต้นทางจะทำการตรวจนับจำนวนข้อมูลที่ส่ง และทำการส่งข้อมูลการนับโดยใช้ข้อความควบคุมที่มีข้อมูลการนับจำนวนข้อมูลที่ส่งไปยังโหนดปลายทาง (cpkt) เมื่อโหนดปลายทางได้รับข้อมูลการนับจะทำการตอบกลับด้วยข้อความควบคุม ACK กลับไปยังต้นทางเพื่อยืนยันว่าได้รับข้อความควบคุม cpkt และส่งข้อมูลของจำนวน

ข้อมูลที่สูญหาย (cmiss) โดยคิดจากจำนวนข้อมูลที่ส่งหักลบกับจำนวนข้อมูลที่ได้รับ จากนั้นเมื่อโหนดต้นทางได้รับข้อมูล จะทำการหาอัตราส่วนระหว่าง cmiss และ cpkt โดยจะถือว่าถ้าเส้นทางที่สื่อสารอยู่มีอัตราส่วนที่ต่ำกว่า 20 จะถือว่าเส้นทางนั้นยังคงมีสมรรถนะในการสื่อสาร

M. S. Obaidat และคณะ [14] ได้ทำการปรับปรุงโพรโทคอล HSAM โดยเรียกว่า Enhance-HSAM (E-HSAM) โดยพัฒนาการส่ง cpkt โดย HSAM เดิมจะมีการส่งข้อความควบคุมแยกออกไปโดยมีขนาด 48 ไบต์ จึงง่ายต่อการสูญหายและการปลอมแปลง ดังนั้นโพรโทคอล E-HSAM ได้ทำการรวมข้อมูลจำนวนการส่งข้อมูลส่งไปพร้อมกับข้อมูลปกติ จึงทำให้การใช้ข้อมูล cpkt จะมีขนาดเล็กลง ภาระงานเครือข่ายจึงลดลง และยังสามารถตรวจสอบความถูกต้องของข้อมูล cpkt ได้อีกด้วย จึงส่งผลทำให้ E-HSAM มีอัตราส่วนในการรับส่งข้อมูลที่สูงกว่า HSAM แต่อย่างไรก็ตามยังคงมีจุดอ่อน เช่นเดียวกับโพรโทคอล HASM ในเรื่องของการนำสัดส่วนมาคิดเป็นเกณฑ์ในการตัดสินถือว่าเป็นจุดอ่อนในการโจมตี เพราะโหนดจะทำการโจมตีเป็นรูปแบบให้ต่ำกว่าเกณฑ์ได้เสมอ และเครือข่ายไม่สามารถจัดการกับการโจมตีได้

1.2.5 การส่งข้อความควบคุมตอบกลับจากโหนดปลายทาง

วิธีการที่ให้โหนดปลายทางส่งข้อความควบคุมกลับไปยังโหนดต้นทาง เพื่อเป็นการแจ้งให้ทราบว่าโหนดปลายทางสามารถรับข้อมูลได้จริง ซึ่งสามารถใช้เป็นการยืนยันความถูกต้องของเส้นทางสื่อสารได้อีกวิธีการหนึ่ง มีอยู่หลายงานวิจัยที่ได้นำเสนอดังนี้

S. Khurana [15] เสนอโพรโทคอลการค้นหาเส้นทาง Reliable Ad hoc On-demand Distance Vector (RAODV) ซึ่งพัฒนามาจากโพรโทคอลการค้นหาเส้นทาง AODV โดยเริ่มกระบวนการตรวจสอบก็ต่อเมื่อโหนดในเครือข่ายที่ได้รับข้อความควบคุม RREP มากกว่า 1 ข้อความและได้รับจากโหนดที่แตกต่างกัน ซึ่งหมายความว่ามีเส้นทางการสื่อสารมากกว่า 1 เส้นทางไปยังโหนดปลายทาง ดังนั้นโหนดจะทำการตรวจสอบเส้นทางโดยการส่งข้อความควบคุม Reliable Route Discovery Unit (RRDU) ไปตามเส้นทางส่งไปยังโหนดปลายทาง เมื่อโหนดปลายทางได้รับข้อความควบคุม RRDU จะทำการตอบกลับด้วยข้อความควบคุม RRDU Reply ซึ่งมีเพียงโหนดปลายทางเท่านั้นที่สามารถสร้างข้อความควบคุม RRDU Reply ได้ ดังนั้นเมื่อโหนดได้รับข้อความควบคุม RRDU Reply จากเส้นทางใด โหนดจะเชื่อถือว่าข้อมูลเส้นทางที่ได้รับนั้นมีความน่าเชื่อถือสามารถใช้เป็นเส้นทางการสื่อสารได้ แต่อย่างไรก็ตามโพรโทคอลการค้นหาเส้นทาง RAODV ยังมีข้อจำกัดในการจัดการกับการโจมตีแบบหลุมดำในกรณีที่ข้อความควบคุม RRDU Reply มีการสูญหายส่งผลทำให้เส้นทางนั้นไม่มีความน่าเชื่อถือ และในกรณีที่มีเส้นทางไป

ยังโหนดปลายทางเส้นทางเดียวโหนดจะไม่สามารถตรวจสอบเส้นทางได้ จึงทำให้เกิดการโจมตีแบบหลุมดำได้

S. S. Ramaswami และ S. Upadhyaya [16] ได้เสนอให้โหนดปลายทางส่งข้อความควบคุม Acknowledgement (ACK) ที่ใช้รูปแบบเช่นเดียวกับข้อความควบคุม RREP ในการแจ้งโหนดต้นทางเมื่อได้รับข้อมูลโดยส่งไปยังเส้นทางสื่อสารต่างๆ โดยการส่งข้อความควบคุม ACK จะขึ้นอยู่กับโหนดต้นทาง เมื่อโหนดต้นทางส่งข้อมูลจะทำการเพิ่มเครื่องหมายใช้แจ้งปลายทางให้ส่ง ACK ส่งแนบไปพร้อมกับข้อมูลที่ส่ง ซึ่งจะแนบไปแบบสุ่มแต่จะไม่เกินร้อยละ 10 ของข้อมูลที่ส่ง และเมื่อโหนดปลายทางได้รับข้อมูลที่แนบเครื่องหมายจะทำการส่งข้อความควบคุม ACK กลับไปยังโหนดต้นทางโดยใช้เส้นทางต่างๆ ไปยังโหนดต้นทาง เมื่อโหนดต้นทางได้รับ ACK จะถือว่าเส้นทางดังกล่าวมีความน่าเชื่อถือและสามารถส่งข้อมูลต่อไปได้ แต่อย่างไรก็ตามกระบวนการนี้มีข้อจำกัดหลายประการได้แก่ ไม่สามารถระบุได้ว่าโหนดใดเป็นโหนดหลุมดำ แต่สามารถระบุได้เพียงว่าเส้นทางที่ใช้อยู่มีการโจมตีแบบหลุมดำหรือไม่ รวมไปถึงข้อจำกัดเช่นเดียวกับโพรโทคอลการค้นหาเส้นทาง RAODV ที่จำเป็นต้องใช้เส้นทางมากกว่าหนึ่งเส้นทาง และการกำหนดค่าที่เหมาะสมในการใช้เครื่องหมายในการแจ้งเตือนให้โหนดปลายทางส่งข้อความควบคุม ACK เนื่องจากจะเป็นการเพิ่มภาระงานให้เครือข่าย

1.2.6 การเก็บข้อมูลจากข้อความควบคุม RREP

N. Mistry และคณะ [17] ได้ทำการปรับปรุงโพรโทคอลการค้นหาเส้นทาง AODV โดยกำหนดให้โหนดทำการเก็บข้อมูลของข้อความควบคุม RREP ไว้ระยะเวลาหนึ่ง เพื่อทำการตรวจสอบค่าเลขลำดับปลายทาง (Destination Sequence Number) โหนดต้นทางจะทำการเปรียบเทียบเลขลำดับปลายทางในข้อความควบคุม RREP กับค่าเลขลำดับปลายทางเกณฑ์มาตรฐาน (Destination Sequence Number Threshold) ในกรณีโหนดหลุมดำส่งข้อความควบคุม RREP ที่ค่าหมายเลขลำดับมีค่ามากเกินกว่าค่าเลขลำดับปลายทางเกณฑ์มาตรฐานที่กำหนด โหนดต้นทางจะทำการแจ้งเตือนไปยังโหนดอื่น และไม่สนใจเส้นทางจากโหนดหลุมดำ ดังนั้นเมื่อเครือข่ายไร้สายแบบ Ad hoc ถูกโจมตีแบบหลุมดำ เครือข่ายยังคงสมรรถนะการทำงานได้เหมือนในกรณีที่ไม่มีการโจมตี แต่การเก็บข้อมูลจากข้อความควบคุม RREP ยังคงมีจุดอ่อนในเรื่องการกำหนดและการเปลี่ยนแปลงค่าเลขลำดับปลายทางเกณฑ์มาตรฐานที่ใช้ในการตรวจสอบ เนื่องจากการกำหนดค่าเลขลำดับปลายทางเกณฑ์มาตรฐานจำเป็นต้องใช้ข้อมูลเลขลำดับปลายทางจากข้อความควบคุม RREP มากกว่าหนึ่งข้อความ ดังนั้นกระบวนการนี้จึงมีข้อจำกัดในการจัดการกับการโจมตีแบบ

หลุมดำเป็นอย่างมาก สำหรับกรณีที่โหนดได้รับข้อความควบคุม RREP จากโหนดหลุมดำเพียงโหนดเดียว จึงส่งผลทำให้ไม่สามารถตรวจสอบการโจมตีได้

ดังนั้นในงานวิจัยนี้จึงมุ่งเน้นในการออกแบบโพรโทคอลที่สามารถจัดการกับการโจมตีแบบหลุมดำ และเพิ่มภาระงานกับเครือข่ายไร้สายแบบ Ad hoc อย่างเหมาะสม

1.3 วัตถุประสงค์ของวิทยานิพนธ์

1.3.1 แสดงผลกระทบจากการโจมตีแบบหลุมดำในเครือข่ายไร้สายแบบ Ad hoc

1.3.2 ออกแบบกระบวนการทำงานเพื่อตรวจสอบและจัดการกับการโจมตีแบบหลุมดำ

1.4 ขอบเขตการวิจัย

1.4.1 การโจมตีแบบหลุมดำเป็นการโจมตีในระดับชั้นเครือข่าย ดังนั้นในงานวิทยานิพนธ์นี้จึงสนใจผลกระทบจากการโจมตีที่ส่งผลต่อการทำงานของระดับชั้นเครือข่าย โดยถือว่าการทำงานของระดับชั้นอื่นมีความถูกต้องและน่าเชื่อถือ

1.4.2 ออกแบบและทดสอบการทำงานที่มีการโจมตีแบบหลุมดำ

1.4.3 สามารถหาวิธีการป้องกันการโจมตีแบบหลุมดำ เมื่อระบบทำงานอยู่บนเครือข่ายไร้สาย

1.5 ขั้นตอนและวิธีดำเนินงานวิจัย

ขั้นตอนการดำเนินงานวิทยานิพนธ์แบ่งออกเป็น 10 ขั้นตอน เริ่มจากเดือนมิถุนายน 2553 และสิ้นสุด เดือนกุมภาพันธ์ 2555 โดยมีรายละเอียดขั้นตอนการดำเนินงานดังนี้

ขั้นที่ 1: ศึกษาแนวทาง และวิธีการดำเนินงานวิจัย
ขั้นที่ 2: ศึกษาทฤษฎีการทำงานของเครือข่ายไร้สายแบบ Ad hoc และการโจมตีในด้านความปลอดภัยของเครือข่ายไร้สายแบบ Ad hoc
ขั้นที่ 3: ศึกษาและทดสอบเครือข่ายไร้สายแบบ Ad hoc ในโปรแกรมจำลองเครือข่าย NS-2
ขั้นที่ 4: ศึกษาการโจมตีแบบหลุมดำในโพรโทคอลการค้นหาเส้นทาง AODV
ขันที่ 5: ออกแบบและเพิ่มการโจมตีแบบหลุมดำในโปรแกรมจำลองเครือข่าย NS-2
ขั้นที่ 6: ออกแบบโพรโทคอลการค้นหาเส้นทาง CAODV
ขั้นที่ 7: ทดสอบโพรโทคอลการค้นหาเส้นทาง CAODV ในโปรแกรมจำลองเครือข่าย NS-2

ขั้นที่ 8: ปรับปรุงและทดสอบการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV
ขั้นที่ 9: ทดสอบและเปรียบเทียบการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV เมื่อเครือข่ายทำงานปกติและมีการโจมตีแบบหลุมดำ
ขั้นที่ 10: สรุปผล จัดทำรายงานฉบับสมบูรณ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 เครือข่ายไร้สายแบบ Ad hoc ที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV ถูกโจมตีแบบหลุมดำ ยังคงสามารถให้บริการและจัดการกับการโจมตีแบบหลุมดำได้

1.6.2 การจัดการค่าความน่าเชื่อถือของโพรโทคอลการค้นหาเส้นทาง CAODV กำหนดจำนวนข้อมูลที่ส่ง ดังนั้นจึงลดผลกระทบจากการโจมตีแบบขัดขวางการให้บริการ (Denial of Service) ได้ ดังนั้นจึงเหมาะกับการติดต่อสื่อสารในการทหาร หรือในสถานการณ์ฉุกเฉิน ยกตัวอย่างเช่น ภัยพิบัติ เพื่อสามารถให้เครือข่ายสามารถบริการได้เมื่อมีการโจมตี

1.7 อุปกรณ์และสถานที่วิจัย

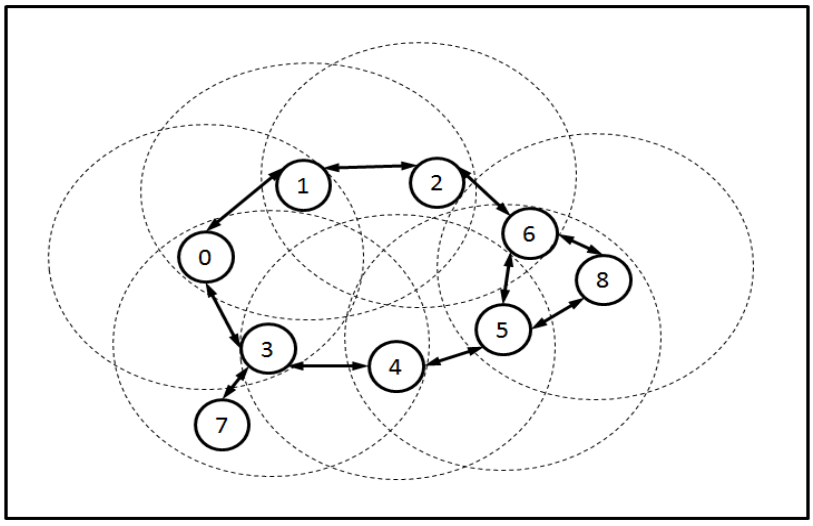
1.7.1 อุปกรณ์ คอมพิวเตอร์และโปรแกรมจำลองเครือข่าย NS-2 รุ่น 2.34 บนระบบปฏิบัติการ Linux Ubuntu รุ่น 10.10

1.7.2 สถานที่ทำวิจัย ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์

บทที่ 2
ทฤษฎีและหลักการ

2.1 เครือข่ายไร้สายแบบ Ad hoc

เครือข่ายไร้สายแบบ Ad hoc เป็นเครือข่ายของกลุ่มโหนดที่ติดต่อสื่อสารถึงกันได้โดยไม่จำเป็นต้องใช้สถานีฐาน และมีคุณลักษณะที่แตกต่างกับเครือข่ายลักษณะอื่น เช่น โหนดสามารถมีการเคลื่อนที่ได้ ส่งผลทำให้สามารถจำแนกเครือข่ายไร้สายแบบ Ad hoc ได้ 2 ประเภทตามการเคลื่อนที่ของโหนด [18] ได้แก่ เครือข่ายของกลุ่มโหนดไม่เคลื่อนที่ Static Ad hoc Networks (SANETs) และ เครือข่ายของกลุ่มโหนดเคลื่อนที่ Mobile Ad hoc Networks (MANETs) ซึ่งการเคลื่อนที่ของโหนดส่งผลให้รูปทรงของเครือข่ายมีการเปลี่ยนแปลง ส่งผลให้เครือข่ายไร้สายแบบ Ad hoc เป็นเครือข่ายในลักษณะพลศาสตร์ (Dynamics) นอกจากนี้เครือข่ายไร้สายแบบ Ad hoc ยังคงมีข้อจำกัดทางด้านทรัพยากรต่างๆ เช่น ประสิทธิภาพของโหนด พลังงาน ระยะทางการติดต่อสื่อสาร และช่องสัญญาณในการสื่อสาร (Bandwidth) โดยยกตัวอย่างเครือข่ายไร้สายแบบ Ad hoc ในรูป 2.1



รูปที่ 2.1 ตัวอย่างเครือข่ายไร้สายแบบ Ad hoc

ตัวอย่างเครือข่ายไร้สายแบบ Ad hoc ในรูปที่ 2.1 ประกอบด้วยกลุ่มโหนดจำนวน 9 โหนด ในกรณีที่โหนดอยู่ในระยะทางการสื่อสารจะสามารถติดต่อสื่อสารกันได้โดยตรง ซึ่งเรียกโหนดเหล่านี้ว่า โหนดเพื่อนบ้าน ยกตัวอย่างเช่น โหนด 1 และ 3 เป็นโหนดเพื่อนบ้านของโหนด 0

เป็นต้น แต่ในอีกกรณีที่โหนดต้องการทำการส่งข้อมูลไปยังโหนดที่อยู่นอกระยะทางการสื่อสารของตนเอง โหนดไม่สามารถทำการส่งข้อมูลได้โดยตรง ดังนั้นโหนดที่ต้องการส่งข้อมูลหรือเรียกว่า โหนดต้นทาง จำเป็นต้องทำการหาเส้นทางการสื่อสารไปยัง โหนดปลายทางซึ่งเป็นโหนดที่ทำการรับข้อมูล โดยการส่งข้อมูลผ่านโหนดเพื่อนบ้านโดยใช้เป็นเส้นทางในการสื่อสารจนไปถึงโหนดปลายทาง ยกตัวอย่างการส่งข้อมูลจากโหนด 0 ไปยังโหนด 7 ซึ่งไม่สามารถติดต่อสื่อสารกันได้โดยตรง โหนด 0 จึงจำเป็นต้องส่งข้อมูลไปยังโหนด 3 และโหนด 3 ทำหน้าที่ส่งข้อมูลต่อไปยังโหนด 7 ที่เป็นปลายทาง หรือในอีกกรณี โหนด 0 อาจจะส่งไปยังโหนด 1 2 6 5 4 3 และ 7 ตามลำดับ ซึ่งในกรณีนี้จะเห็นว่าเป็นเส้นทางการสื่อสารที่ใช้จำนวนโหนดในการส่งข้อมูลมาก ดังนั้นการจัดการเส้นทางการสื่อสารของโหนดในเครือข่ายจึงเป็นเรื่องที่จำเป็น โดยการจัดการเส้นทางที่ดี สามารถช่วยลดภาระงาน (Overhead) ให้เครือข่ายได้ จึงมีการกำหนดมาตรฐานในการจัดการเส้นทางโดยการใช้โพรโทคอลการค้นหาเส้นทางในการจัดการเส้นทางการสื่อสารในเครือข่าย

2.2 โพรโทคอลการค้นหาเส้นทางในเครือข่ายไร้สายแบบ Ad hoc

การติดต่อสื่อสารของโหนดในเครือข่ายไร้สายแบบ Ad hoc สามารถติดต่อสื่อสารกันได้โดยตรงเมื่อโหนดอยู่ในระยะทางการสื่อสารโดยไม่จำเป็นต้องใช้สถานีฐาน แต่ในกรณีที่โหนดปลายทางอยู่นอกระยะทางการสื่อสาร โหนดต้นทางจำเป็นต้องทำการหาเส้นทางการสื่อสารไปยังโหนดปลายทางโดยกำหนดวิธีการสร้างเส้นทางสื่อสารด้วยการใช้โพรโทคอลการค้นหาเส้นทาง โดยสามารถจำแนกตามการจัดการข้อมูลเส้นทางการสื่อสารได้ 3 ลักษณะ คือ โพรโทคอลการค้นหาเส้นทางแบบ Proactive โพรโทคอลการค้นหาเส้นทางแบบ Reactive และโพรโทคอลการค้นหาเส้นทางแบบ Hybrid

2.2.1 โพรโทคอลการค้นหาเส้นทางแบบ Proactive

โหนดในเครือข่ายจะมีการจัดการกับตารางเส้นทางของเครือข่ายร่วมกันอยู่ตลอดเวลา โดยจะทำการแก้ไขข้อมูลเป็นช่วงเวลาอยู่เสมอ ส่งผลทำให้โหนดจะมีเส้นทางไปยังโหนดทั้งหมด ดังนั้นจึงมีการใช้ข้อความควบคุม (Control Messages) มากกว่าโพรโทคอลการค้นหาเส้นทางในลักษณะอื่น ยกตัวอย่างเช่น โพรโทคอลการค้นหาเส้นทาง DSDV เลือกเส้นทางที่สั้นที่สุดในการติดต่อสื่อสารกับทุกโหนด และทำการปรับปรุงตารางเส้นทางเป็นช่วงเวลาอยู่เสมอ ซึ่งทำให้มีการใช้ข้อความควบคุมจำนวนมากและจะมีข้อมูลเส้นทางการสื่อสารที่ไม่จำเป็น ส่งผลทำให้เป็นภาระงานของเครือข่ายเพิ่มขึ้น ดังนั้นจึงมีการพัฒนาการจัดการเส้นทางเพื่อลดภาระของ

เครือข่ายลง โดยสร้างเส้นทางการสื่อสารเท่าที่จำเป็น ซึ่งเป็นหลักการจัดการเส้นทางสื่อสารของโพรโทคอลการค้นหาเส้นทางแบบ Reactive

2.2.2 โพรโทคอลการค้นหาเส้นทางแบบ Reactive

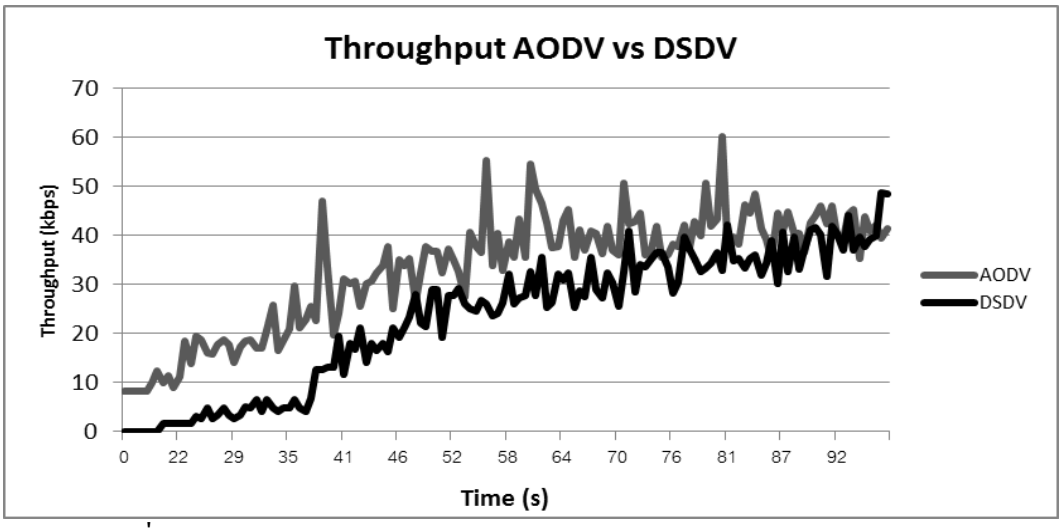
การทำงานของโพรโทคอลการค้นหาเส้นทางแบบ Reactive จะทำการค้นหาเส้นทางหรือทำการปรับปรุงตารางเส้นทางก็ต่อเมื่อโหนดมีความต้องการใช้เส้นทางในการสื่อสารหรือเส้นทางการสื่อสารเดิมเสียหายเท่านั้น ซึ่งแต่ละโหนดจะมีตารางเส้นทางและสามารถจัดการเส้นทางการสื่อสารด้วยตนเอง ดังนั้นจะทำให้การใช้ข้อความควบคุมลดลงไปอย่างมากเมื่อเปรียบเทียบกับโพรโทคอลการค้นหาเส้นทางแบบ Proactive ตัวอย่างเช่น โพรโทคอลการค้นหาเส้นทาง AODV ซึ่งพัฒนามาจากโพรโทคอลการค้นหาเส้นทาง DSDV มีการใช้ข้อความควบคุมเพื่อสร้างเส้นทางสื่อสารก็ต่อเมื่อโหนดต้องการส่งข้อมูล ส่งผลทำให้แต่ละโหนดจะมีตารางเส้นทางเส้นทางเป็นของตนเอง ซึ่งจะแตกต่างกับโพรโทคอลการค้นหาเส้นทาง DSDV ที่จะมีตารางเส้นทางของโหนดทั้งหมดในเครือข่าย ค่าภาระงานของเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV จึงน้อยกว่าโพรโทคอลการค้นหาเส้นทาง DSDV โดยการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV อธิบายไว้ในหัวข้อ 2.3

2.2.3 โพรโทคอลการค้นหาเส้นทางแบบ Hybrid

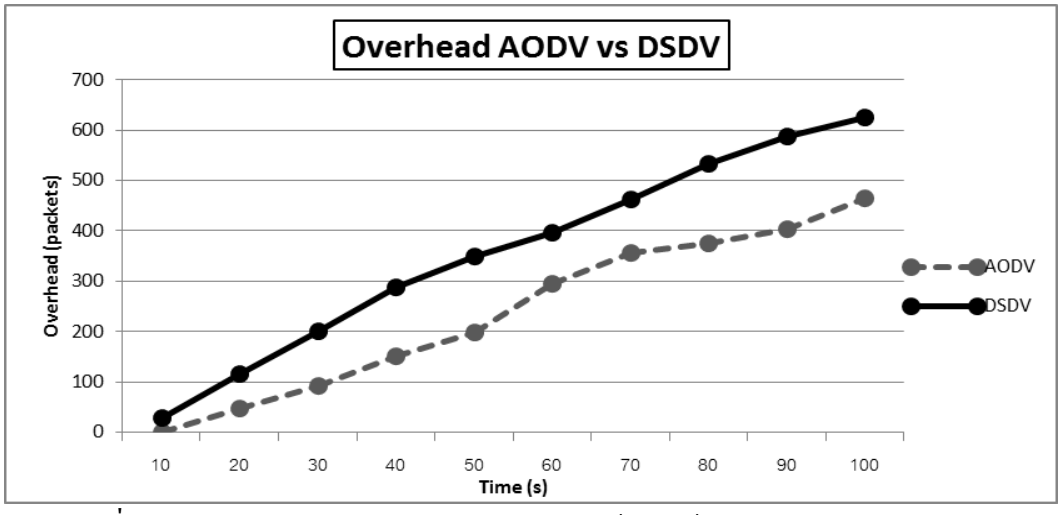
โพรโทคอลการค้นหาเส้นทางแบบ Hybrid นำรูปแบบการจัดการเส้นทางของโพรโทคอลการค้นหาเส้นทางแบบ Proactive และแบบ Reactive มาใช้ร่วมกัน โดยใช้กระบวนการของโพรโทคอลการค้นหาเส้นทาง Proactive ในการปรับปรุงเส้นทางกับโหนดเพื่อนบ้าน ส่วนโหนดอื่นในเครือข่ายจะทำการปรับปรุงเส้นทางเมื่อมีการร้องขอเท่านั้น โพรโทคอลการค้นหาเส้นทางแบบ Hybrid เช่น โพรโทคอลการค้นหาเส้นทาง Zone Routing Protocol (ZRP) [9] ลักษณะการทำงานจะเป็นลักษณะแบ่งเครือข่ายเป็นส่วนๆ โดยโหนดบางส่วนจะมีการใช้การปรับปรุงเส้นทางตลอดเวลาและโหนดบางส่วนจะทำการปรับปรุงเส้นทางเมื่อมีการร้องขอหรือโหนดต้องการส่งข้อมูลเท่านั้น

การทำงานของโพรโทคอลการค้นหาเส้นทางส่งผลต่อสมรรถนะของเครือข่ายไร้สายแบบ Ad hoc เป็นอย่างมาก โดยเฉพาะในกรณีที่โหนดไม่สามารถค้นหาเส้นทางการสื่อสารได้จะทำให้ไม่สามารถส่งข้อมูลไปยังโหนดปลายทางได้ ดังนั้นการเลือกใช้โพรโทคอลการค้นหาเส้นทางจึงเป็นปัจจัยที่สำคัญอย่างยิ่งต่อเครือข่ายไร้สายแบบ Ad hoc ดังนั้นงานวิทยานิพนธ์นี้จึงเลือกใช้โพรโทคอลการค้นหาเส้นทาง AODV ในการจัดการเส้นทางการสื่อสาร เพราะเป็น

โพรโทคอลการค้นหาเส้นทางแบบ Reactive ที่ทำการค้นหาเส้นทางก็ต่อเมื่อโหนดจำเป็นต้องส่งข้อมูลเท่านั้น จึงมีภาระงานต่ำแต่ยังคงมีสมรรถนะในการค้นหาเส้นทางเช่นเดียวกับโพรโทคอลการค้นหาเส้นทาง DSDV โดยได้ทำการทดสอบในเครือข่ายไร้สายแบบ Ad hoc ที่จำนวนโหนด 30 โหนด ดังรูปที่ 2.2 และการเปรียบเทียบค่าภาระงานระหว่างโพรโทคอลการค้นหาเส้นทาง AODV และโพรโทคอลการค้นหาเส้นทาง DSDV ในรูปที่ 2.3



รูปที่ 2.2 ค่าสมรรถนะของโพรโทคอลการค้นหาเส้นทาง AODV และ DSDV



รูปที่ 2.3 ค่าภาระงานสะสมของโพรโทคอลการค้นหาเส้นทาง AODV และ DSDV

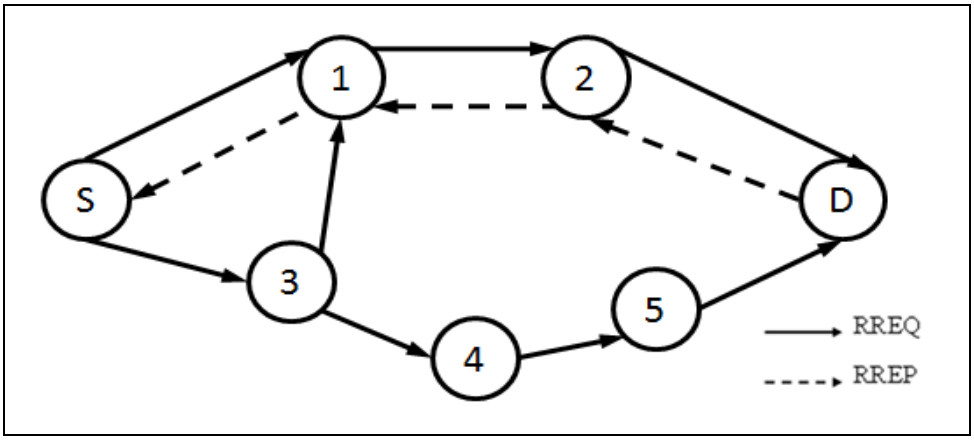
รูปที่ 2.2 และ 2.3 เปรียบเทียบสมรรถนะการทำงานและค่าภาระงานของเครือข่ายไร้สายแบบ Ad hoc ที่จำนวนโหนด 30 โหนด เมื่อใช้โพรโทคอลการค้นหาเส้นทาง AODV และ DSDV ในการจัดการเส้นทาง โดยค่าสมรรถนะการทำงานของเครือข่ายใกล้เคียงกัน แต่เมื่อ

เปรียบเทียบในด้านภาระงานของเครือข่าย เครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง DSDV มีภาระงานที่สูงกว่าโพรโทคอลการค้นหาเส้นทาง AODV เป็นอย่างมาก เนื่องจากโพรโทคอลการค้นหาเส้นทาง DSDV จำเป็นต้องปรับปรุงเส้นทางอยู่ตลอดเวลา แต่โพรโทคอลการค้นหาเส้นทาง AODV เมื่อสร้างเส้นทางสื่อสารได้จะไม่มีการปรับปรุงเส้นทาง จนกว่าเส้นทางการสื่อสารจะเสียหายเท่านั้น ดังนั้นการจัดการเส้นทางของ AODV จึงมีประสิทธิภาพและยังมีภาระงานที่ต่ำเหมาะสมกับเครือข่ายไร้สายแบบ Ad hoc

2.3 โพรโทคอลการค้นหาเส้นทาง AODV

โพรโทคอลการค้นหาเส้นทาง AODV เป็นโพรโทคอลการค้นหาเส้นทางแบบ Reactive จะเลือกเส้นทางที่สั้นที่สุดในการติดต่อสื่อสารและทำการสร้างเส้นทางก็ต่อเมื่อโหนดจำเป็นต้องใช้เส้นทางเท่านั้น โดยการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV ใช้ข้อความควบคุม 3 ชนิดคือ Route Request (RREQ), Route Reply (RREP) และ Route Error (RERR) ซึ่งสามารถแบ่งการทำงานได้ 2 กระบวนการคือ กระบวนการค้นหาเส้นทาง (Route Discovery) และกระบวนการบำรุงรักษาเส้นทาง (Route Maintenance)

เมื่อโหนดต้นทางต้องการเส้นทางการสื่อสารเพื่อใช้ในการส่งข้อมูล โหนดต้นทางจะทำการตรวจสอบเส้นทางในตารางเส้นทางของตนเอง ในกรณีที่มีเส้นทางการสื่อสารก็สามารถส่งข้อมูลได้ทันที แต่ในกรณีที่ไม่มีเส้นทางสื่อสาร โหนดจะเริ่มกระบวนการค้นหาเส้นทาง โดยทำการส่งกระจาย (Broadcast) ข้อความควบคุม RREQ ไปยังโหนดเพื่อนบ้าน เมื่อโหนดเพื่อนบ้านได้รับข้อความควบคุม RREQ จะทำการตรวจสอบความถูกต้องของข้อความควบคุม RREQ และข้อมูลในตารางเส้นทาง ในกรณีที่มีข้อมูลเส้นทาง โหนดจะทำการส่งข้อความควบคุม RREP กลับไปยังโหนดต้นทาง หรือกรณีที่ไม่มีข้อมูลเส้นทางของโหนดปลายทาง โหนดจะส่งกระจายข้อความควบคุม RREQ ต่อไปจนกระทั่งถึงโหนดปลายทาง เมื่อโหนดปลายทางได้รับข้อความควบคุม RREQ ตอบกลับด้วยข้อความควบคุม RREP ไปยังโหนดต้นทาง และเมื่อโหนดต้นทางได้รับข้อความควบคุม RREP โหนดต้นทางจะทำการพิจารณาข้อมูลจาก เลขลำดับปลายทางเพื่อป้องกันการวน (Loop) ของเส้นทางและตรวจสอบความใหม่ของข้อมูล และจำนวนโหนดที่ใช้ส่งข้อมูล (Hop count) เพื่อเลือกเส้นทางที่สั้นที่สุดในการสร้างเส้นทาง โดยยกตัวอย่างการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV ในรูป 2.4



รูปที่ 2.4 กระบวนการทำงานค้นหาเส้นทางของ AODV

จากรูปที่ 2.4 ตัวอย่างการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV โดยโหนด S เป็นโหนดต้นทาง ต้องการทำการส่งข้อมูลไปยังโหนด D ซึ่งเป็นโหนดปลายทาง ในกรณีที่โหนด S ไม่มีข้อมูลเส้นทาง จะทำการส่งกระจายข้อความควบคุม RREQ ไปยังโหนดเพื่อนบ้าน คือ โหนด 1 และ โหนด 3 ในกรณีที่โหนดเพื่อนบ้านไม่มีเส้นทางจะทำการส่งกระจายข้อความควบคุม RREQ ต่อไป จนกระทั้งโหนด D ได้รับข้อความควบคุม RREQ จะทำการตอบกลับด้วยข้อความควบคุม RREP ไปยังโหนด 2 ส่งแบบโดยตรง (Unicast) เมื่อโหนด S ได้รับข้อความควบคุม RREP จะทำการบันทึกข้อมูลเส้นทางลงในตารางเส้นทาง และสามารถส่งข้อมูลได้จนกว่าเส้นทางในการส่งข้อมูลจะเสียหาย จากนั้นจะเริ่มกระบวนการบำรุงรักษาเส้นทาง

กระบวนการบำรุงรักษาเส้นทางจะทำการตรวจสอบเส้นทางในการส่งข้อมูล กรณีที่โหนดมีการเคลื่อนที่หรือโหนดหายไป (เนื่องจากพลังงานหมดหรืออยู่ในสภาวะหลับ (Sleep)) ซึ่งเป็นสาเหตุทำให้เส้นทางในการส่งข้อมูลเสียหาย ดังนั้นโพรโทคอลการค้นหาเส้นทาง AODV จึงใช้ข้อความควบคุม RREP ที่กำหนดให้มีระยะการส่งหนึ่งโหนด ซึ่งอาจเรียกว่าข้อความควบคุม Hello เพื่อใช้ในการตรวจสอบสถานะของโหนดเพื่อนบ้าน ในกรณีที่โหนดเพื่อนบ้านเป็นโหนดที่ใช้เป็นเส้นทางในการส่งข้อมูล เมื่อโหนดพบความเสียหายจะทำการตรวจสอบว่าใกล้ต้นทางหรือใกล้ปลายทาง ในกรณีที่โหนดอยู่ใกล้ปลายทางโหนดจะเริ่มกระบวนการซ่อมแซมเฉพาะที่ (Local Repair) โดยโหนดที่พบเส้นทางเสียหายจะพยายามซ่อมแซมเส้นทางด้วยกระบวนการค้นหาเส้นทางใหม่ไปยังโหนดปลายทางด้วยตนเอง แต่ในกรณีที่ไม่สามารถค้นหาเส้นทางได้หรือโหนดที่พบความเสียหายอยู่ใกล้โหนดต้นทางโหนดที่พบความเสียหายของเส้นทางจะทำการส่งข้อความควบคุม RERR ไปยังโหนดต้นทางเพื่อเริ่มกระบวนการค้นหาเส้นทางใหม่อีกครั้ง

กระบวนการจัดการเส้นทางของโพรโทคอลการค้นหาเส้นทาง AODV โหนดจำเป็นต้องเชื่อถือข้อมูลในข้อความควบคุม RREQ RREP และ RERR ในการจัดการเส้นทางโดยไม่

มีการตรวจสอบความน่าเชื่อถือและความถูกต้องของข้อมูล ดังนั้นโพรโทคอลการค้นหาเส้นทาง AODV จึงมีจุดอ่อนอย่างมากในด้านการจัดการด้านความปลอดภัย ซึ่งระบบการรักษาความปลอดภัยของเครือข่ายไร้สายแบบ Ad hoc เป็นส่วนที่สำคัญที่มีผลต่อด้านการให้บริการของเครือข่าย

2.4 ระบบการรักษาความปลอดภัยในเครือข่ายไร้สายแบบ Ad hoc

ระบบการรักษาความปลอดภัยของเครือข่ายเป็นเรื่องที่สำคัญ เครือข่ายไร้สายแบบ Ad hoc ต้องการความปลอดภัยที่สำคัญ 5 อย่าง [19-21] คือ (1) เครือข่ายต้องมีความสามารถให้บริการได้ (Availability) ซึ่งเครือข่ายสามารถให้บริการรับและส่งข้อมูลได้ (2) ความถูกต้องสมบูรณ์ (Integrity) ของข้อมูลที่ส่งและข้อมูลที่ได้รับจำเป็นต้องถูกต้องเหมือนเดิม (3) การรักษาความลับ (Confidential) คือข้อมูลที่ส่งจะมีเพียงโหนดต้นทางและโหนดปลายทางเท่านั้นที่สามารถอ่านข้อมูลได้อย่างถูกต้อง (4) การพิสูจน์ตัวตน (Authentication) ต้องระบุโหนดและข้อมูลส่งจากโหนดที่ถูกต้องได้ และ (5)ไม่สามารถปฏิเสธความรับผิดชอบได้ (Non-repudiation) คือเมื่อมีการส่งข้อมูลแล้ว ไม่สามารถปฏิเสธได้ว่าเป็นการส่งที่มาจากตนเองได้ ซึ่งความปลอดภัยข้างต้นสามารถถูกโจมตีได้ง่ายเนื่องจากคุณลักษณะเฉพาะของเครือข่ายไร้สายแบบ Ad hoc

เครือข่ายไร้สายแบบ Ad hoc เป็นเครือข่ายแบบเปิดและใช้อากาศเป็นตัวกลางในการส่งสัญญาณซึ่งง่ายต่อการดักฟัง ประกอบกับการที่เครือข่ายไม่ใช้สถานีฐานในการจัดการ ส่งผลให้ไม่มีศูนย์กลางที่น่าเชื่อถือ โหนดจึงจำเป็นต้องตัดสินใจด้วยตนเอง ดังนั้นการจะรักษาความปลอดภัยในเครือข่ายไร้สายแบบ Ad hoc จึงทำได้ยากและการที่โหนดมีทรัพยากรอย่างจำกัด จึงเกิดเหตุการณ์ที่แตกต่างจากเครือข่ายอื่นๆบ้าง เช่น การเป็นโหนดเห็นแก่ตัว (Selfish node) โดยไม่ยอมเป็นโหนดในเส้นทางในการส่งข้อมูล การโจมตีโหนดอื่นๆให้สูญเสียพลังงาน เป็นต้น จุดอ่อนที่สำคัญอีกประการคือการที่โหนดจำเป็นต้องใช้ข้อมูลจากโหนดต่างๆในการตัดสินใจ โดยเฉพาะการสร้างเส้นทางการสื่อสาร ส่งผลให้โหนดมีโอกาสถูกโจมตีได้ง่ายมากจากโหนดอื่นๆ โดยการโจมตีในเครือข่ายไร้สายแบบ Ad hoc สามารถแบ่งได้ 2 ประเภทคือ (1) การโจมตีแบบไม่แก้ไขข้อมูล (Passive attack) ยกตัวอย่างเช่น การดักฟัง การขโมยแพ็กเก็ตข้อมูล เป็นต้น (2) การโจมตีแบบแก้ไขข้อมูล (Active attack) หรือการขัดขวางการทำงาน เช่น การแก้ไขข้อมูลในข้อความควบคุม การทำให้แพ็กเก็ตข้อมูลสูญหายหรือปลอมแปลงแพ็กเก็ตข้อมูล เป็นต้น ซึ่งบทความงานวิจัย [20] ได้ทำการสรุปการโจมตีและมีความต้องการด้านความปลอดภัยในระบบเครือข่ายไร้สายแบบAd hocทุกระดับชั้นดังนี้

ชั้นกายภาพ (Physical layer) ในเครือข่ายไร้สายแบบ Ad hocใช้อากาศเป็นสื่อกลาง ทำให้ง่ายต่อการดักฟังและการรบกวนของสัญญาณ การโจมตีในระดับชั้นกายภาพนั้นเป็นในลักษณะของการขัดขวางการให้บริการ เช่น การปล่อยสัญญาณรบกวน (Signal jamming) ซึ่งทำให้เกิดการชนกันของสัญญาณได้

ชั้นเชื่อมโยง (Link layer) ทำหน้าที่ในการติดต่อสื่อสารระหว่างโหนด การตรวจสอบช่องสัญญาณ การพิสูจน์ตัวตน การจัดการกุญแจในการเข้ารหัสและถอดรหัส ซึ่งโพรโท-คอลในระดับชั้นเชื่อมโยง เช่น IEEE 802.11 MAC มีจุดอ่อนหลายกระบวนการ เช่น กระบวนการ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) ที่มีการใช้เวลา Backoff สุ่มเพื่อให้สิทธิในการใช้ช่องสัญญาณ ในการโจมตีด้วยโหนดที่เห็นแก่ตัว จะทำการลดเวลา Backoff เพื่อแย่งชิงการใช้ช่องสัญญาณ จึงมีปัญหาในเรื่องความไม่เท่าเทียมในการใช้ช่องสัญญาณ และปัญหาหลักอีกอย่างของชั้นเชื่อมโยงคือ การจัดการคีย์ในการเข้ารหัสและถอดรหัส เพราะในเครือข่ายแบบไร้สายแบบ Ad hoc มีข้อจำกัดด้านทรัพยากรในด้านพลังงานและความสามารถของตัวประมวลผล ทำให้ไม่สามารถเข้ารหัสที่ซับซ้อนได้

ชั้นเครือข่าย (Network layer) ทำหน้าที่ในการกำหนดและจัดการเส้นทางการสื่อสารจากโหนดต้นทางไปยังโหนดปลายทาง ซึ่งการโจมตีในระดับชั้นเครือข่ายสามารถจำแนกได้เป็น 2 ลักษณะ คือ การโจมตีโดยแก้ไขข้อมูลเส้นทางและการโจมตีในการส่งแพ็กเก็ตข้อมูลจำนวนมาก การโจมตีโดยการเปลี่ยนแปลงหรือปลอมแปลงข้อมูลในการจัดการเส้นทางแบ่งได้ 2 ลักษณะ คือ (1) การเปลี่ยนแปลงข้อมูล และการเปลี่ยนแปลงข้อมูลสถานะของเส้นทางในข้อความควบคุม (2) การโจมตีโดยขัดขวางการส่งข้อมูล โดยการทิ้งข้อมูล (Drop) ของโหนดอื่นๆที่ใช้เป็นเส้นทางในการส่งข้อมูล ซึ่งในปัจจุบันโพรโทคอลการค้นหาเส้นทางบางตัวมีประสิทธิภาพในการสร้างเส้นทางสื่อสารได้เป็นอย่างดี แต่ไม่มีความสามารถในการจัดการด้านความปลอดภัย ดังนั้นเมื่อมีการโจมตีในชั้นเครือข่ายทำให้สมรรถนะของเครือข่ายไร้สายแบบ Ad hoc ลดลงเป็นอย่างมาก

ชั้นขนส่ง (Transport layer) ทำหน้าที่ควบคุมการส่งข้อมูลและความน่าเชื่อถือในการส่งข้อมูล สมรรถนะการทำงานของโพรโทคอลในชั้นขนส่งในเครือข่ายไร้สายแบบ Ad hoc ขึ้นกับหลายปัจจัย เช่น เส้นทางการสื่อสารมีการเปลี่ยนแปลงตลอดเวลา การขัดขวางการให้บริการ การโจมตีแบบ Session Hijack โดยปกติแล้วหากมีการป้องกันในชั้นเครือข่ายและชั้นเชื่อมโยงแล้วถือว่าแพ็กเก็ตข้อมูลที่ได้รับในชั้นขนส่งมีความปลอดภัยในด้านของการรักษาความลับ การยืนยันตัวบุคคล และความถูกต้องของข้อมูลหน้าที่ของชั้นขนส่งคือ การควบคุม การจัดลำดับ และการจัดการสถานะเชื่อมต่อของโหนด

ชั้นโปรแกรมประยุกต์ (Application layer) ในเครือข่ายแบบไร้สายแบบ Ad hoc ต้องมีการป้องกัน ค้นหาโปรแกรมที่ไม่พึงประสงค์และการเข้ารหัสข้อมูลในระดับชั้นโปรแกรมประยุกต์ หากไม่มีการป้องกันในระดับชั้นโปรแกรมประยุกต์ส่งผลให้ ระดับชั้นล่างได้รับข้อมูลที่ผิดได้

การจัดการด้านความปลอดภัยในเครือข่ายไร้สายแบบ Ad hoc มีความสำคัญทุกระดับชั้น โดยเฉพาะความปลอดภัยในระดับเครือข่าย เพราะใช้ในการจัดการเส้นทางในการส่งข้อมูล ในกรณีที่มีการโจมตีในระดับชั้นเครือข่ายส่งผลทำให้โหนดในเครือข่ายไม่สามารถส่งข้อมูลไปยังโหนดปลายทางได้ จึงส่งผลทำให้สมรรถนะของเครือข่ายลดลงอย่างมาก

2.5 การโจมตีในระดับชั้นเครือข่ายบนเครือข่ายไร้สายแบบ Ad hoc

ระดับชั้นเครือข่ายทำหน้าที่ในการจัดการค้นหาเส้นทางในการส่งข้อมูล ความปลอดภัยในระดับเครือข่ายมีความสำคัญต่อสมรรถนะในเครือข่ายไร้สายแบบ Ad hoc เป็นอย่างมาก ซึ่งการโจมตีในระดับเครือข่ายทำได้โดย การแก้ไขข้อมูลเส้นทางให้มีข้อมูลเส้นทางที่ผิดและการขัดขวางการส่งข้อมูลไปยังโหนดปลายทาง ซึ่งการโจมตีในระดับเครือข่ายสามารถแบ่งออกได้ดังนี้ [22-25]

การโจมตีแบบ Flooding [26] เป้าหมายของการโจมตีคือ การขัดขวางการให้บริการหรือการทำให้โหนดอื่นจำเป็นต้องทำงานขยะจนไม่สามารถทำงานที่ถูกต้องได้ ซึ่งในเครือข่ายไร้สายแบบ Ad hoc มีทรัพยากรที่จำกัดคือ ช่องสัญญาณและพลังงานของโหนด ซึ่งการโจมตีแบบ Flooding ทำให้โหนดอื่นไม่สามารถใช้ช่องสัญญาณได้และทำให้โหนดสูญเสียพลังงานไปโดยเปล่าประโยชน์

การโจมตีแบบหลุมดำ (Blackhole attack) เป็นการโจมตีที่เกิดขึ้นได้ง่ายในกระบวนการค้นหาเส้นทางของโพรโทคอลการค้นหาเส้นทางแบบ Reactive โดยโหนดหลุมดำทำการส่งข้อความควบคุมปลอมที่มีข้อมูลเส้นทางเท็จ เพื่อทำให้โหนดต้นทางเลือกเส้นทางการสื่อสารที่ผิด เมื่อโหนดที่ทำการโจมตีแบบหลุมดำได้รับข้อมูล และทำการทิ้งข้อมูลที่ได้รับทั้งหมด ส่งผลเครือข่ายมีการสูญหายของแพ็กเก็ตร้อยละ 90 [27]

การโจมตีแบบรูหนอน (Wormhole attack) เป็นการโจมตีโดยการร่วมมือระหว่างโหนดอย่างน้อย 2 โหนด โดยทำการสร้างเส้นทางเฉพาะที่ติดต่อระหว่างโหนดที่ทำการโจมตีส่งผลให้สามารถติดต่อสื่อสารและส่งข้อมูลถึงกันได้โดยตรง การโจมตีแบบรูหนอนอาจทำให้เกิดการโจมตีลักษณะอื่นๆได้ง่ายมากยิ่งขึ้น เช่น การโจมตีแบบส่งซ้ำ การทำให้ข้อมูลหายไป เป็นต้น [28]

การโจมตีแบบส่งซ้ำ (Replay attack) โหนดจะทำการโจมตีด้วยการเก็บข้อความควบคุมที่ถูกต้องของโหนดอื่นๆ ที่เคยใช้ไปแล้วนำกลับมาใช้อีก ซึ่งการโจมตีแบบส่งซ้ำยากต่อการตรวจสอบเพราะโหนดในเครือข่ายมีการเคลื่อนที่อยู่ตลอดเวลา [29]

การโจมตีโดยไม่ปกปิดข้อมูล (Information Disclosure attack) เป็นการโจมตีทำให้ข้อมูลที่เป็นความลับของเครือข่ายเปิดเผยออกไปยังโหนดที่ไม่ได้รับสิทธิ์ เช่น รหัสผ่าน กุญแจที่ใช้ในการเข้ารหัส เป็นต้น [30]

การโจมตีโดยการแบ่งเครือข่าย (Partition attack) โหนดในเครือข่ายพยายามส่งข้อมูลเส้นทางปลอมให้กับโหนดอื่นๆ เพื่อทำการแบ่งเครือข่ายให้แยกออกจากกัน ทำให้โหนดในเครือข่ายไม่สามารถสร้างเส้นทางการสื่อสารถึงกันได้ [26]

การโจมตีแบบ Jellyfish คือการชะลอการส่งข้อมูลไปยังโหนดอื่น แต่กระบวนการในการค้นหาเส้นทางยังคงเหมือนเดิม การโจมตีในลักษณะนี้ทำให้เกิดเวลาหน่วง (Delay) ในเครือข่าย [31]

การโจมตีแบบ Blackmail การโจมตีนี้เกิดขึ้นได้เมื่อมีการกำหนดวิธีการเพื่อความปลอดภัย โหนดทำการโจมตีโดยประกาศว่าโหนดอื่นเป็นโหนดที่ทำการโจมตีในเครือข่าย เพื่อให้โหนดอื่นๆทำการขึ้นบัญชีดำ (Blacklist) ดังนั้นควรมีการป้องกัน เมื่อมีการออกแบบกระบวนการที่ให้สิทธิโหนดในการขึ้นบัญชีดำโหนดอื่น [24]

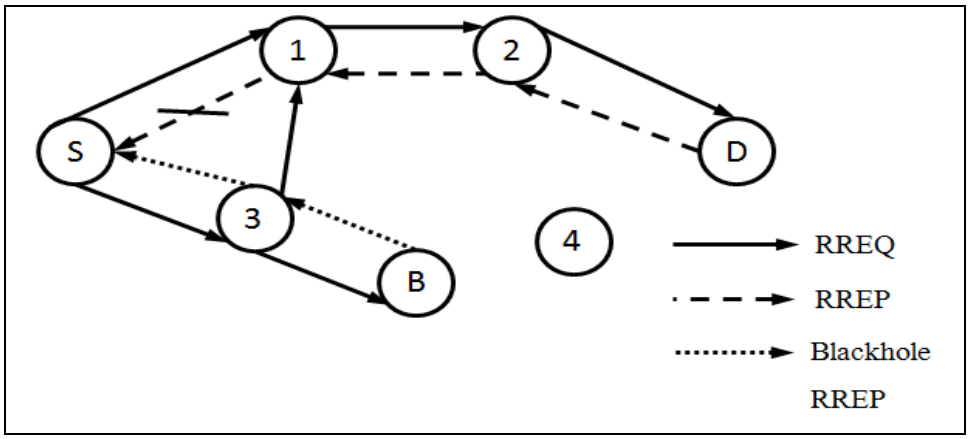
การโจมตีโดยโหนดเพื่อนบ้าน (Neighbor attack) เป็นการโจมตีโพรโทคอลที่มีการบันทึกหมายเลขโหนดเพื่อทำการสร้างเส้นทาง เมื่อโหนดได้รับข้อความควบคุมจะทำการส่งต่อไป โดยไม่มีการบันทึกหมายเลขโหนด ทำให้เมื่อมีการส่งข้อมูลทำให้เกิดการทิ้งข้อมูล เนื่องจากไม่สามารถส่งข้อมูลไปยังเส้นทางที่สร้างได้ [24]

อย่างไรก็ตาม เมื่อมีการโจมตีในระดับชั้นเครือข่าย ส่งผลทำให้สมรรถนะของระบบเครือข่ายไร้สายแบบ Ad hoc ลดลง โดยขึ้นอยู่กับความรุนแรงในการโจมตี และการจัดการด้านความปลอดภัยของโพรโทคอลการค้นหาเส้นทาง แต่การโจมตีโพรโทคอลการค้นหาเส้นทางที่ไม่มีการจัดการในด้านความปลอดภัย ยกตัวอย่างเช่น โพรโทคอลการค้นหาเส้นทาง AODV ที่มีการค้นหาเส้นทางแบบ Reactive เมื่อมีการโจมตีเกิดขึ้นจะไม่สามารถตรวจสอบหรือจัดการการโจมตีได้ โดยเฉพาะการโจมตีแบบหลุมดำเป็นการโจมตีที่เกิดขึ้นได้ง่ายในโพรโทคอลการค้นหาเส้นทาง AODV [32] และลดสมรรถนะของระบบเครือข่ายไร้สายแบบ Ad hoc เป็นอย่างมาก ซึ่งงานวิทยานิพนธ์นี้ทำการศึกษาการโจมตีแบบหลุมดำในโพรโทคอลการค้นหาเส้นทาง AODV และนำเสนอวิธีการแก้ปัญหาการโจมตีแบบหลุมดำด้วยโพรโทคอลการค้นหาเส้นทาง Credit based Ad hoc On-demand Distance Vector (CAODV)

บทที่ 3
การออกแบบและพัฒนาด้านความปลอดภัยบนโพรโทคอลการค้นหาเส้นทาง AODV

3.1 การโจมตีแบบหลุมดำในโพรโทคอลการค้นหาเส้นทาง AODV

การโจมตีแบบหลุมดำ เป็นการโจมตีในระดับเครือข่าย ที่มีเป้าหมายในการการขัดขวางการบริการ โดยทำการทิ้งข้อมูลของโหนดอื่นๆที่มีการใช้โหนดหลุมดำเป็นเส้นทางในการส่งข้อมูลทั้งหมด โดยการโจมตีแบบหลุมดำจะเกิดขึ้นได้ง่ายในกระบวนการค้นหาเส้นทางในโพรโทคอลการค้นหาเส้นทาง AODV เมื่อโหนดต้นทางต้องการทำการค้นหาเส้นทางไปยังโหนดปลายทาง โหนดต้นทางจะทำการกระจายข้อความควบคุม RREQ ไปยังโหนดอื่นๆ เมื่อโหนดหลุมดำ (Blackhole node) ได้รับข้อความควบคุม RREQ แล้วจะทำการส่งข้อความควบคุม RREP ที่มีข้อมูลเท็จกลับไปยังโหนดต้นทาง เมื่อโหนดต้นทางได้รับข้อความควบคุม RREP ของโหนดหลุมดำ เมื่อตรวจสอบข้อมูลที่ได้รับจะพบว่าได้รับข้อมูลเส้นทางที่ดี คือมีจำนวนโหนดที่ใช้ส่งข้อมูลน้อย และมีเลขลำดับปลายทางที่มีค่ามาก ดังนั้นโหนดต้นทางจะทำการสร้างเส้นทางการสื่อสารไปยังโหนดหลุมดำและทำการส่งข้อมูลไปยังโหนดปลายทาง เมื่อโหนดหลุมดำได้รับข้อมูลจะทำการทิ้งข้อมูลทั้งหมด ส่งผลให้โหนดปลายทางไม่ได้รับข้อมูล โดยแสดงตัวอย่างการโจมตีแบบหลุมดำในรูปที่ 3.1

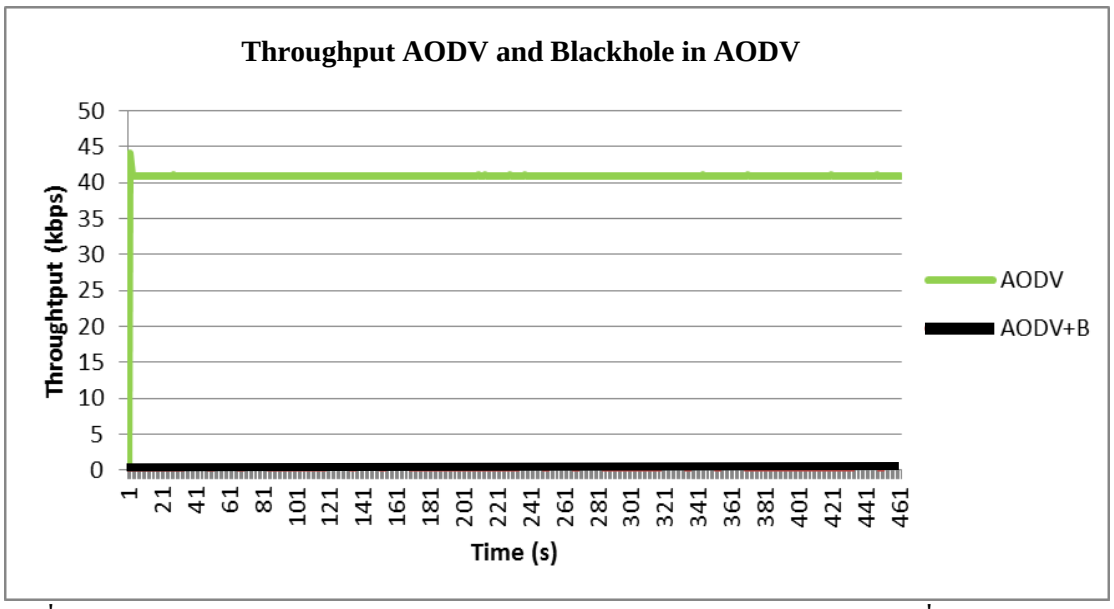


รูปที่ 3.1 การโจมตีแบบหลุมดำในโพรโทคอลการค้นหาเส้นทาง AODV

ตัวอย่างการโจมตีแบบหลุมดำในโพรโทคอลการค้นหาเส้นทาง AODV ในรูปที่ 3.1 โดยโหนด S เป็นโหนดต้นทาง โหนด D เป็นโหนดปลายทาง และโหนด B เป็นโหนดหลุมดำ เมื่อโหนด S

ต้องการเส้นทางในการส่งข้อมูล โหนด S จะเริ่มกระบวนการค้นหาเส้นทาง โดยทำการกระจายข้อความควบคุม RREQ ไปยังโหนดเพื่อนบ้านคือ โหนด 1 และโหนด 3 เมื่อโหนดได้รับข้อความควบคุม RREQ จะตรวจสอบข้อมูลเส้นทางในตารางเส้นทาง เมื่อไม่มีข้อมูลโหนดจะทำการกระจายข้อความควบคุม RREQ เมื่อโหนด B ซึ่งเป็นโหนดหลุมดำได้รับข้อความควบคุม RREQ จะทำการตอบกลับด้วยข้อความควบคุม RREP ที่มีข้อมูลปลอม โดยกำหนดค่าเลขลำดับปลายทางสูง และกำหนดค่าจำนวนโหนดที่ใช้ในการส่งข้อมูลเป็น 1 ซึ่งหมายความว่าโหนดปลายทางเป็นโหนดเพื่อนบ้าน ส่งไปยังโหนด 3 เมื่อโหนด S ได้รับจะทำการตรวจสอบเลขลำดับปลายทางและจำนวนโหนดที่ใช้ในการส่งข้อมูล จากนั้นทำการเพิ่มข้อมูลเส้นทางลงในตารางข้อมูลเส้นทาง และเริ่มส่งข้อมูลตามเส้นทางไปยังโหนด B เมื่อได้รับข้อมูลจะทำการการทิ้งข้อมูลทั้งหมด ในช่วงเวลาที่โหนด 3 กระจายข้อมูลควบคุม RREQ โหนด 1 ได้กระจายข้อความควบคุม RREQ ไปยังโหนดเพื่อนบ้านคือโหนด 2 จากนั้นโหนด 2 กระจายข้อความควบคุม RREQ ต่อไปยังโหนด D ที่เป็นปลายทาง เมื่อโหนด D ได้รับข้อความควบคุม RREQ จะทำการตอบกลับด้วยข้อความควบคุม RREP ที่มีค่าเลขลำดับปลายทางเท่ากับค่าเลขลำดับของโหนด D เอง และจำนวนโหนดที่ใช้ส่งข้อมูลเป็น 0 ส่งกลับไปยังโหนด 2 โหนด 1 และกลับไปยังโหนด S เมื่อโหนด S ได้รับข้อความควบคุม RREP จากโหนด 1 จะเปรียบเทียบค่าเลขลำดับปลายทางกับข้อมูลเส้นทางในตารางข้อมูล ในกรณีนี้โหนด S จะไม่ทำการแก้ไขข้อมูลในตารางเส้นทางเพราะเลขลำดับปลายทางต่ำกว่าเลขลำดับปลายทางที่ได้จากข้อความควบคุม RREP ที่มีข้อมูลปลอม ดังนั้นโหนด S จะทำการทิ้งข้อความควบคุม RREP จากโหนด 1 เนื่องจากถือว่าเป็นข้อมูลเก่า ส่งผลให้การส่งข้อมูลโหนด S ไปยังโหนด D ไม่ได้รับการบริการ

โพรโทคอลการค้นหาเส้นทาง AODV แสดงให้เห็นว่าไม่มีการตรวจสอบความถูกต้องในข้อความควบคุมส่งผลทำให้ง่ายต่อการเกิดการโจมตีแบบหลุมดำ และเมื่อเกิดการโจมตีแล้วยังไม่สามารถตรวจสอบหรือแก้ไขได้ ดังนั้นการโจมตีแบบหลุมดำจึงส่งผลให้สมรรถนะการให้บริการของเครือข่ายไร้สายแบบ Ad hoc ลดลงเป็นอย่างมาก โดยทำการทดสอบโดยใช้เครือข่ายไร้สายแบบ Ad hoc ในรูปที่3.1 โดยมีโหนด S เป็นโหนดต้นทาง โหนด D เป็นโหนดปลายทาง โดยมีเส้นทางการสื่อสาร 2 เส้นทาง โดยมีโหนด B ทำการโจมตีแบบหลุมดำ และแสดงผลกระทบจากการโจมตีดังรูปที่ 3.2

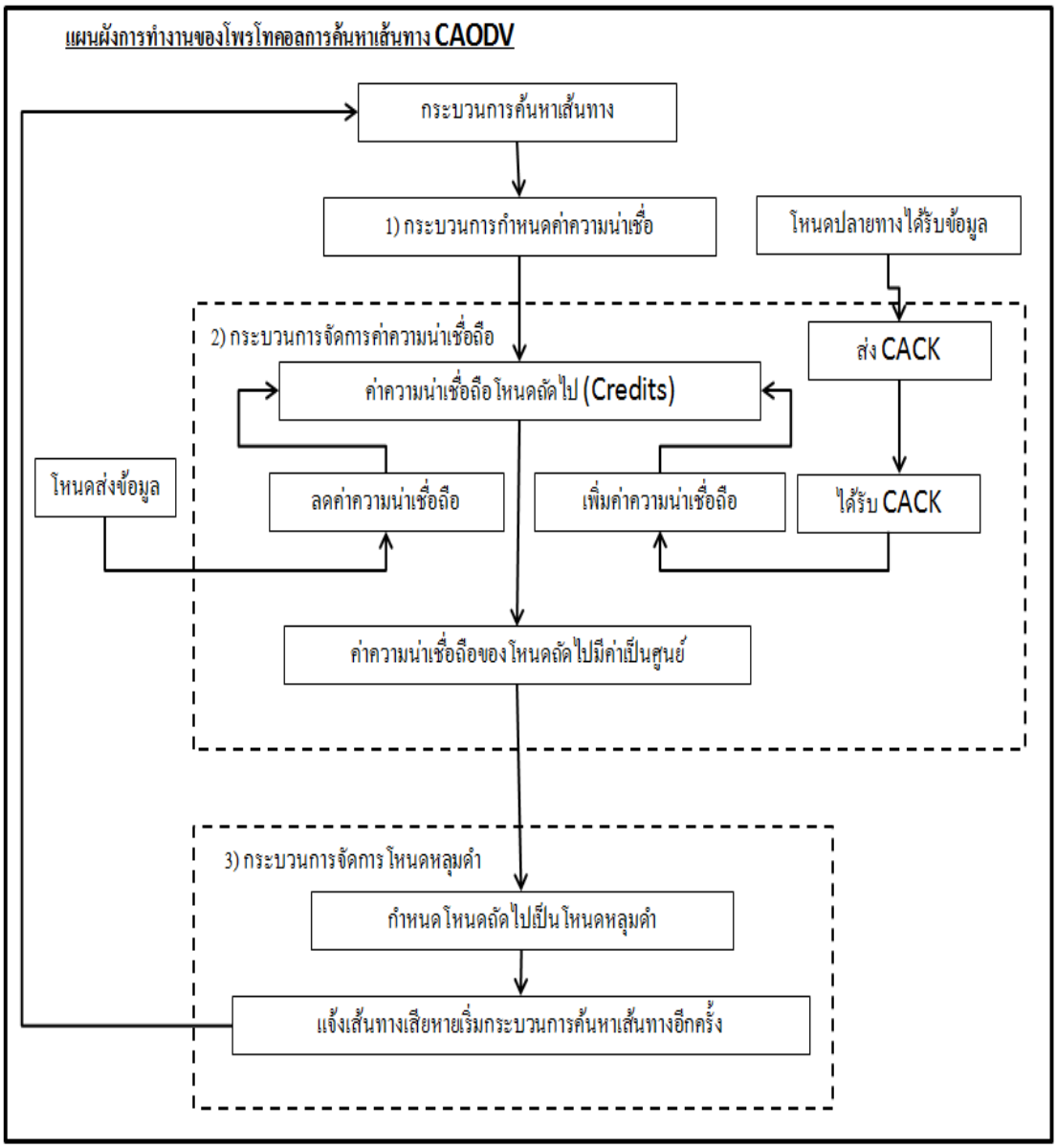


รูปที่ 3.2 ค่าสมรรถนะของโพรโทคอลการค้นหาเส้นทาง AODV ทำงานปกติและเมื่อมีการโจมตี

จากรูปที่ 3.2 ค่าสมรรถนะของเครือข่ายไร้สายแบบ Ad hoc เมื่อมีโหนดหลุมดำในเครือข่ายทำการโจมตี ส่งผลทำให้ค่าสมรรถนะการทำงานของเครือข่ายที่มีรูปทรงเครือข่ายดังรูปที่ 3.1 จนโหนดต้นทางไม่สามารถส่งข้อมูลไปยังโหนดปลายทางได้ จึงส่งผลทำให้ค่าสมรรถนะของเครือข่ายเป็น 0 ซึ่งเป็นผลกระทบที่รุนแรงมากจนเครือข่ายไม่สามารถให้บริการได้ ดังนั้นงานวิทยานิพนธ์นี้จึงนำเสนอกระบวนการที่พัฒนาโพรโทคอลการค้นหาเส้นทาง AODV โดยการใช้ระบบการให้ความน่าเชื่อถือแก่โหนดถัดไป (Credit) เพื่อเป็นเป็นการป้องกันการโจมตีแบบหลุมดำและการโจมตีที่มีลักษณะขัดขวางการให้บริการ โดยเรียกโพรโทคอลนี้ว่า โพรโทคอลการค้นหาเส้นทาง CAODV

3.2 การออกแบบและการพัฒนาด้านความปลอดภัยบนโพรโทคอลการค้นหาเส้นทาง AODV

การโจมตีแบบหลุมดำเป็นการโจมตีที่มุ่งเน้นในการขัดขวางการให้บริการของเครือข่าย ดังนั้นเป้าหมายของการป้องกันการโจมตีแบบหลุมดำต้องทำให้เครือข่ายไร้สายแบบ Ad hoc สามารถให้บริการได้เมื่อถูกโจมตีแบบหลุมดำเกิดขึ้น วิทยานิพนธ์นี้จึงทำการออกแบบ และพัฒนากระบวนการที่ทำการกำหนดและควบคุมการรับส่งข้อมูลด้วยการใช้ระบบการให้ความน่าเชื่อถือแก่โหนดถัดไปโดยเรียกว่า โพรโทคอลนี้ว่าโพรโทคอลการค้นหาเส้นทาง CAODV โดยประกอบด้วยขั้นตอนการทำงาน 3 ขั้นตอน คือ (1) กระบวนการกำหนดความน่าเชื่อถือโหนดถัดไป (2) กระบวนการจัดการค่าความน่าเชื่อถือโหนดถัดไป และ (3) กระบวนการจัดการกับโหนดหลุมดำ ซึ่งสามารถเขียนเป็นลำดับการทำงานได้ดังนี้

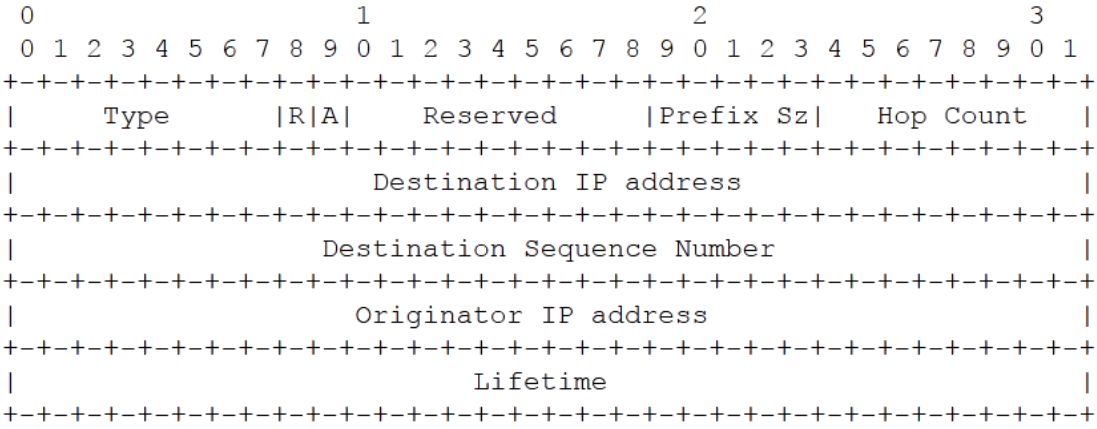


รูปที่ 3.3 แผนผังการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV

จากรูปที่ 3.3 แผนผังขั้นตอนการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV จะเริ่มต้นก็ต่อเมื่อโหนดต้นทางสามารถสร้างเส้นทางการสื่อสารไปยังโหนดปลายทางได้ โดยกระบวนการการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV จะใช้กระบวนการการค้นหาเส้นทางเดียวกับโพรโทคอลการค้นหาเส้นทาง AODV โดยใช้ข้อความควบคุม RREQ และ RREP ในการสร้างเส้นทาง เมื่อสามารถสร้างเส้นทางการสื่อสารได้ โหนดในเส้นทางการสื่อสารทั้งหมดที่ได้รับข้อความควบคุม RREP จะทำการกำหนดความน่าเชื่อถือให้แก่โหนดถัดไป โดยการ

ใช้ข้อมูลในส่วนของจำนวนโหนดที่ใช้ในการส่งข้อมูลในการเป็นตัวแปรในการกำหนดความน่าเชื่อถือแก่โหนดถัดไป โดยกำหนดให้ค่าความน่าเชื่อถือมีค่าเป็นสามเท่าของจำนวนโหนดที่ใช้ในการส่งข้อมูล เนื่องจากโหนดที่มีจำนวนโหนดในการส่งข้อมูลจำนวนมากมีโอกาสเกิดการสูญหายและการชนกันของข้อมูล (Collision) มากกว่าโหนดที่ใช้จำนวนโหนดในการส่งข้อมูลจำนวนน้อย เมื่อกำหนดค่าความน่าเชื่อถือของโหนดถัดไปได้ จากนั้นโพรโทคอลการค้นหาเส้นทาง CAODV จะเริ่มกระบวนการจัดการค่าความน่าเชื่อถือโหนดถัดไป โดยกระบวนการนี้จะดำเนินการในช่วงของการรับและส่งข้อมูล

กระบวนการจัดการค่าความน่าเชื่อถือจะเริ่มขึ้นเมื่อโหนดต้นทางทำการส่งข้อมูลไปยังโหนดปลายทาง เมื่อโหนดในเส้นทางการสื่อสารทำการส่งข้อมูลจะทำการลดค่าความน่าเชื่อถือแก่โหนดถัดไปโดยจะทำการลดค่าความน่าเชื่อถือเป็นสัดส่วน 1:1 หมายความว่าเมื่อโหนดทำการส่งข้อมูล 1 แพ็กเก็ต (Packet) จะทำการลดค่าความน่าเชื่อถือ 1 เช่นเดียวกัน ดังนั้นอัตราการส่งข้อมูลให้โหนดถัดไปจะถูกกำหนดโดยจำนวนค่าความน่าเชื่อถือโหนดถัดไป เมื่อโหนดปลายทางได้รับข้อมูลจะทำการส่งข้อความควบคุมกลับไปคือ ข้อความควบคุม Credit Acknowledge (CACK) โดยได้ทำการดัดแปลงจากข้อความควบคุม RREP โดยได้ทำการเพิ่มและเปลี่ยนแปลงหน้าที่ของส่วนข้อมูล โดยรูปที่ 3.4 แสดงรูปแบบโครงสร้างของข้อความควบคุม RREP



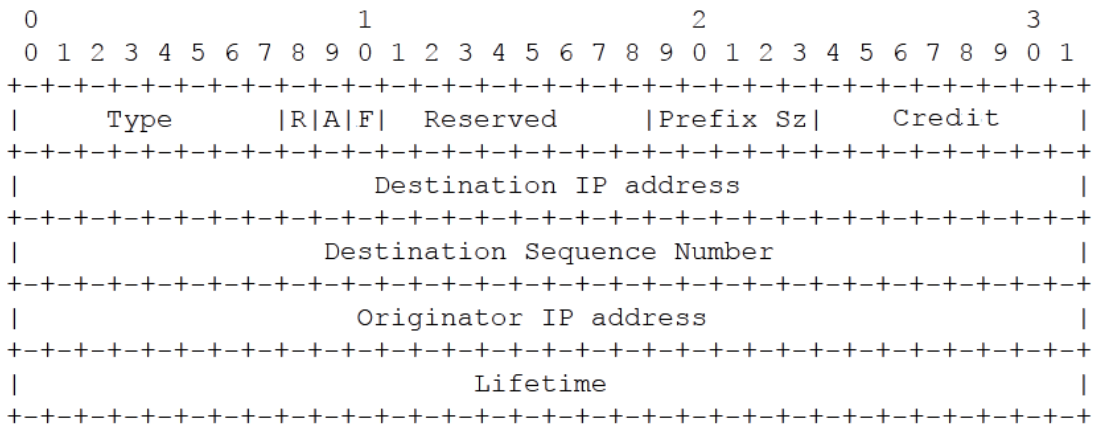
รูปที่ 3.4 รูปแบบโครงสร้างของข้อความควบคุม RREP [4]

ข้อความควบคุม RREP มีขนาด 160 บิต โดยประกอบไปด้วยส่วนของข้อมูลที่มีหน้าที่แตกต่างกันดังตารางที่ 3.1

ตารางที่ 3.1 รายละเอียดแต่ละส่วนภายในข้อความ RREP

ข้อมูลที่จัดเก็บ	**ความหมาย**
Type	ประเภทของข้อความควบคุม ซึ่งในที่นี้ Type = 2 หมายถึง RREP
R	Repair Flag ใช้สำหรับการส่งแบบกระจาย
A	Acknowledgement required เป็นตัวแปรกำหนดว่าข้อความ RREP ดังกล่าวมีความต้องการในการตอบกลับ เมื่อได้รับ RREP แล้ว
Reserved	พื้นที่สงวนขนาด 8 บิต มีค่าเป็น 0 โดยโหนดจะไม่สนใจข้อมูลในส่วนนี้
Prefix Size	ถ้า Prefix size ไม่เป็น 0 แล้ว 5-bit ในข้อมูลของ Prefix size จะเป็นตัวกำหนดหมายเลขของโหนดถัดไปที่ถูกใช้สำหรับทุกๆ โหนดด้วยเส้นทางในการส่งข้อมูลเส้นทางเดียวกัน
Hop count	จำนวนของโหนดที่ใช้ในการส่งต่อข้อมูลจากต้นทางจนกระทั่งถึงปลายทาง
Destination IP Address	เลขที่อยู่ของโหนดปลายทาง
Destination Sequence Number	หมายเลขลำดับล่าสุดที่เกี่ยวข้องกับเส้นทางสื่อสาร
Originator IP Address	หมายเลขของโหนดต้นทางที่สร้างข้อความ RREQ หรือโหนดต้นทาง
Lifetime	เวลาอายุของข้อความควบคุม RREP

ข้อความควบคุม CACK จะทำการดัดแปลงรูปแบบจากข้อความควบคุม RREP โดยใช้พื้นที่สงวน (Reserved) ของข้อความควบคุม RREP ขนาด 1 บิต เพื่อเป็นการแยกระหว่างข้อความควบคุม CACK และ RREP โดยกำหนดให้มีในกรณีที่เป็นข้อความ RREP ข้อมูลจะเป็น 0 แต่ข้อความควบคุม CACK จะเป็น 1 และเปลี่ยนหน้าที่ในส่วนของ Hop Count ให้ทำหน้าที่ในการระบุค่าความน่าเชื่อถือ โดยมีรูปแบบดังรูปที่ 3.5 รูปแบบโครงสร้างของข้อความควบคุม CACK



รูปที่ 3.5 รูปแบบโครงสร้างของข้อความควบคุม CACK [4]

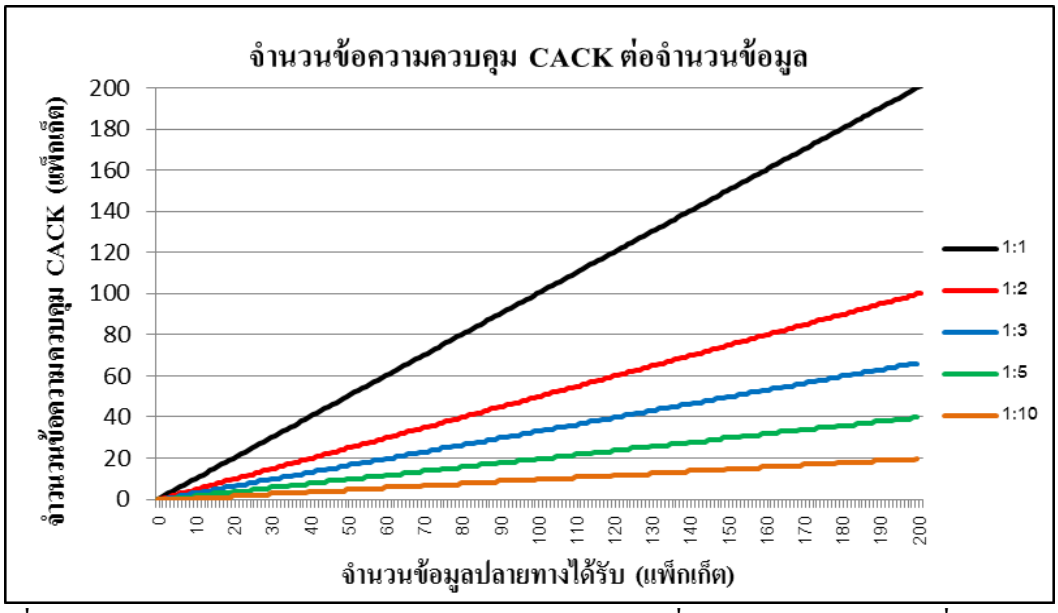
จากรูปที่ 3.5 ข้อความควบคุม CACK ในส่วนบิตที่ 10 ระบุค่าเป็น 1 และมีค่าความน่าเชื่อถือระบุในบิตที่ 24 ถึง 31 โดยข้อความควบคุม CACK จะทำหน้าที่แจ้งกลับไปในเส้นทางการสื่อสารเพื่อให้โหนดในเส้นทางทราบว่าโหนดปลายทางได้รับข้อมูลเสร็จสิ้น เมื่อโหนดในเส้นทางได้รับข้อความควบคุม CACK จะทำการเพิ่มค่าความน่าเชื่อถือให้แก่โหนดถัดไป ดังนั้นในกรณีที่โหนดปลายทางได้รับข้อมูล ค่าความน่าเชื่อถือโหนดถัดไปของโหนดในเส้นทางการสื่อสารจะเพิ่มขึ้นเรื่อยๆจนกระทั้งเข้าสู่สภาวะเสถียรของค่าความน่าเชื่อถือ โดยจะกำหนดให้ค่าความน่าเชื่อถือมีค่าที่จำกัด โดยจะมีค่าสูงสุดแตกต่างในแต่ละโหนด (อธิบายในหัวข้อ 3.3) ซึ่งค่าดังกล่าวจะทำให้ในกรณีที่เกิดการโจมตีเมื่อทำการส่งข้อมูลไประยะหนึ่งแล้วเกิดการโจมตีเกิดขึ้นจากโหนดในเส้นทาง ดังนั้นการจำกัดค่าความน่าเชื่อถือจึงเป็นการจำกัดผลกระทบจากการโจมตีไปอีกทางหนึ่งด้วย และเมื่อในกรณีที่โหนดในเส้นทางไม่ได้รับข้อความควบคุม CACK จากโหนดปลายทางเมื่อโหนดในเส้นทางทำการส่งข้อมูลจะทำการลดค่าความน่าเชื่อถือลงเรื่อยๆ จนกระทั้งค่าความน่าเชื่อถือของโหนดถัดไปลดลงเป็นศูนย์ โหนดจะเริ่มกระบวนการจัดการกับโหนดหลุมดำ

กระบวนการจัดการกับโหนดหลุมดำจะเกิดขึ้นเมื่อโหนดต้นทางหรือโหนดในเส้นทางพบว่าค่าความน่าเชื่อถือแก่โหนดถัดไปลดลงเป็นศูนย์ โหนดจะทำการกำหนดว่าโหนดถัดไปไม่มีความน่าเชื่อถือโดยโหนดจะไม่สนใจข้อความควบคุมจากโหนดที่ไม่มีความน่าเชื่อถือ จากนั้นโหนดที่พบโหนดที่มีความไม่น่าเชื่อจะทำการแจ้งเส้นทางเสียหายเพื่อเริ่มกระบวนการค้นหาเส้นทางอีกครั้ง ส่วนที่สำคัญของโพรโทคอลการค้นหาเส้นทาง CAODV คือกระบวนการจัดการค่าความน่าเชื่อ โดยเฉพาะในส่วนของการเพิ่มและลดค่าของความน่าเชื่อถือ ดังนั้นในหัวข้อ 3.3 เสนอการออกแบบและกำหนดลักษณะของการจัดการค่าความน่าเชื่อถือในโพรโทคอลการค้นหาเส้นทาง CAODV

3.3การออกแบบและการพัฒนากระบวนการจัดการค่าความน่าเชื่อถือในโพรโทคอลการค้นหาเส้นทาง CAODV

โพรโทคอลการค้นหาเส้นทาง CAODV สามารถแบ่งกระบวนการทำงานเป็น 3 ส่วน ซึ่งกระบวนการจัดการค่าความน่าเชื่อถือเป็นส่วนที่มีความสำคัญมากที่สุดในโพรโทคอลการค้นหาเส้นทาง CAODV โดยจะใช้การส่งข้อมูลและการรับข้อความควบคุม CACK ในการลดและเพิ่มค่าความน่าเชื่อถือตามลำดับ แต่อย่างไรก็ตามการใช้ข้อความควบคุม CACK ถือเป็นการเพิ่มภาระงานให้เครือข่ายจากเดิม ดังนั้นจึงจำเป็นต้องมีการจัดการและควบคุมปริมาณการส่งข้อความควบคุม CACK เพื่อให้เครือข่ายไร้สายแบบ Ad hoc มีสมรรถนะการทำงานเทียบเท่ากับโพรโทคอลการค้นหาเส้นทาง AODV เมื่อเครือข่ายไม่ได้ถูกโจมตีและสามารถจัดการและลดผลกระทบจากการโจมตีแบบหลุมดำได้

กระบวนการจัดการค่าความน่าเชื่อถือในโพรโทคอลการค้นหาเส้นทาง CAODV มีเป้าหมายหลักคือ โหนดสามารถกำหนดและควบคุมจำนวนข้อมูลที่ส่งให้กับโหนดถัดไปโดยจะขึ้นอยู่กับค่าความน่าเชื่อถือจำกัดผลกระทบจากการโจมตี แต่การใช้ค่าความน่าเชื่อถือนั้นต้องแลกกับการเพิ่มภาระงานดังรูปที่ 3.6 แสดงค่าภาระงานของการส่งข้อมูลเมื่อมีการกำหนดการส่งข้อความควบคุม CACK ในอัตราที่แตกต่างกัน



รูปที่ 3.6 จำนวนข้อความควบคุมเปรียบเทียบต่อจำนวนข้อมูลที่ได้รับในอัตราสัดส่วนที่แตกต่างกัน

จากรูปที่ 3.6 แสดงความสัมพันธ์ระหว่างจำนวนข้อความควบคุม CACK เปรียบเทียบกับจำนวนข้อมูลที่โหนดปลายทางได้รับ โดยเปรียบเทียบในอัตราการส่งข้อความคุม

CACK กับจำนวนข้อมูลโดยมี 5 อัตราส่วนคือ โหนดปลายทางส่งข้อความควบคุม CACK กลับเมื่อได้รับข้อมูล 1 แพ็กเก็ต (1:1) 2 แพ็กเก็ต (1:2) 3 แพ็กเก็ต (1:3) 5 แพ็กเก็ต (1:5) และ 10 แพ็กเก็ต (1:10) พบว่าจำนวนภาระงานจะเพิ่มขึ้นตามอัตราการส่งข้อความควบคุม CACK โดยสามารถคำนวณเป็นอัตราได้ดังนี้

$$N = m*p \qquad \text{(สมการที่ 3.1)}$$

โดยให้ N เป็นจำนวนข้อความควบคุม CACK
m เป็นอัตราส่วนการส่งข้อความควบคุม CACK
p เป็นจำนวนข้อมูลที่โหนดปลายทางได้รับ

จำนวนข้อความควบคุม CACK ซึ่งเป็นภาระงานที่เพิ่มขึ้นจากโพรโทคอลการค้นหาเส้นทาง AODV จะขึ้นอยู่กับอัตราส่วนในการส่งข้อความควบคุม CACK ดังนั้นงานวิจัยนี้จึงออกแบบการส่งข้อความควบคุม CACK เพื่อลดภาระงานของเครือข่ายไร้สายแบบ Ad hoc ลงจากอัตราส่วนตามสมการเชิงเส้นเปลี่ยนเป็นอยู่ในรูปแบบเงื่อนไข โดยในช่วงการเริ่มต้นของการส่งข้อมูล ซึ่งค่าความน่าเชื่อถือโหนดถัดไปต่ำ ดังนั้นในเริ่มแรกกำหนดให้โหนดปลายทางส่งข้อความควบคุมด้วยความถี่ที่สูง โดยกำหนดอัตราเป็น 1:1 จากนั้นจึงลดอัตราส่วนในการส่งข้อความควบคุม CACK ลง เป็น 1:2 1:4 และ1:8 ตามลำดับ ตามสมการที่ 3.2

$$\text{Credit} = \begin{cases} \text{Hop\_count}*3 & \text{; ค่าความน่าเชื่อถือเริ่มต้น} \\ \text{Credit}-1 & \text{; เมื่อส่งข้อมูล 1 แพ็กเก็ต} \\ \text{Credit}+\text{CACK\_credit} & \text{; เมื่อได้รับข้อความควบคุม CACK} \\ \text{Credit\_limit} & \text{; เมื่อ Credit} > \text{Credit\_limit} \end{cases} \qquad \text{(สมการที่ 3.2)}$$

โดย Credit คือค่าความน่าเชื่อถือโหนดถัดไป

Hop_count คือจำนวนโหนดที่ใช้ในการส่งข้อมูล

Credit_limit คือค่าสูงสุดของค่าความน่าเชื่อถือโหนดถัดไปซึ่งมีค่าตามสมการ 3.3

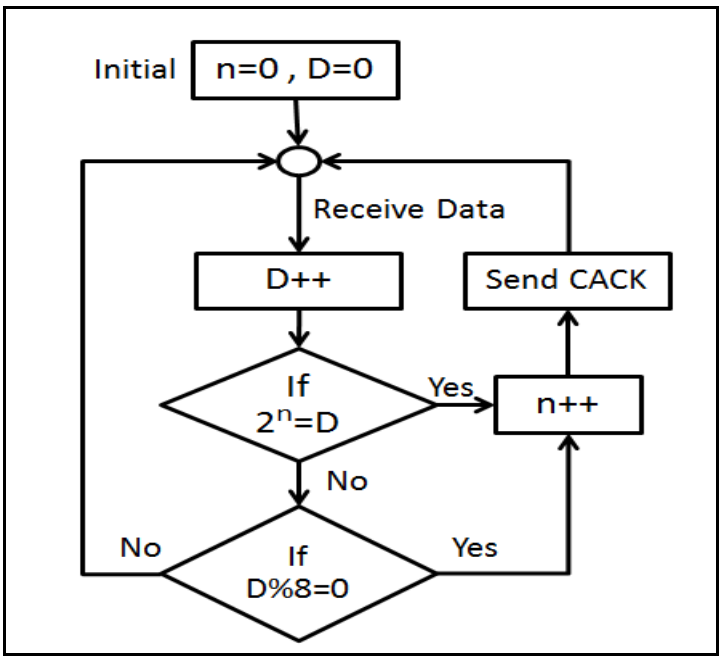
$$\text{Credit\_limit} = (\text{Hop\_count}+2)*5 \qquad \text{(สมการที่ 3.3)}$$

CACK_credit คือค่าความน่าเชื่อถือที่ถูกกำหนดอยู่ใน CACK ที่ได้รับ โดยกำหนดค่าความน่าเชื่อถือตามสมการ 3.4

$$CACK\_Credit = \begin{cases} 2 & ; \text{เมื่อ } n = 1 \\ 3 & ; \text{เมื่อ } n = 2 \\ 5 & ; \text{เมื่อ } n = 3 \\ 9 & ; \text{เมื่อ } n >= 4 \end{cases} \qquad \text{(สมการที่ 3.4)}$$

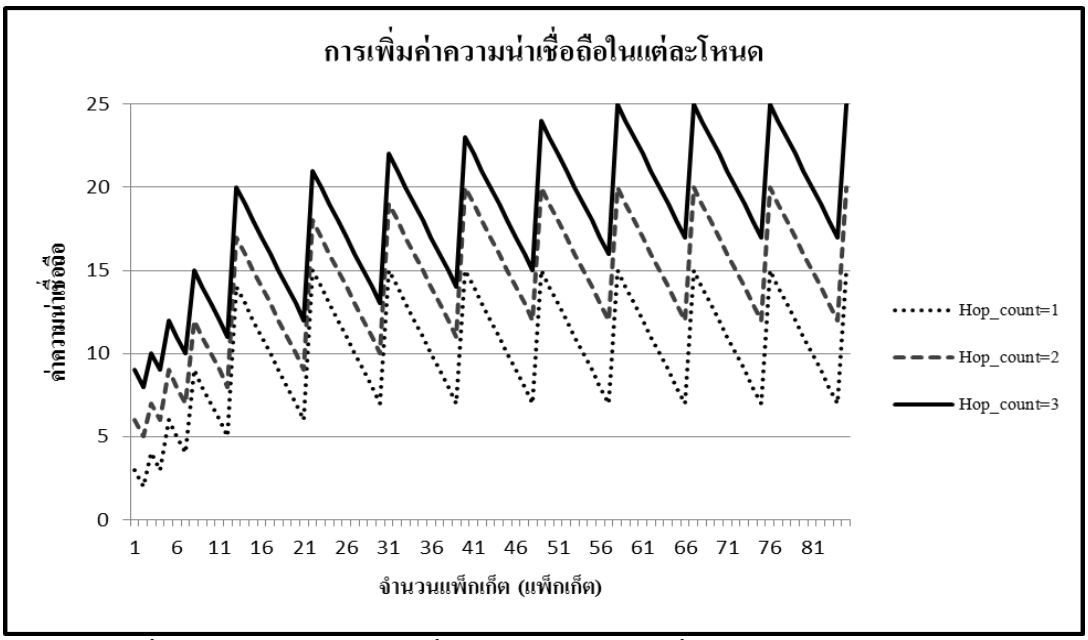
โดยกำหนดให้ n คือ จำนวนครั้งที่ส่งข้อความควบคุม CACK

การกำหนดค่าความน่าเชื่อถือเริ่มต้นเป็น Hop_count*3 เนื่องจากในเครือข่ายไร้สายแบบ Ad hoc มีโอกาสที่จะมีข้อมูลสูญหายอยู่เสมอ ดังนั้นจึงกำหนดให้โหนดที่มีจำนวนโหนดในการส่งข้อมูลค่าความน่าเชื่อถือเริ่มต้นที่ต่ำที่สุดเป็น 3 และมากขึ้นตามจำนวนโหนดที่ใช้ในการส่งข้อมูล และการกำหนดค่าสูงสุดของความน่าเชื่อถือดังสมการที่ 3.3 โดยเป็นการจำกัดค่าความน่าเชื่อถือไม่ให้มีมากเกินไป ในกรณีที่มีความน่าเชื่อถือมากจนเกินไป ส่งผลทำให้เครือข่ายไม่สามารถจัดการกับการโจมตีแบบหลุมดำได้อย่างทันที ประกอบกับการออกแบบการเพิ่มขึ้นของค่าความน่าเชื่อถือดังสมการที่ 3.4 มีการเพิ่มค่าความน่าเชื่อถือสูงสุดคือ 9 และมีการส่งข้อความควบคุม CACK แบบมีเงื่อนไข โดยกระบวนการนี้ ได้นำรูปแบบของหน้าต่างในการจัดการการตอบกลับของ ACK ในโพรโทคอล TCP (Transmission Control Protocol) [33] มาประยุกต์ใช้ในการตอบกลับของข้อความควบคุม CACK แต่กำหนดขนาดหน้าต่างของ CACK ให้มีขนาดสูงสุดคือ 8 ซึ่งหมายความว่าจะมีการตอบกลับช้าที่สุดคือทุก 8 ข้อมูลที่ได้รับ แต่อย่างไรก็ตามรูปแบบการเพิ่มขึ้นของหน้าต่างจะค่อยๆเพิ่มขึ้นดังรูปที่ 3.5ที่แสดงความสัมพันธ์ในการส่งข้อความควบคุม CACK กับจำนวนข้อมูลที่โหนดปลายทางได้รับ โดยกำหนดให้ตัวแปร D คือ จำนวนทั้งหมดที่ข้อมูลโหนดปลายทางที่ได้รับ

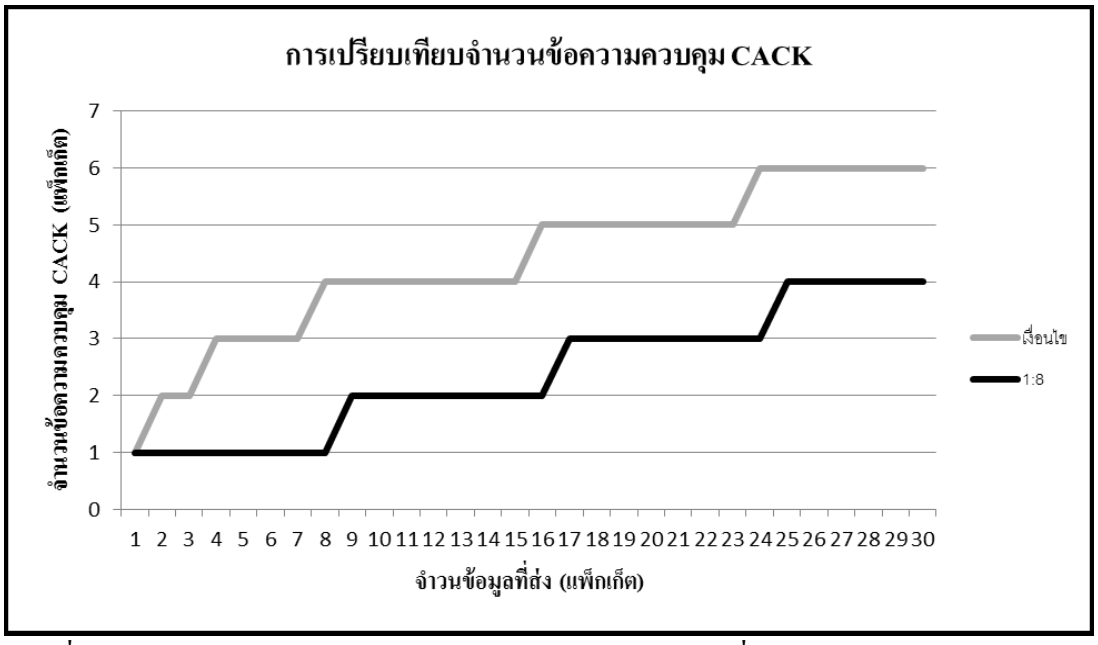


รูปที่ 3.7 ความสัมพันธ์ในการส่งข้อความควบคุม CACK และจำนวนข้อมูลที่โหนดปลายทางได้รับ

จากสมการที่ 3.2 การเพิ่มค่าความน่าเชื่อถือจะเพิ่มขึ้นตามเงื่อนไขของสมการที่ 3.4 และรูปที่ 3.7 โดยการเพิ่มค่าความน่าเชื่อถือจะเพิ่มขึ้นและลดอัตราในการส่ง CACK เพื่อลดการเพิ่มขึ้นของภาระงานในโพรโทคอลการค้นหาเส้นทาง CAODV ซึ่งตัวอย่างการเพิ่มค่าความน่าเชื่อถือของแต่ละโหนดแสดงในรูปที่ 3.5 และเปรียบเทียบกับอัตราส่วน 1:8 ในรูปที่ 3.8

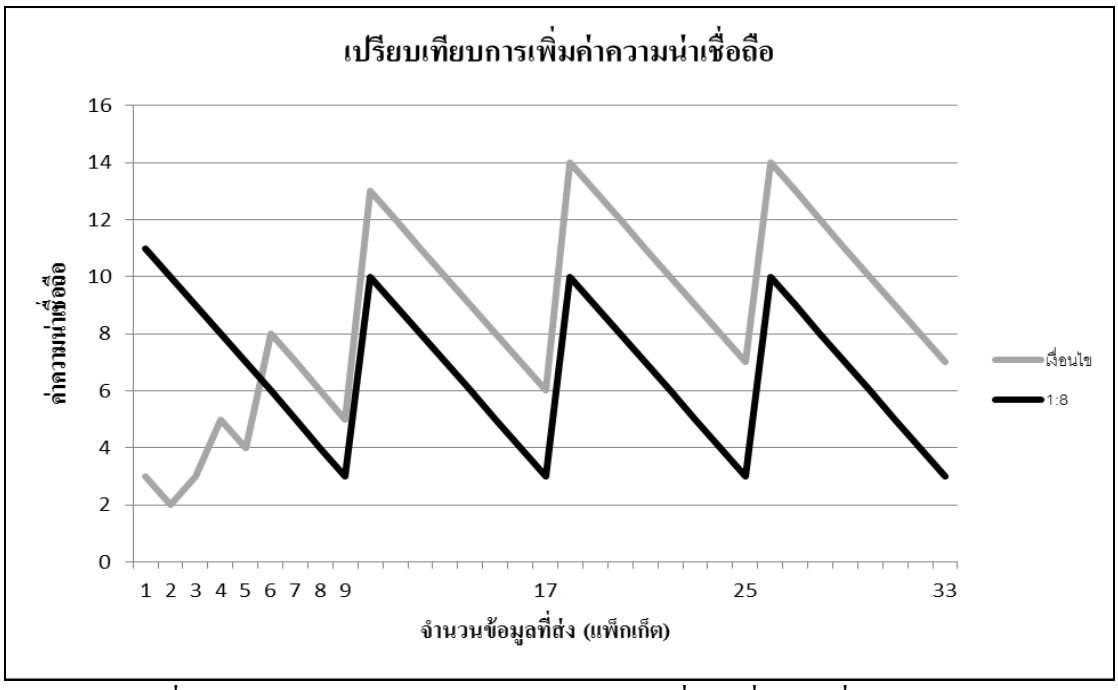


รูปที่ 3.8 การเพิ่มค่าความน่าเชื่อถือในแต่ละโหนดเมื่อไม่มีการสูญหายของข้อมูล



รูปที่ 3.9 การเปรียบเทียบจำนานข้อความควบคุม CACK แบบมีเงื่อนไข และส่งในอัตราส่วน 1:8

จากรูปที่ 3.8 แสดงการเพิ่มค่าของค่าความน่าเชื่อถือในโหนดต่างๆในเส้นทาง ประกอบด้วย โหนดที่มี Hop_count =1 ซึ่งเป็นโหนดที่ติดต่อโหนดปลายทางโดยตรง Hop_count = 2 และ Hop_count = 3 ซึ่งเป็นโหนดที่ถัดมาตามลำดับ โดยในช่วงแรกของการติดต่อสื่อสาร โหนดในเส้นทางจะกำหนดค่าความเชื่อถือโหนดถัดไปต่ำและค่อยๆเพิ่มขึ้นเมื่อได้รับข้อความควบคุม CACK จากโหนดปลายทาง โดยค่าความน่าเชื่อถือที่เพิ่มจะเพิ่มขึ้นตามลำดับตามตารางที่ 1 และจะเข้าสู่สภาวะเสถียรที่ค่า Credit_limit เพื่อเป็นการจำกัดการสูญเสียข้อมูลเมื่อเกิดการโจมตีและเมื่อเปรียบเทียบภาระงานในรูปที่ 3.9 ค่าภาระงานของการส่งข้อความควบคุม CACK แบบมีเงื่อนไขเพิ่มขึ้นมากกว่าการส่งข้อความควบคุม CACK แบบสัดส่วน 1:8 อยู่เพียง 2-3 แพ็กเก็ตเท่านั้น แต่ลักษณะการจัดการค่าความน่าเชื่อถือมีประสิทธิภาพสูงกว่าซึ่งแสดงในรูปที่ 3.7



รูปที่ 3.10 การเปรียบเทียบการจัดการค่าความน่าเชื่อถือที่โหนดที่มี Hop_count = 1

เมื่อเปรียบเทียบการจัดการค่าความน่าเชื่อถือที่โหนดที่มี Hop_count = 1 ในรูปที่ 3.10 การจัดการค่าความน่าเชื่อถือในการส่งข้อความควบคุม CACK แบบมีเงื่อนไข ในช่วงเริ่มต้นค่าความน่าเชื่อถือต่ำ โดยจะมีค่าเท่ากับ Hop_count*3 ซึ่งในรูปเป็นโหนดที่มี Hop_count = 1 ค่าความน่าเชื่อถือจึงเริ่มต้นที่ค่า 3 ส่วนกรณีการส่งข้อความควบคุม CACK กลับในรูปแบบอัตราส่วน 1:8 จะมีค่าความน่าเชื่อถือที่ค่า (1/m)+(Hop_count*3) ซึ่งได้ค่าความน่าเชื่อถือเป็น 11 เพราะจำเป็นต้องรอการตอบกลับของข้อความควบคุม CACK เมื่อมีการโจมตีจะส่งผลกระทบที่สูงกว่า และการเพิ่มค่าความน่าเชื่อถือในแบบมีเงื่อนไขจะทำการรับข้อความควบคุม CACK ตั้งแต่การส่งข้อมูลแพ็กเก็ตแรก ซึ่งแตกต่างกับการส่งข้อความควบคุม CACK แบบอัตราส่วน 1:8 ซึ่งจะได้รับข้อความควบคุม CACK เมื่อมีการส่งไปแล้ว 8 แพ็กเก็ต ดังนั้นโพรโทคอล CAODV จะทำการเพิ่มค่าความน่าเชื่อถือในรูปแบบของเงื่อนไขเพื่อประสิทธิภาพในการจัดการการโจมตีแบบหลุมดำ ซึ่งในส่วนต่อไปในหัวข้อ 3.4 เป็นหัวข้ออธิบายการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV ในกรณีเครือข่ายไร้สายแบบ Ad hoc ที่ทำงานปกติและมีการโจมตีแบบหลุมดำ

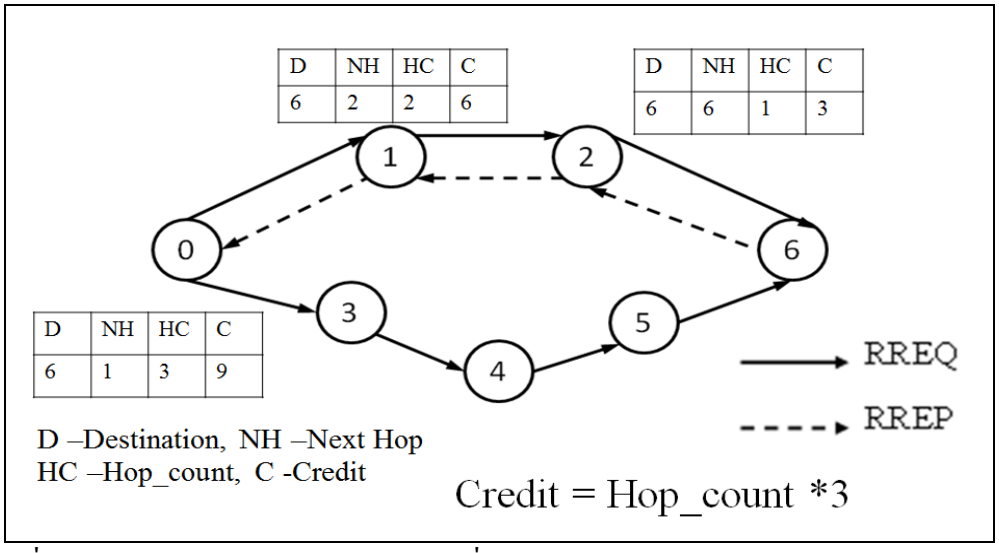
3.4 ตัวอย่างการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV ในเครือข่ายไร้สายแบบ Ad hoc

โพรโทคอลการค้นหาเส้นทาง CAODV ในเครือข่ายไร้สายแบบ Ad hoc ได้มีการอธิบายการออกแบบและวิธีการทำงานในหัวข้อ 3.2 และ 3.3 ซึ่งในหัวข้อ 3.4 นี้จะแสดงตัวอย่าง

เครือข่ายไร้สายแบบ Ad hoc ที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV 2 เครือข่ายคือ (1) เครือข่ายที่ทำงานปกติ และ (2) เครือข่ายที่มีการโจมตีแบบหลุมดำ โดยจะแสดงลักษณะการทำงานของโพรโทคอล การจัดการค่าความน่าเชื่อถือของแต่ละโหนด และการตรวจสอบการโจมตีแบบหลุมดำ

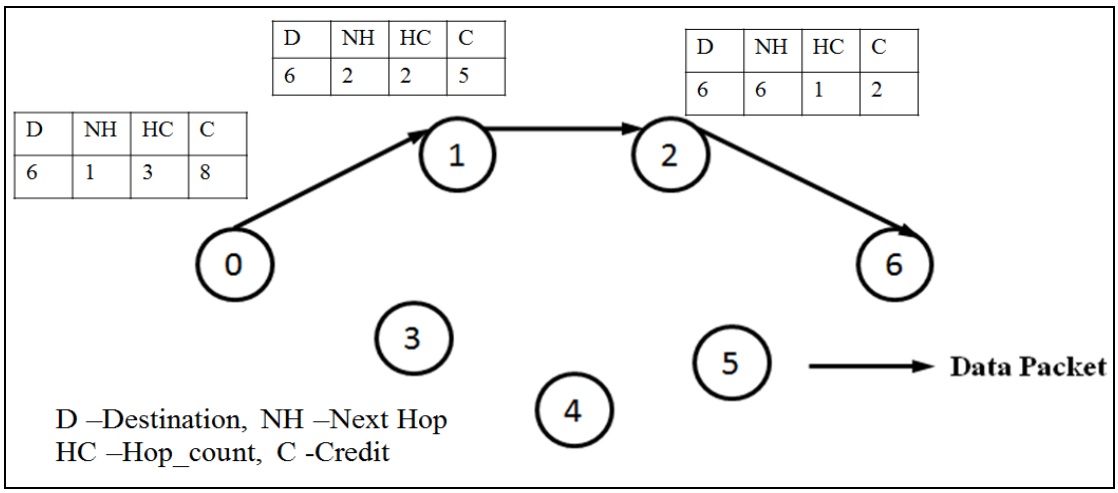
3.4.1 การทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV เมื่อไม่มีการโจมตี

เครือข่ายไร้สายแบบ Ad hoc ในรูปที่ 3.11 ประกอบด้วยโหนดจำนวน 7 โหนด โดยกำหนดให้โหนด 0 เป็นโหนดต้นทางที่ต้องการส่งข้อมูลไปยังโหนด 6 ซึ่งเป็นโหนดปลายทาง เมื่อทำการค้นหาเส้นทาง จะได้เส้นทางการสื่อสารคือ โหนด 0-1-2-6 ตามลำดับ และเมื่อเข้าสู่กระบวนการแรกของโพรโทคอลการค้นหาเส้นทาง CAODV คือกระบวนการกำหนดค่าความน่าเชื่อถือ โดยจะกำหนดค่าความน่าเชื่อถือของโหนดถัดไปลงในตารางเส้นทางตามรูปที่ 3.8

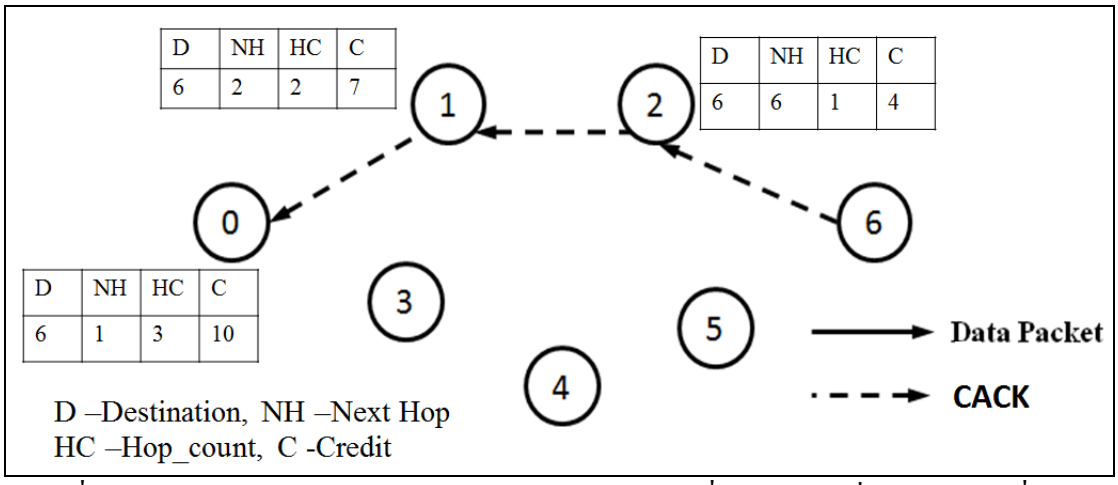


รูปที่ 3.11 กระบวนการกำหนดค่าความน่าเชื่อถือในโพรโทคอลการค้นหาเส้นทาง CAODV

การกำหนดค่าความน่าเชื่อถือของโพรโทคอลการค้นหาเส้นทาง CAODV จะกำหนดค่าเริ่มต้นโดยการนำค่าของจำนวนโหนดที่ใช้ในการส่งข้อมูลมาคำนวณ ซึ่งโหนดในรูปที่ 3.8 จะกำหนดค่าความน่าเชื่อถือดังนี้ โหนด 2 ซึ่งมีจำนวนโหนดในการส่งข้อมูลเป็น 1 (HC=1) จะกำหนดค่าความน่าเชื่อถือของโหนดถัดไป 3 ต่อมาโหนด 1 ซึ่งมีจำนวนโหนดในการส่งข้อมูลเป็น 2 (HC=2) จะกำหนดค่าความน่าเชื่อถือของโหนดถัดไป มีค่าเป็น 6 และโหนด 0 ซึ่งมีจำนวนโหนดในการส่งข้อมูลเป็น 3 (HC=3) จะกำหนดค่าความน่าเชื่อถือของโหนดถัดไปคือ 9 การกำหนดค่าความน่าเชื่อถือเริ่มต้นก่อนจะมีการส่งข้อมูล เมื่อมีการส่งข้อมูลค่าความน่าเชื่อถือของโหนดถัดไปจะลดลงดังในรูปที่ 3.9



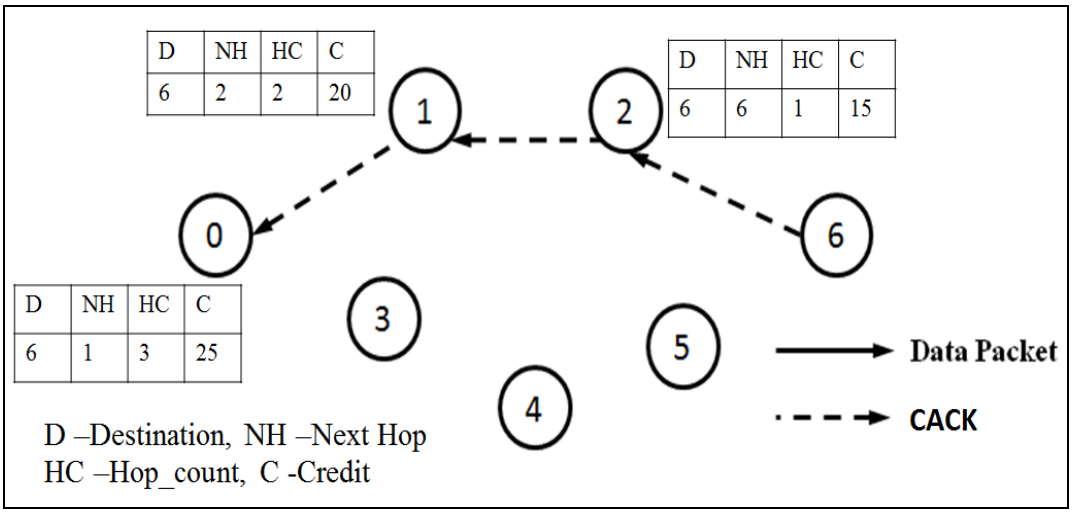
รูปที่ 3.12 การลดค่าความน่าเชื่อถือของโหนดถัดไปเมื่อโหนดมีการส่งข้อมูล



รูปที่ 3.13 โหนดปลายทางส่งข้อความควบคุม CACK กลับเพื่อให้โหนดเพิ่มค่าความน่าเชื่อถือ

จากรูปที่ 3.12 เมื่อโหนด 0 ซึ่งเป็นโหนดต้นทางทำการส่งข้อมูลไปยังโหนดปลายทาง โหนด 0 จะทำการลดค่าความน่าเชื่อถือของโหนด 1 จากนั้นทำการส่งข้อมูลต่อไปให้โหนด 2 จะลดค่าความน่าเชื่อถือของโหนด 2 และโหนด 2 ทำการส่งข้อมูลไปยังโหนด 6 ซึ่งเป็นโหนดปลายทาง โหนด 2 จะทำการลดค่าความน่าเชื่อถือลงเช่นเดียวกัน จากนั้นเมื่อโหนด 6 ได้รับข้อมูลจะทำการตอบกลับด้วยข้อความควบคุม CACK กลับไปยังโหนดต้นทางโดยใช้เส้นทางการสื่อสารเดิมเพื่อให้โหนดในเส้นทางทำการเพิ่มค่าความน่าเชื่อถือให้โหนดถัดไป ซึ่งในรูปที่ 3.13 โหนด 2 ได้ทำการเพิ่มค่าความน่าเชื่อถือของโหนด 6 ไปอีก 2 จากนั้นโหนด 2 ทำการส่งข้อความควบคุม CACK ไปยังโหนด 1 เมื่อโหนด 1 ได้รับข้อความควบคุม CACK จะทำการเพิ่มค่าเช่นเดียวกันและทำการส่งข้อความควบคุม CACK ไปยังโหนด 0 ที่เป็นโหนดต้นทาง เมื่อโหนด0 ได้รับข้อความ CACK จะทำการเพิ่มค่าความน่าเชื่อถือให้โหนด 1 ซึ่งการเพิ่มค่าความน่าเชื่อถือและ

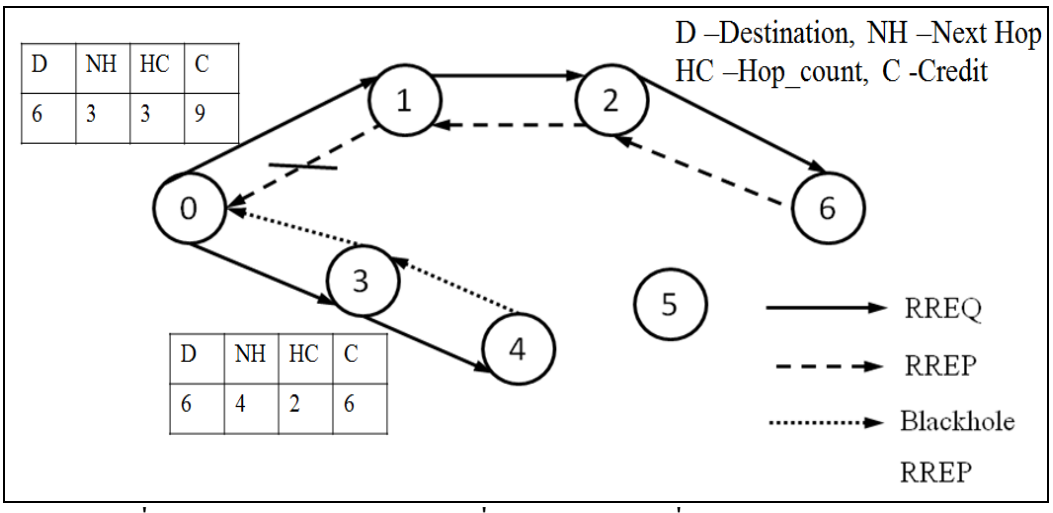
การส่งข้อความควบคุม CACK กลับจะมีค่าตามตารางที่ 1 ในหัวข้อที่ 3.3 และในกรณีที่ไม่มีข้อมูลสูญหายโหนดในเส้นทางจะมีค่าความน่าเชื่อถือตามค่าดังรูปที่ 3.5 ในหัวข้อที่ 3.3 ดังนั้นเมื่อมีการส่งข้อมูลจนไปถึงสภาวะเสถียร โหนดปลายทางส่งข้อความควบคุม CACK ทุกครั้งเมื่อได้รับข้อมูล 8 แพ็กเก็ต และโหนดในเส้นทางจะกำหนดค่าความน่าเชื่อถือได้ไม่เกินค่าจำกัดความน่าเชื่อถือ (Credit_limit) ดังนั้นในเส้นทางการสื่อสารของโหนดในตัวอย่างนี้จะมีค่าจำกัดความน่าเชื่อถือคือ โหนด 0 จะจำกัดค่าความน่าเชื่อโหนด 1 ที่ค่า 25 โหนด 1 จะจำกัดค่าความน่าเชื่อโหนด 2 ที่ค่า 20 และโหนด 2 จำกัดค่าความน่าเชื่อถือโหนด 6 ที่ค่า 15 ตามรูปที่ 3.14



รูปที่ 3.14 ค่าจำกัดความน่าเชื่อถือเมื่อเข้าสู่ภาวะเสถียร

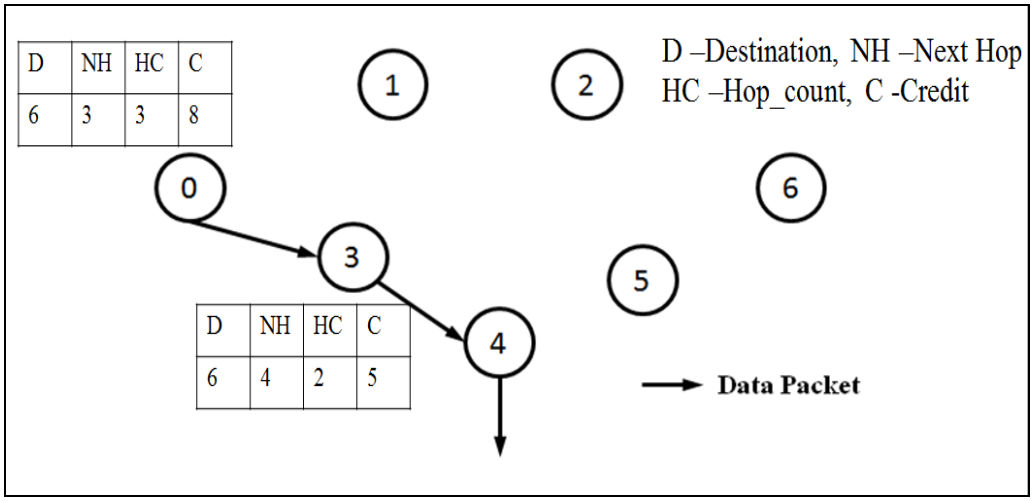
3.4.2 ลักษณะการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV เมื่อมีการโจมตีแบบหลุมดำ

โพรโทคอลการค้นหาเส้นทาง CAODV จึงได้ทำการเพิ่มการจำกัดการส่งข้อมูลโดยการใช้ค่าความน่าเชื่อถือของโหนดถัดไป โดยยกตัวอย่างการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV ในเครือข่ายดังรูปที่ 3.15 โดยโหนด 0 เป็นโหนดต้นทาง โหนด 6 เป็นโหนดปลายทาง และ โหนดที่ 4 เป็นโหนดหลุมดำทำการส่งข้อความควบคุม RREP ปลอมไปยังโหนด 0 ส่งผลให้โหนด 0 เชื่อว่าเส้นทางที่ได้จาก RREP ปลอมเป็นเส้นทางที่ดีที่สุด ดังนั้นโหนด 0 จึงส่งข้อมูลผ่านไปยังโหนด 4



รูปที่ 3.15 การกำหนดค่าความน่าเชื่อถือของโหนดเมื่อโดนโจมตีแบบหลุมดำ

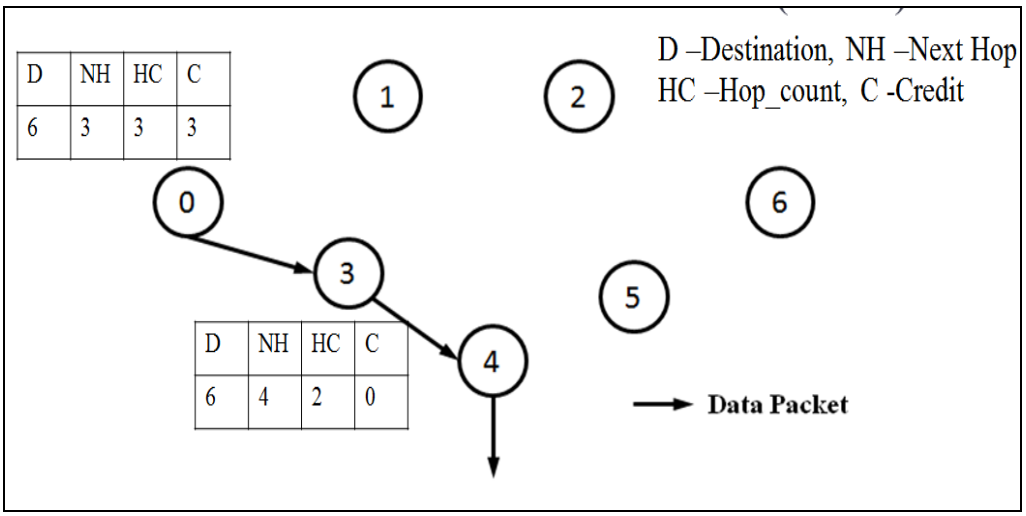
เมื่อโหนด 4 ได้รับข้อความควบคุม RREQ จะทำการตอบกลับข้อความควบคุม RREP โดยข้อมูลของจำนวนโหนดถัดไปในข้อความควบคุม RREP มีค่าเป็น 2 ไปให้โหนด 3 และเมื่อโหนด 0 ซึ่งเป็นโหนดต้นทางจะกำหนดค่าเส้นทางลงในตารางเส้นทาง โดยกำหนดจำนวนโหนดในการสื่อสารเป็น 3 และค่าความน่าเชื่อถือของโหนดถัดไปเป็น 9 และเมื่อมีการส่งข้อมูลโหนดจะทำการลดค่าความน่าเชื่อถือลงตามรูปที่ 3.16



รูปที่ 3.16 การลดค่าความน่าเชื่อถือเมื่อส่งข้อมูลในเครือข่ายที่ถูกโจมตีแบบหลุมดำ

เมื่อมีการส่งข้อมูลและไม่มีการตอบกลับข้อความควบคุม CACK จากโหนดปลายทางส่งผลให้ไม่มีการเพิ่มค่าความน่าเชื่อถือให้โหนดถัดไปดังนั้นค่าความน่าเชื่อถือของโหนด 4 จึงมีค่าเป็น 0 ซึ่ง

จากตัวอย่างเครือข่ายในรูปที่ 3.16 โหนด 3 เมื่อส่งข้อมูล 6 แพ็กเก็ต หากยังไม่ได้รับข้อความควบคุม CACK โหนด 3 จะใช้กระบวนการจำกัดการโจมตีแบบหลุมดำดังรูปที่ 3.17



รูปที่ 3.17 กระบวนการจำกัดการโจมตีแบบหลุมดำ

จากรูปที่ 3.17 เมื่อโหนด 3 ไม่ได้รับข้อความควบคุม CACK จากโหนดปลายทาง ดังนั้นเมื่อโหนด 3 ส่งข้อมูลจะทำการลดค่าความน่าเชื่อถือของโหนดถัดไป ซึ่งคือโหนด 4 จนค่าความน่าเชื่อถือมีค่าเป็น 0 จากนั้นโหนด 3 จะเข้าสู่กระบวนการที่ 3 ของโพรโทคอลการค้นหาเส้นทาง CAODV คือ กระบวนการจัดการโหนดหลุมดำ โดยกำหนดให้โหนด 4 เป็นโหนดหลุมดำ ซึ่งหมายความว่าข้อความควบคุมใดๆจากโหนด 4 เป็นข้อความที่ไม่มีความน่าเชื่อถือและทำการทิ้งข้อมูลนั้นทันที จากนั้นจะเข้ากระบวนการบำรุงรักษาเส้นทางโดยการส่งข้อความควบคุม RERR ไปยังโหนดต้นทางเพื่อทำการหาเส้นทางการสื่อสารใหม่

3.5 สรุปการออกแบบและการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV

การออกแบบและการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV โดยการออกแบบเน้นการจัดการกับการโจมตีแบบหลุมดำและเพิ่มภาระงานให้กับเครือข่ายไร้สายแบบ Ad hoc เพียงเล็กน้อยเมื่อเปรียบเทียบกับเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV เดิมซึ่งไม่สามารถจัดการกับการโจมตีแบบหลุมดำได้ ดังนั้นโพรโทคอลการค้นหาเส้นทาง CAODV จึงมีการจัดการข้อความควบคุม CACK เพื่อสมรรถนะการทำงานที่ดีของเครือข่าย โดยจะทำการวัดค่าสมรรถนะการทำงานและภาระงานด้วยการจำลองเครือข่ายผ่านโปรแกรมจำลองเครือข่าย NS-2 ในบทที่ 4

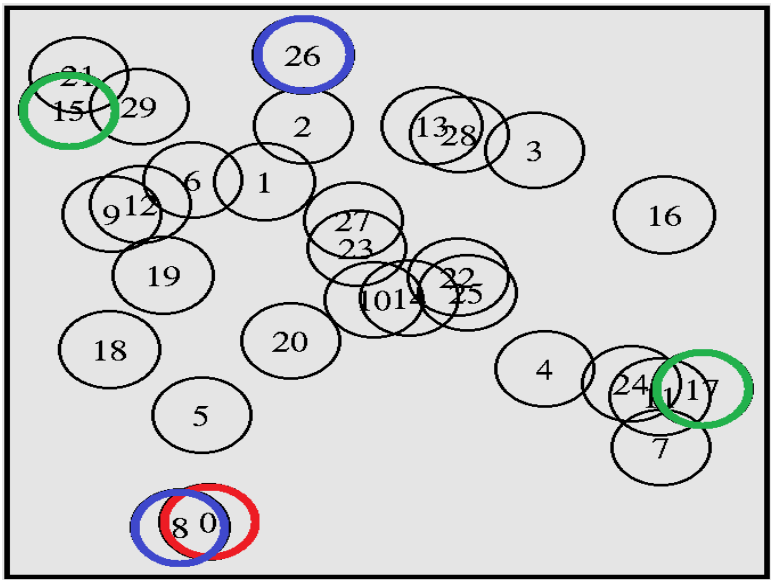
บทที่ 4

ผลการทดสอบ

เครือข่ายไร้สายแบบ Ad hoc เป็นเครือข่ายของโหนดไร้สายโดยทำการติดต่อสื่อสารด้วยตนเอง ดังนั้นจึงมีหลายปัจจัยที่ส่งผลต่อสมรรถนะการทำงานของเครือข่ายไร้สายแบบ Ad hoc เช่น การทำงานของโพรโทคอลการค้นหาเส้นทาง ความหนาแน่นของโหนดในเครือข่าย จำนวนการติดต่อสื่อสาร และการจัดการด้านความปลอดภัย ซึ่งในวิทยานิพนธ์นี้ทำการศึกษา และทดสอบเครือข่ายไร้สายแบบ Ad hoc ที่มีการโจมตีแบบหลุมดำ และเปรียบเทียบสมรรถนะการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV กับโพรโทคอลการค้นหาเส้นทาง CAODV โดยทำการจำลองเครือข่ายผ่านโปรแกรมจำลองเครือข่าย NS-2

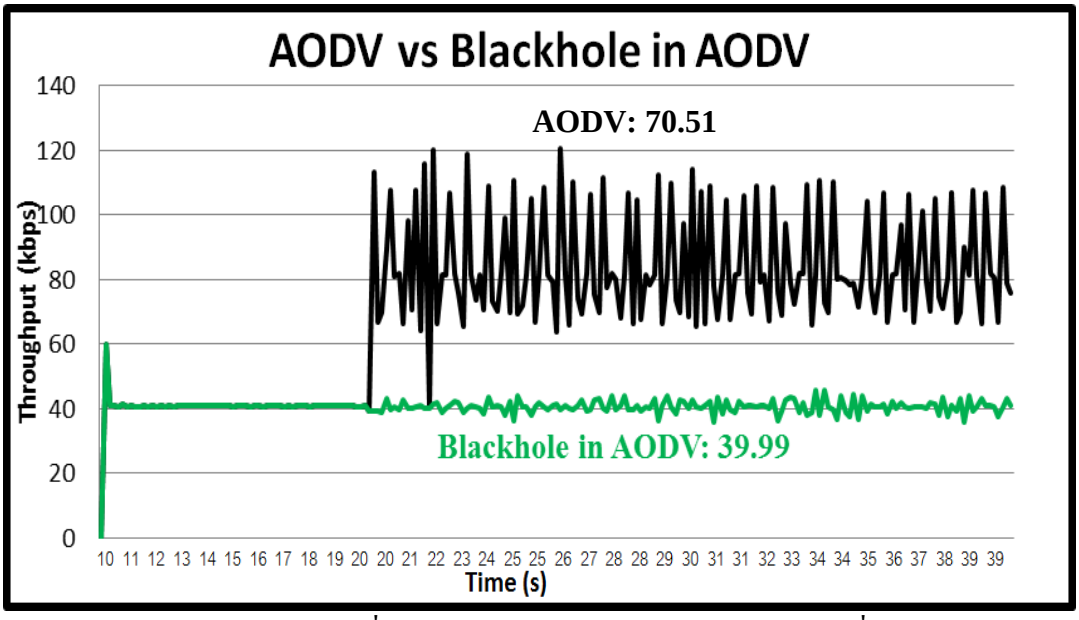
4.1 การทดสอบการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV

ออกแบบเครือข่ายไร้สายแบบ Ad hoc เพื่อใช้ทดสอบการทำงานและสมรรถนะของเครือข่ายเมื่อถูกโจมตีด้วยการโจมตีแบบหลุมดำ โดยเปรียบเทียบการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV โดยยกตัวอย่างเครือข่ายไร้สายแบบ Ad hoc โดยมีรูปแบบเครือข่ายดังรูปที่ 4.1



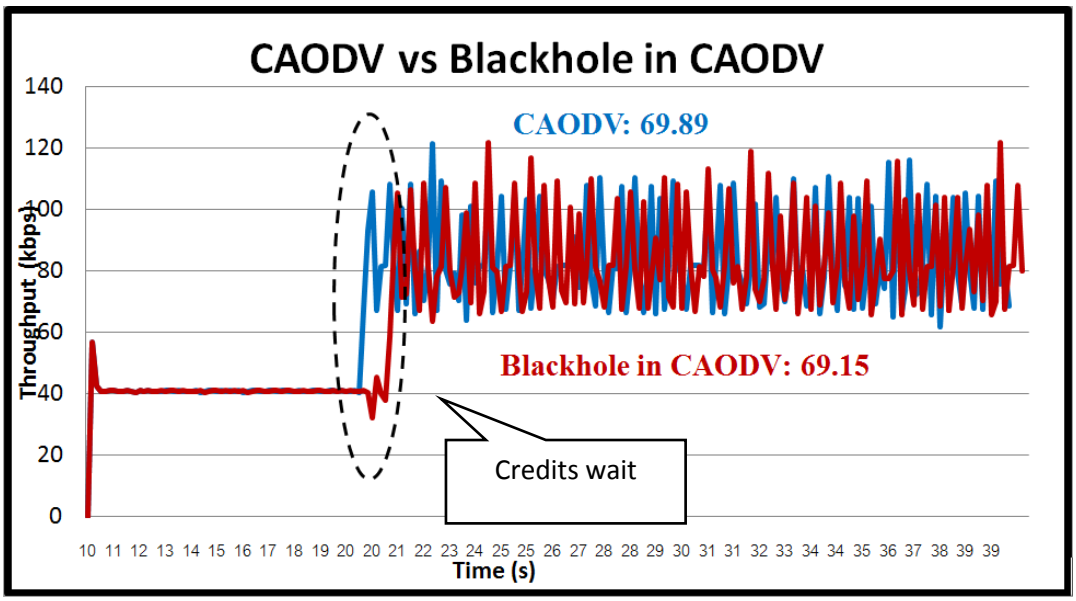
รูปที่ 4.1 ตัวอย่างรูปแบบเครือข่ายไร้สายแบบ Ad hoc

จากรูปที่ 4.1 รูปแบบเครือข่ายไร้สายแบบ Ad hoc ที่มีจำนวนโหนดเท่ากับ 30 โหนด และมีการสื่อสาร 2 คู่สัญญาณ โดยทำการสื่อสารระหว่างโหนด 15 ไปยังโหนด 17 จะส่งข้อมูลในวินาทีที่ 10 จนถึงวินาที 40 และคู่สัญญาณที่ 2 คือโหนด 8 ไปยังโหนด 26 ทำการส่งข้อมูลในวินาทีที่ 20 โดยมีโหนด 0 เป็นโหนดหลุมดำ ซึ่งในกรณีของรูปแบบเครือข่ายนี้ การสื่อสารระหว่างโหนด 8 ไปยังโหนด 26 จะถูกโจมตีโดยโหนด 0 ทำให้ไม่สามารถส่งข้อมูล ในกรณีที่เครือข่ายใช้งานโพรโทคอลการค้นหาเส้นทาง AODV เครือข่ายจะมีค่าสมรรถนะการทำงานดังรูปที่ 4.2



รูป 4.2 ค่าสมรรถนะของเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV เมื่อทำงานปกติและมีการโจมตีแบบหลุมดำ

เมื่อเปรียบเทียบค่าสมรรถนะเครือข่ายไร้สายแบบ Ad hoc เมื่อเครือข่ายทำงานปกติและมีการโจมตีดังรูปที่ 4.2 การโจมตีแบบหลุมดำส่งผลทำให้การคู่การสื่อสารที่ 2 ไม่สามารถติดต่อสื่อสารได้ ดังนั้นจึงส่งผลทำให้ค่าสมรรถนะของเครือข่ายลดลง ซึ่งในรูปแบบเครือข่ายตัวอย่างนี้ค่าสมรรถนะของเครือข่ายลดลงถึงร้อยละ 43.28 แต่เมื่อทำการเปรียบเทียบในเครือข่ายเมื่อใช้โพรโทคอลการค้นหาเส้นทาง CAODV จะทำให้สามารถป้องกันการโจมตีได้ซึ่งแสดงให้เห็นดังรูปที่ 4.3



รูปที่ 4.3 ค่าสมรรถนะของเครือข่ายที่ใช้งานโพรโทคอลการค้นหาเส้นทาง CAODV เมื่อทำงานปกติและมีการโจมตีแบบหลุมดำ

ค่าสมรรถนะของเครือข่ายไร้สายแบบ Ad hoc ที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV ดังรูปที่ 4.3 เมื่อเปรียบเทียบค่าสมรรถนะของเครือข่ายพบว่าผลกระทบจากการโจมตีแบบหลุมดำ ส่งผลกระทบเพียงร้อยละ 1.05 เท่านั้น ซึ่งค่าสมรรถนะที่ลดลงเนื่องมาจากโหนดต้นทางจำเป็นต้องรอการจัดการด้านความน่าเชื่อถือของโพรโทคอล CAODV ดังนั้นข้อจำกัดของการโจมตีแบบหลุมดำจึงส่งผลกระทบต่อสมรรถนะของเครือข่ายไร้สายแบบ Ad hoc ต่ำกว่าการใช้โพรโทคอลการค้นหาเส้นทาง AODV **แต่อย่างไรก็ตามเครือข่ายที่ได้นำเสนอในรูป 4.1 เป็นเพียงตัวอย่างในการเปรียบเทียบการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV เท่านั้น ซึ่งในหัวข้อที่ 4.2 จะเป็นการออกแบบลักษณะของเครือข่ายไร้สายแบบ Ad hoc โดยทำการจำลองด้วยเงื่อนไขที่แตกต่างกัน เพื่อทดสอบสมรรถนะของเครือข่ายเมื่อมีการโจมตีแบบหลุมดำ โดยเปรียบเทียบการทำงานของทั้งโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV**

4.2 การออกแบบการทดสอบ

การออกแบบการทดสอบโดยการเปรียบเทียบเครือข่ายไร้สายแบบ Ad hoc ซึ่งใช้โพรโทคอล การค้นหาเส้นทาง AODV และ โพรโทคอลการค้นหาเส้นทาง CAODV ทำการทดสอบการทำงานของเครือข่ายที่ทำงานปกติ และเครือข่ายที่มีการโจมตีแบบหลุมดำโดยมีโหนดหลุมดำ 1 โหนดทำการโจมตี ทำการทดสอบโดยกำหนดให้โหนดในเครือข่ายติดต่อสื่อสาร 10 คู่การสื่อสาร (10 Connections) โดยทำการส่งข้อมูลแบบคงที่ (Constant Bit Rate) และแต่ละโหนด

ในเครือข่ายมีระยะในการติดต่อสื่อสาร 50 เมตร กำหนดพื้นที่ในการทดสอบ 500 x 500 ตารางเมตร และทำการกำหนดจำนวนโหนดในเครือข่ายโดยอ้างอิงจากความหนาแน่น ซึ่งค่าความหนาแน่นเป็นตัวชี้วัดค่าเฉลี่ยของจำนวนโหนดเพื่อนบ้าน ดังในสมการที่ 4.1 [34]

$$D = (N * \pi r^2)/A \qquad \text{(สมการที่ 4.1)}$$

D คือ ความหนาแน่น (โหนด)

N คือ จำนวนโหนดทั้งหมดในเครือข่าย (โหนด)

r คือ ระยะทางในการสื่อสารของโหนด (เมตร)

A คือ พื้นที่ในการทดสอบ (เมตร^2)

เนื่องจากกำหนดจำนวนคู่การสื่อสารเป็น 10 คู่การสื่อสารดังนั้นจึงจำเป็นที่ต้องมีโหนดอย่างน้อย 20 โหนด ดังนั้นเมื่อคิดเป็นค่าความหนาแน่นของโหนดในพื้นที่การทดสอบ 500*500 เมตร ค่าความหนาแน่นของเครือข่ายจึงต่ำคือ 0.2π หรือคิดเป็น 0.62 โหนดต่อพื้นที่ ซึ่งถือว่าเป็นค่าความหนาแน่นที่ต่ำ โหนดไม่สามารถทำการสร้างเส้นทางสื่อสารถึงกันได้ ดังนั้นในการทดสอบจึงกำหนดจำนวนโหนดในเครือข่ายดังนี้ 40, 60, 80, 100, 150 และ 200 โหนด ตามลำดับ หรือค่าความหนาแน่นของเครือข่ายที่ทำการทดสอบคือ 0.4π (1.257 โหนด), 0.6π (1.885 โหนด), 0.8π (2.514 โหนด), π (3.141 โหนด), 1.5π (4.714 โหนด), และ 2π (6.282โหนด) ตามลำดับ ดังตารางที่ 4.1 จำนวนโหนดและค่าความหนาแน่นของเครือข่าย

ตารางที่ 4.1 ความสัมพันธ์ระหว่างจำนวนโหนดและความหนาแน่นของเครือข่าย

จำนวนโหนด (โหนด)	ค่าความหนาแน่น (โหนดต่อพื้นที่)
40	1.257 โหนด (0.4π)
60	1.885 โหนด (0.6π)
80	2.514 โหนด (0.8π)
100	3.141 โหนด (π)
150	4.714 โหนด (1.5π)
200	6.282 โหนด (2π)

เนื่องจากธรรมชาติของเครือข่ายไร้สายแบบ Ad hoc มีหลายปัจจัยที่ส่งผลต่อค่าสมรรถนะของเครือข่าย ดังนั้นการทดสอบจึงมุ่งเน้นในการทดสอบผลกระทบและวิธีการจัดการกับการโจมตีแบบหลุมดำ จึงไม่นำปัจจัยด้านการเคลื่อนที่ของโหนดมาเกี่ยวข้อง ซึ่งได้ผลการทดสอบดังนี้

4.2.1 ผลกระทบของการโจมตีแบบหลุมดำ

การทดสอบเครือข่ายไร้สายแบบ Ad hoc โดยโหนดทำการติดต่อสื่อสาร 10 คู่ และเครือข่ายมีความหนาแน่นที่แตกต่างกัน โดยมีจำนวนโหนด 40, 60, 80, 100, 150 และ 200 ตามลำดับ เปรียบเทียบผลกระทบจากการโจมตีแบบหลุมดำ โดยทำการวัดจำนวนการโจมตีแบบหลุมดำและโอกาสสำเร็จในการโจมตี โดยตารางที่ 4.2 การวัดค่าโดยเฉลี่ยเมื่อมีการเกิดการโจมตีแบบหลุมดำในเครือข่ายไร้สายแบบ Ad hoc ที่มีการใช้โพรโทคอลการค้นหาเส้นทาง AODV โดยกำหนดให้

#Node	หมายถึง จำนวนโหนดในเครือข่ายไร้สายแบบ Ad hoc
#RREQ	หมายถึง จำนวนข้อความควบคุม RREQ ที่โหนดต้นทางทำการส่ง เพื่อค้นหาเส้นทาง
#RREP_B	หมายถึง จำนวนการส่งข้อความควบคุม RREP จากโหนดหลุมดำ (จำนวนการโจมตีแบบหลุมดำ)
Success (%)	หมายถึง อัตราร้อยละของการโจมตีแบบหลุมดำที่สำเร็จ
PDR decrease (%)	หมายถึง อัตราร้อยละของการลดลงของจำนวนการรับข้อมูลสำเร็จต่อการส่งข้อมูล

ตารางที่ 4.2 การโจมตีแบบหลุมดำและผลกระทบเมื่อใช้โพรโทคอลการค้นหาเส้นทาง AODV

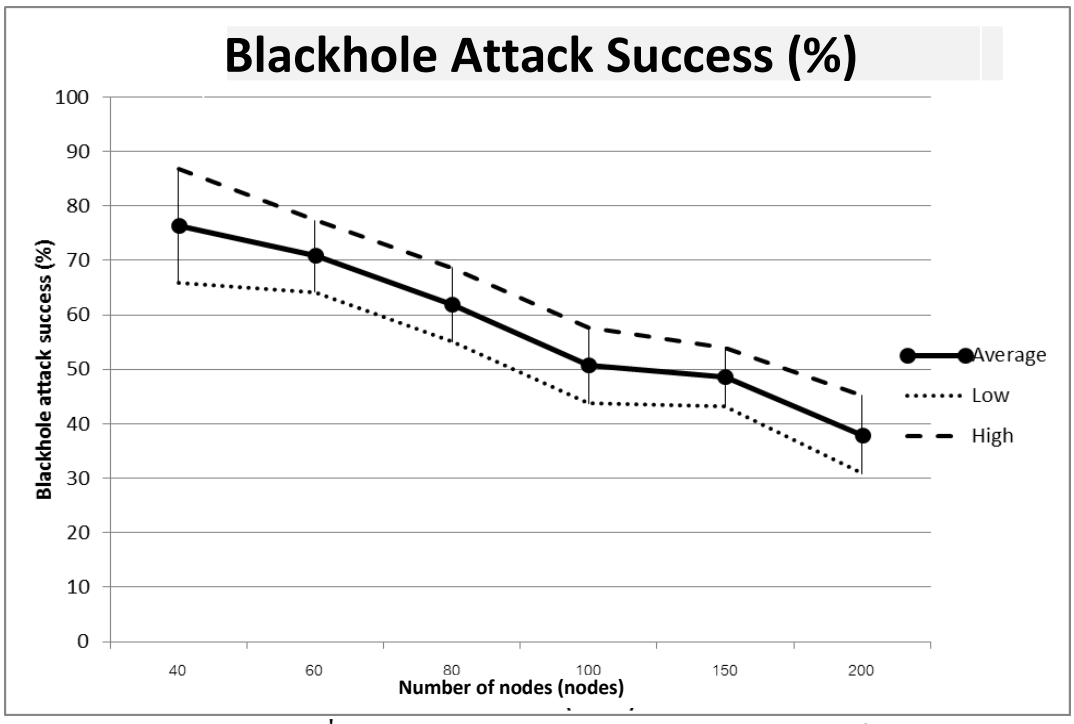
	Blackhole attack in AODV			
#Node	**#RREQ (packets)**	**#RREP_B (packets)**	**Success (%)**	**PDR decrease (%)**
40	75.8	6.8	76.4	41.86
60	69.8	26.8	70.8	68.64
80	73.2	42	61.9	61.52
100	52.2	26	50.7	32.72
150	69.6	50.4	48.6	50
200	83.4	60.4	38	41.3

จากตารางที่ 4.2 เป็นการแสดงถึงผลกระทบต่อการโจมตีแบบหลุมดำในเครือข่ายไร้สายแบบ Ad hoc ที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV โดยแสดงจำนวนของข้อความควบคุม RREQ ที่โหนดต้นทางสร้างขึ้นเพื่อใช้ในการค้นหาเส้นทางไปยังปลายทาง (คอลัมน์ #RREQ) ซึ่งการส่งข้อความควบคุม RREQ จะทำให้มีโอกาสที่โหนดหลุมดำจะทำการโจมตี ซึ่งในกรณีที่โหนดหลุมดำได้รับข้อความควบคุม RREQ จะเริ่มทำการโจมตีโดยการส่งข้อความควบคุม RREP ที่มีข้อความเท็จกลับไปยังโหนดต้นทาง (คอลัมน์ #RREP_B) แต่อย่างไรก็ตามโอกาสในการโจมตีแบบหลุมดำได้สำเร็จ (คอลัมน์ Success) ขึ้นอยู่กับความหนาแน่นของเครือข่าย ดังข้อมูลในตารางที่ 4.3 และรูปที่ 4.4 โดยสาเหตุที่การโจมตีแบบหลุมดำได้สำเร็จลดลงเนื่องด้วยมาจากการเกิดการชนกันของข้อมูล ดังรูปที่ 4.5 ดังนั้นอัตราการโจมตีสำเร็จจะมีค่าลดลงเมื่อความหนาแน่นของเครือข่ายมีค่ามากขึ้น แต่เมื่อพิจารณาถึงผลกระทบจากการโจมตีแบบหลุมดำที่ส่งผลกับอัตราความสำเร็จในการส่งข้อมูล (คอลัมน์ PDR decrease) นั้นกลับมีค่าใกล้เคียงกัน จึงแสดงให้เห็นว่าผลจากการโจมตีแบบหลุมดำนั้นส่งผลกระทบต่อเครือข่ายไร้สายแบบ Ad hoc เป็นอย่างมากเมื่อมีการโจมตีแบบหลุมดำเกิดขึ้น

#Node	หมายถึง จำนวนโหนดในเครือข่ายไร้สายแบบ Ad hoc
Mean	หมายถึง ค่าเฉลี่ยของอัตราการโจมตีสำเร็จ (ในกราฟ เส้นทึบ)
CI 95%	หมายถึง ค่าของช่วงความเชื่อมั่นร้อยละ 95
Low	หมายถึง ค่าต่ำที่สุดในช่วงความเชื่อมั่นร้อยละ 95 (ในกราฟ เส้นจุด)
High	หมายถึง ค่าสูงที่สุดในช่วงความเชื่อมั่นร้อยละ 95 (ในกราฟ เส้นประ)

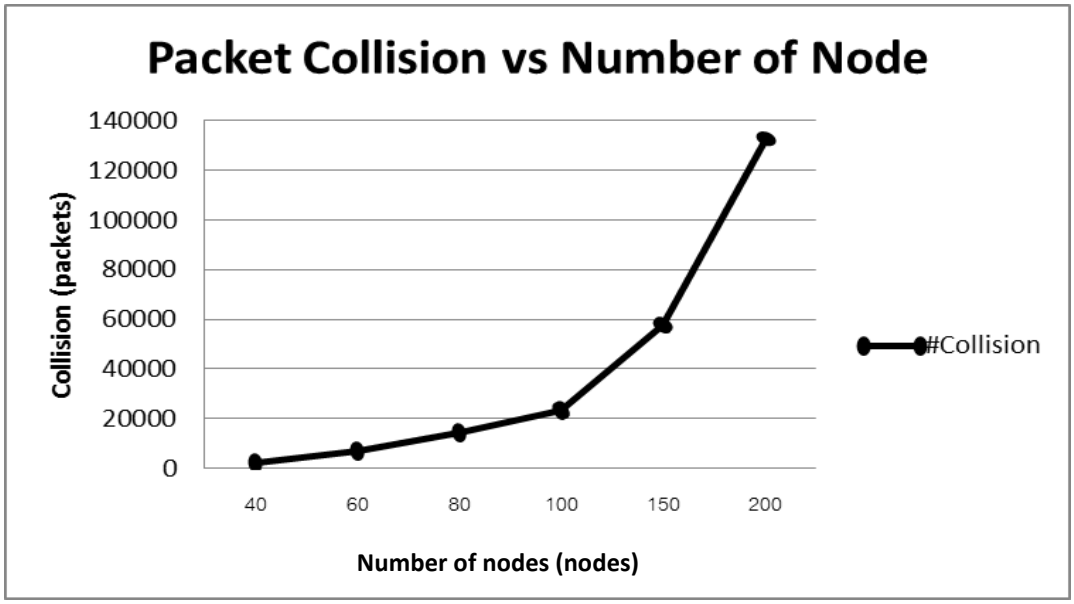
ตารางที่ 4.3 อัตราการโจมตีแบบหลุมดำสำเร็จในโพรโทคอลการค้นหาเส้นทาง AODV

#Node	Mean	CI 95%	Low	High
40	76.4	10.5	65.9	86.9
60	70.8	6.6	64.2	77.4
80	61.9	6.8	55.1	68.7
100	50.7	7	43.7	57.7
150	48.6	5.4	43.2	54
200	38	7.2	30.8	45.2



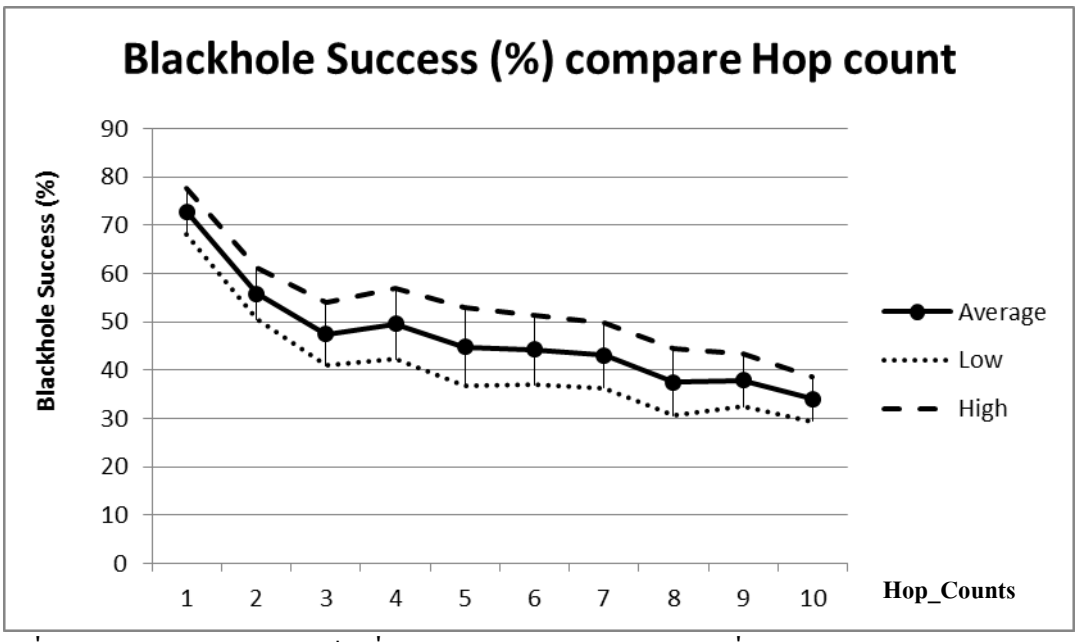
รูปที่ 4.4 อัตราร้อยละของการโจมตีแบบหลุมดำสำเร็จ

จากรูปที่ 4.4 อัตราร้อยละการโจมตีแบบหลุมดำสำเร็จในเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV เมื่อความหนาแน่นของเครือข่ายสูงขึ้น ค่าอัตราการโจมตีแบบสำเร็จจะลดลง เนื่องด้วยมาจากเครือข่ายไร้สายแบบ Ad hoc มีความหนาแน่นส่งผลทำให้มีการชนกันของข้อมูล (Collision) สูงเช่นเดียวกันดังรูป 4.5



รูปที่ 4.5 การชนกันของข้อมูลในเครือข่ายที่ทดสอบ

การชนกันของข้อมูลในรูปที่ 4.5 จะเพิ่มขึ้นตามความหนาแน่นของเครือข่าย ซึ่งจำนวนการชนกันของข้อมูลจะแตกต่างกันมากเมื่อเปรียบเทียบระหว่างเครือข่ายที่มีจำนวน 40 โหนดโดยมีการชนกันของมูลโดยเฉลี่ยเพียง 2308 เท่านั้น ซึ่งแตกต่างกับเครือข่ายที่จำนวนโหนด 200 โหนดที่มีการชนกันของข้อมูลโดยเฉลี่ยถึง 133107 ซึ่งเมื่อคิดในอัตราส่วนพบว่าจำนวนโหนดเพิ่มขึ้นเพียง 5 เท่าแต่จำนวนการชนกันของข้อมูลเพิ่มถึง 58 เท่า ซึ่งเป็นผลมาจากข้อจำกัดและคุณลักษณะของเครือข่ายไร้สายแบบ Ad hoc ที่โหนดในเครือข่ายไม่มีศูนย์กลางในการจัดการเส้นทางและลำดับในการส่งข้อมูล จึงส่งผลทำให้โหนดในเครือข่ายไม่สามารถตรวจสอบได้ว่าช่องสัญญาณของโหนดถัดไปว่างอยู่หรือไม่ทำให้ง่ายต่อการชนกันของข้อมูล อย่างไรก็ตามปัจจัยที่ส่งผลกระทบต่อการชนกันของข้อมูลคือ โหนดจำเป็นต้องกระจายข้อความควบคุมไปทั้งเครือข่าย ดังนั้นในเครือข่ายที่มีความหนาแน่นสูงจะทำให้การชนกันของข้อมูลสูงตามไปด้วย จึงส่งผลทำให้การโจมตีแบบหลุมดำที่จำเป็นต้องรับข้อความควบคุม RREQ และทำการส่งข้อความควบคุม RREP ที่มีข้อมูลเท็จกลับไปนั้น จึงมีโอกาสที่เกิดการชนกันข้อมูลเกิดขึ้นได้ และส่งผลทำให้ข้อความควบคุม RREP ที่มีข้อความเท็จไปไม่ถึงยังโหนดต้นทาง ส่งผลให้การโจมตีแบบหลุมดำไม่สำเร็จ ดังนั้นจึงทำให้อัตราการโจมตีหลุมดำสำเร็จลดลง เมื่อความหนาแน่นของเครือข่ายเพิ่มขึ้นในเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV และเมื่อพิจารณาผลจากจำนวนโหนดที่ส่งข้อมูลไปยังโหนดหลุมดำกับอัตราของผลการโจมตีแบบหลุมดำสำเร็จได้ดังรูปที่ 4.6



รูปที่ 4.6 ค่าอัตราการโจมตีสำเร็จเมื่อเปรียบเทียบกับจำนวนโหนดที่ใช้ส่งข้อมูลมายังโหนดหลุมดำ

จากรูปที่ 4.6 ค่าอัตราการโจมตีสำเร็จเมื่อเปรียบเทียบกับจำนวนโหนดที่ใช้ส่งข้อมูลมายังโหนดหลุมดำ อัตราการโจมตีสำเร็จจะลดลงเมื่อจำนวนโหนดสูงขึ้น เนื่องจากโหนดที่ใช้ในการส่งข้อมูลที่มากขึ้น จะมีโอกาสทำให้เกิดข้อผิดพลาดในการส่งข้อมูลที่สูงขึ้น เพราะมีโอกาสการชนกันของข้อมูลมีมากกว่าในการส่งข้อมูลของจำนวนโหนดน้อย แต่อย่างไรก็ตามเมื่อเกิดการโจมตีแบบหลุมดำจะส่งผลทำให้ค่าสมรรถนะของเครือข่ายลดลงอย่างมาก ซึ่งในหัวข้อ 4.2.2 จะทำการพิจารณาค่าสมรรถนะของเครือข่าย

4.2.2 ค่าสมรรถนะของเครือข่าย (Throughput)

การทดสอบหาค่าสมรรถนะของเครือข่ายไร้สายแบบ Ad hoc โดยทำการเปรียบเทียบการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV โดยเครือข่ายทำงานอย่างปกติและมีการโจมตีแบบหลุมดำดังตารางที่ 4.4 โดยกำหนดให้

AODV หมายถึง โพรโทคอลการค้นหาเส้นทาง AODV

AODV+B หมายถึง โพรโทคอลการค้นหาเส้นทาง AODV ที่มีการโจมตีแบบหลุมดำ

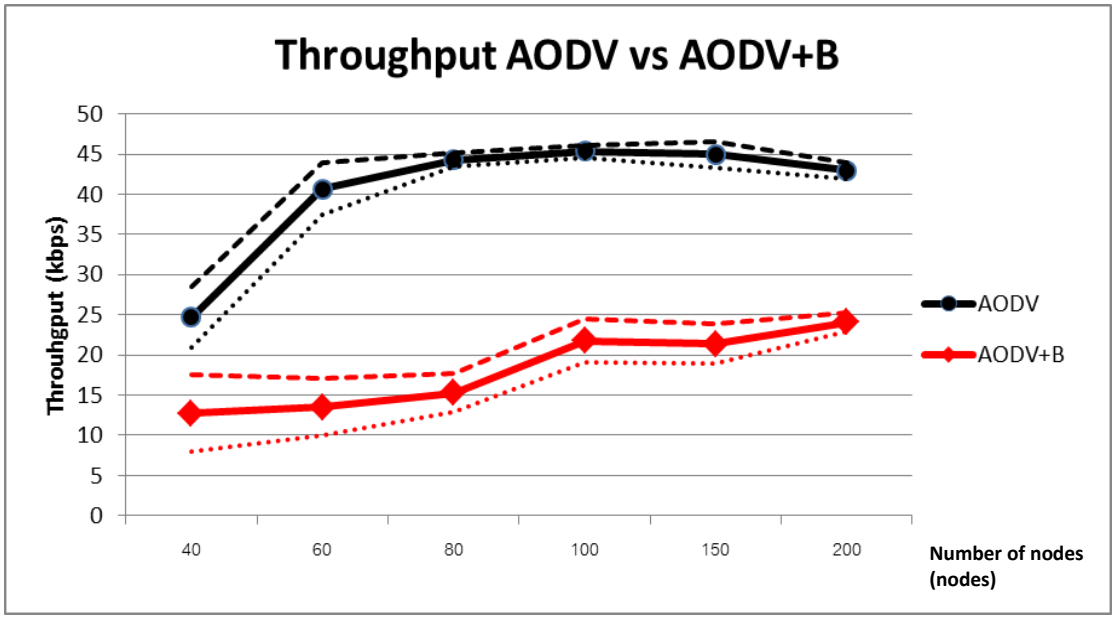
CAODV หมายถึง โพรโทคอลการค้นหาเส้นทาง CAODV

CAODV+B หมายถึง โพรโทคอลการค้นหาเส้นทาง CAODV ที่มีการโจมตีแบบหลุมดำ

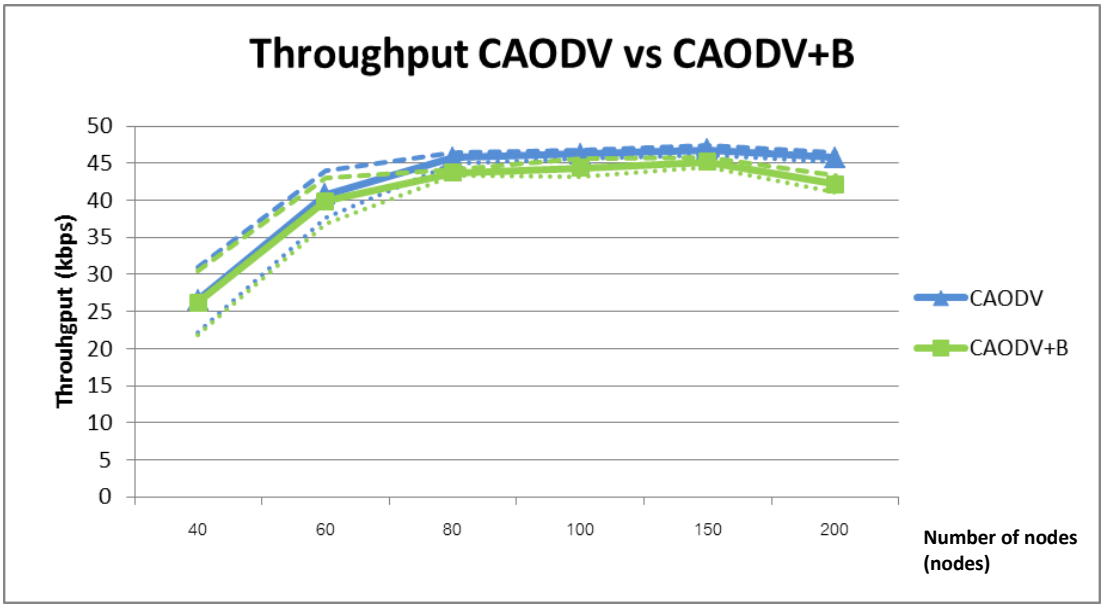
ตารางที่ 4.4 ค่าสมรรถนะเครือข่ายในสถานการณ์ที่แตกต่างกัน

	AODV				AODV+B			
#Nodes	**Mean**	**CI 95%**	**Low**	**High**	**Mean**	**CI 95%**	**Low**	**High**
40	24.7	3.78	20.92	28.48	12.75	4.78	7.97	17.53
60	40.66	3.27	37.39	43.93	13.54	3.5	10.04	17.04
80	44.3	0.86	43.44	45.16	15.3	2.35	12.95	17.65
100	45.36	0.74	44.62	46.1	21.78	2.66	19.12	24.44
150	44.94	1.64	43.3	46.58	21.36	2.48	18.88	23.84
200	42.95	1.02	41.93	43.97	24.07	1.18	22.89	25.25
	CAODV				**CAODV+B**			
#Nodes	**Mean**	**CI 95%**	**Low**	**High**	**Mean**	**CI 95%**	**Low**	**High**
40	26.53	4.39	22.14	30.92	26.17	4.33	21.84	30.5
60	40.78	3.15	37.63	43.93	39.9	3.07	36.83	42.97
80	45.72	0.76	44.96	46.48	43.73	0.45	43.28	44.18
100	46.2	0.54	45.66	46.74	44.4	1.15	43.25	45.55
150	46.83	0.65	46.18	47.48	45.18	0.63	44.55	45.81
200	45.78	0.69	45.09	46.47	42.16	1.13	41.03	43.29

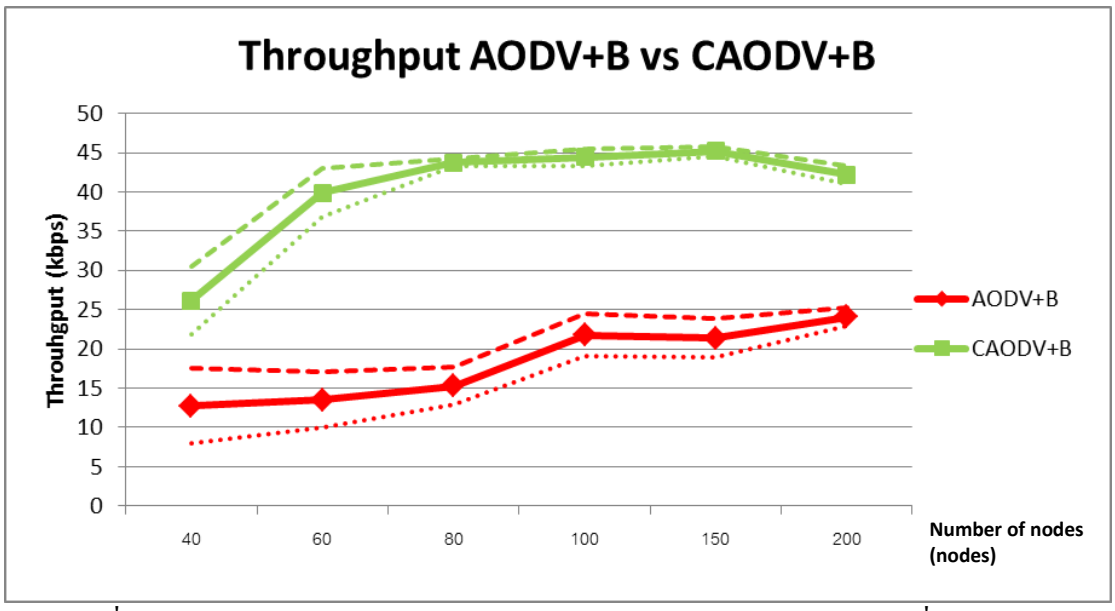
จากข้อมูลในตารางที่ 4.7 สามารถวาดเป็นกราฟได้ดังรูปที่ 4.7 ถึงรูปที่ 4.10 แสดงการเปรียบเทียบค่าสมรรถนะของเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV และ CAODV เมื่อเครือข่ายทำงานปกติและมีการโจมตีแบบหลุมดำ



รูปที่ 4.7 ค่าสมรรถนะเครือข่ายของโพรโทคอล AODV เมื่อทำงานปกติและถูกโจมตี



รูปที่ 4.8 ค่าสมรรถนะเครือข่ายของโพรโทคอล CAODV เมื่อทำงานปกติและถูกโจมตี



รูปที่ 4.9 ค่าสมรรถนะเครือข่ายระหว่างโพรโทคอล AODV และ CAODV เมื่อถูกโจมตี

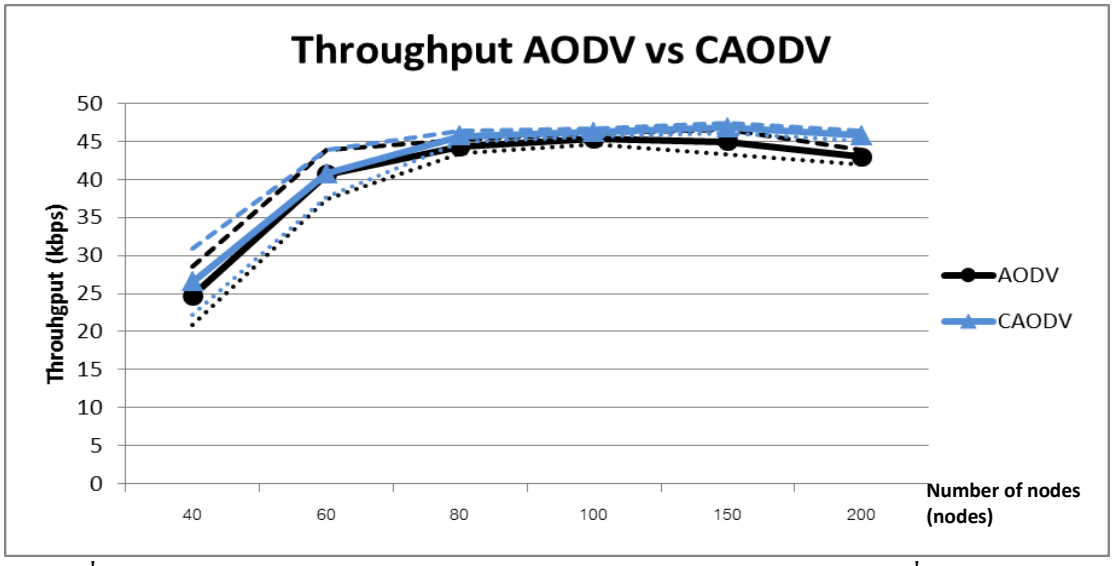
เมื่อพิจารณาผลกระทบของการโจมตีแบบหลุมดำในโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV ในรูปที่ 4.7 ถึงรูปที่ 4.9 ผลกระทบจากการโจมตีของหลุมดำจะลดลงเมื่อความหนาแน่นสูงขึ้น ซึ่งด้วยมาจากอัตราการโจมตีสำเร็จของโหนดหลุมดำลดลงเมื่อเครือข่ายหนาแน่นสูงขึ้น ดังที่ได้แสดงในการทดสอบ 4.21 และเมื่อได้นำค่าสมรรถนะมาเปรียบเทียบจะได้ค่าดังตารางที่ 4.5

ตารางที่ 4.5 ค่าสมรรถนะของเครือข่ายที่ลดลงจากผลการโจมตีแบบหลุมดำ

Throughput Decrease (%)		
#Nodes	**AODV**	**CAODV**
40	48.38	1.35
60	66.7	2.15
80	65.46	4.35
100	51.98	3.89
150	52.47	3.52
200	43.95	7.9
Mean	54.82	3.86
CI 95%	8.11	1.82
Low	46.71	2.04
High	62.93	5.68

จากตารางที่ 4.5 ค่าสมรรถนะของเครือข่ายที่ลดลงจากผลการโจมตีแบบหลุมดำในเครือข่ายที่ความหนาแน่นที่แตกต่างกัน โพรโทคอลการค้นหาเส้นทาง AODV เมื่อถูกโจมตีแบบ

หลุมดำค่าสมรรถนะลดลงโดยเฉลี่ย 54.82 และช่วงความเชื่อมั่นร้อยละ 95 ค่าสมรรถนะของเครือข่ายลดลงอยู่ในช่วงร้อยละ 46.71 ถึง 62.93 แต่เมื่อเปรียบเทียบกับโพรโทคอลค้นหาเส้นทาง CAODV เมื่อถูกโจมตีหลุมดำลดลงโดยเฉลี่ย 3.86 โดยช่วงความเชื่อมั่นร้อยละ 95 ค่าสมรรถนะของเครือข่ายลดลงอยู่ในช่วงร้อยละ 2.04 ถึง 5.68 เมื่อเปรียบเทียบผลกระทบจากการโจมตีพบว่าโพรโทคอลการค้นหาเส้นทาง CAODV เพิ่มค่าสมรรถนะเครือข่ายไร้สายแบบ Ad hoc ถึงร้อยละ 112 เมื่อเปรียบเทียบกับโพรโทคอลการค้นหาเส้นทาง AODV ที่ถูกโจมตีในลักษณะเดียวกัน อย่างไรก็ตามโพรโทคอลการค้นหาเส้นทาง CAODV ยังคงมีข้อจำกัด เมื่อเครือข่ายมีความหนาแน่นสูงขึ้น ผลกระทบจากการโจมตีแบบหลุมดำกลับสูงขึ้น โดยเฉพาะอย่างยิ่งเครือข่ายที่มีจำนวนโหนด 200 โหนด ที่ผลกระทบจากการโจมตีแบบหลุมดำสามารถลดค่าสมรรถนะของเครือข่ายสูงถึงร้อยละ 7.9 เนื่องด้วยการทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV มีข้อจำกัดในช่วงเวลาที่จำเป็นต้องรอค่าความน่าเชื่อถือดังเช่นที่แสดงในรูป 4.3 ซึ่งผลกระทบดังกล่าวเมื่อความหนาแน่นของเครือข่ายสูงขึ้น โอกาสที่เส้นทางสื่อสารเสียหายและโอกาสการชนกันของข้อมูลจะสูงกว่าเครือข่ายที่มีความหนาแน่นต่ำ โอกาสเกิดการโจมตีแบบหลุมดำจึงสูง (จำนวนครั้งในการโจมตี) และ ประกอบกับการจัดการค่าความน่าเชื่อถือที่จำเป็นต้องได้รับข้อความควบคุม CACK จากโหนดปลายทาง มีโอกาสที่จะมีการชนกันของข้อมูลที่สูง ดังนั้นในบางกรณีโหนดจะไม่ได้รับข้อความควบคุม CACK จากโหนดปลายทาง แต่อย่างไรก็ตามโพรโทคอลการค้นหาเส้นทาง CAODV ก็ยังสามารถจัดการและป้องกันการโจมตีแบบหลุมดำ โดยจำกัดผลกระทบของการโจมตีแบบหลุมดำได้ รวมไปถึงในกรณีที่เครือข่ายไม่ถูกโจมตี โพรโทคอลการค้นหาเส้นทาง CAODV มีสมรรถนะใกล้เคียงกับโพรโทคอลการค้นหาเส้นทาง AODV ดังรูปที่ 4.10



รูปที่ 4.10 ค่าสมรรถนะเครือข่ายระหว่างโพรโทคอล AODV และ CAODV เมื่อทำงานปกติ

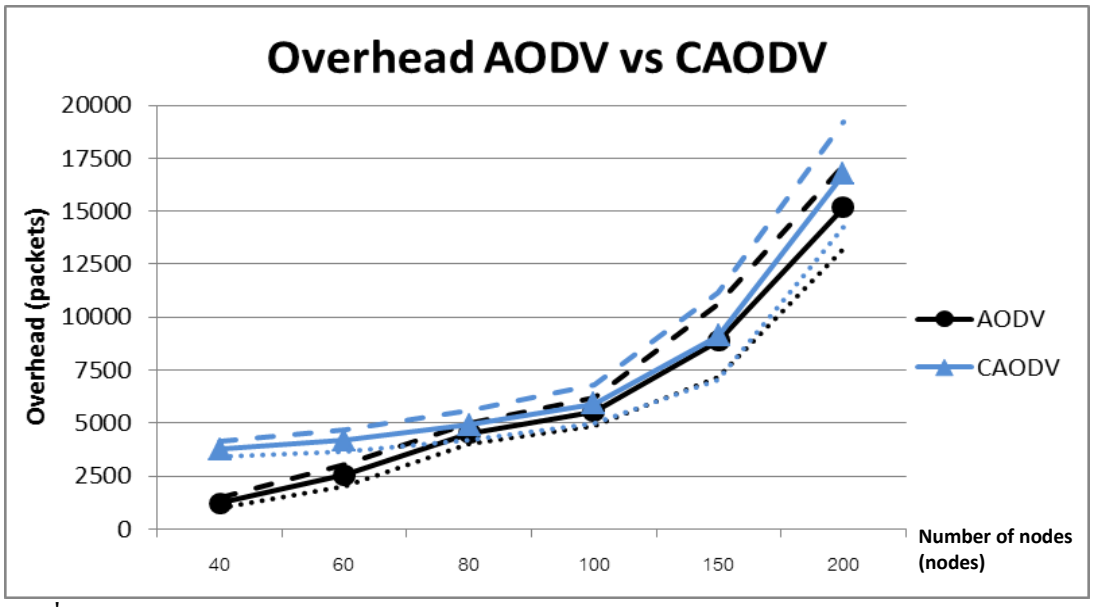
จากรูปที่ 4.10 ค่าสมรรถนะเครือข่ายระหว่างโพรโทคอล AODV และ CAODV เมื่อเครือข่ายไม่ถูกโจมตี ค่าสมรรถนะของเครือข่ายเฉลี่ยมีค่าใกล้เคียงกัน คือ 41 กิโลบิตต่อวินาที และมีค่าช่วงเชื่อมั่นร้อยละ 95 อยู่ที่ 35.7 ถึง 48.3 แต่อย่างไรก็ตามการทำงานของ CAODV จำเป็นต้องเพิ่มภาระงานให้กับเครือข่ายดังนั้นในหัวข้อ 4.2.3 จะเป็นการเปรียบเทียบค่าภาระงานของเครือข่าย

4.2.3 ค่าภาระงานของเครือข่าย (Overhead)

ทดสอบหาค่าภาระงานของเครือข่ายไร้สายแบบ Ad hoc โดยทำการเปรียบเทียบการทำงานของโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV เมื่อเครือข่ายทำงานอย่างปกติ และมีการโจมตีแบบหลุมดำโดยผลการทดสอบดังตารางที่ 4.6 และ รูปที่ 4.11

ตารางที่ 4.6 ค่าภาระงานของเครือข่ายที่จำนวนโหนดแตกต่างกัน

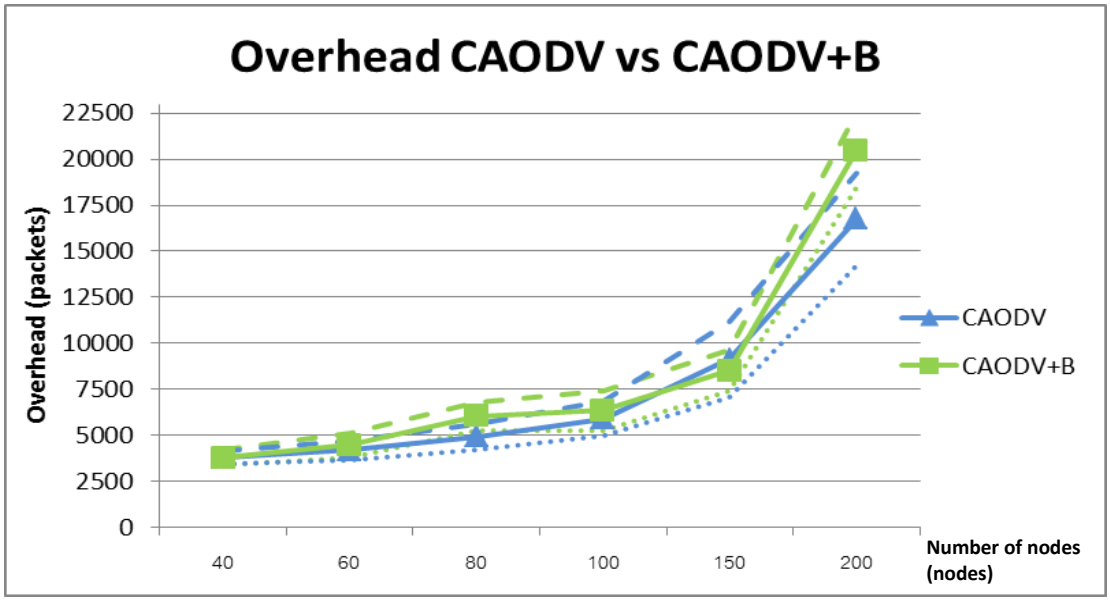
Overhead								
	AODV				**AODV+B**			
#Nodes	**Mean**	**CI 95%**	**Low**	**High**	**Mean**	**CI 95%**	**Low**	**High**
40	1206	244	962	1450	877	198	679	1556
60	2543	525	2018	3068	1644	302	1342	2986
80	4516	477	4039	4993	3124	334	2790	5914
100	5541	685	4856	6226	3727	429	3298	7025
150	8886	1711	7175	10597	7911	1209	6702	14613
200	15190	1961	13229	17151	11180	852	10328	21508
	CAODV				**CAODV+B**			
#Nodes	**Mean**	**CI 95%**	**Low**	**High**	**Mean**	**CI 95%**	**Low**	**High**
40	3765	344	3421	4109	3780	396	3384	7164
60	4177	512	3665	4689	4450	660	3790	8240
80	4907	712	4195	5619	6024	788	5236	11260
100	5897	933	4964	6830	6353	1084	5269	11622
150	9117	2060	7057	11177	8509	1123	7386	15895
200	16745	2500	14245	19245	20480	2028	18452	38932



รูปที่ 4.11 ค่าภาระงานของเครือข่ายระหว่างโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV

ค่าในตารางที่ 4.6 แสดงค่าภาระงานของเครือข่ายไร้สายแบบ Ad hoc เมื่อใช้โพร-โทคอลการค้นหาเส้นทาง AODV และ CAODV เมื่อทำงานปกติและมีการโจมตีแบบหลุมดำ เมื่อเครือข่ายไม่มีการโจมตีแบบหลุมดำ ค่าภาระงานของเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV เพิ่มขึ้นจากเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV เฉลี่ยร้อยละ 17.75 แต่อย่างไรก็ตามในช่วงความหนาแน่นของเครือข่ายต่ำ เช่น 40 โหนด และ 60 โหนด นั้นค่าภาระงานของ CAODV จะสูงกว่าโพรโทคอล AODV ถึงร้อยละ 212 และ 64 ตามลำดับ ซึ่งภาระงานที่สูงขึ้นของ CAODV ในเครือข่ายที่มีความหนาแน่นต่ำเนื่องจาก โหนดจำเป็นต้องค้นหาเส้นทางในการส่งข้อมูลและเมื่อโหนดทำการสร้างเส้นทางได้โหนดจะใช้ระบบความน่าเชื่อถือในการจัดการเส้นทาง โดยกระบวนการดังกล่าวซึ่งเริ่มต้นในการจัดการค่าความน่าเชื่อถือจะมีการใช้ภาระงานที่สูงกว่าเครือข่ายที่มีความหนาแน่นในการสื่อสารอย่างจำนวนโหนด 80 และ 100 โหนด ซึ่งแสดงให้เห็นว่าภาระงานของ CAODV ไม่แตกต่างจาก AODV โดยแตกต่างกันเพียงร้อยละ 6.42 ในเครือข่ายจำนวนโหนด 100 โหนด จึงแสดงให้เห็นว่าภาระงานของโพรโทคอลการค้นหาเส้นทาง CAODV จะขึ้นอยู่กับการจัดการเส้นทางในเครือข่าย ดังนั้นในเครือข่ายที่มีความหนาแน่นต่ำ ที่จำเป็นต้องค้นหาเส้นทางอยู่เสมอ หรือเครือข่ายที่มีความหนาแน่นสูงที่ส่งผลต่อการชนกันของมูล นั้นจะส่งผลทำให้ภาระงานของโพรโทคอลการค้นหาเส้นทาง CAODV สูงตามไปด้วย

แต่อย่างไรก็ตามการเพิ่มภาระงานของโพรโทคอลการค้นหาเส้นทาง CAODV เมื่อเฉลี่ยแล้วจะเพิ่มภาระงานให้เครือข่ายร้อยละ 14.7 ซึ่งภาระงานที่เพิ่มขึ้นมีจุดประสงค์เพื่อใช้ในการจัดการกับการโจมตีแบบหลุมดำ และเมื่อถูกโหนดหลุมดำโจมตีเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV จะมีภาระงานเพิ่มขึ้นดังรูปที่ 4.12



รูปที่ 4.12 เปรียบเทียบภาระงานของโพรโทคอลการค้นหาเส้นทาง CAODV เมื่อทำงานปกติและถูกโจมตีแบบหลุมดำ

เมื่อมีการโจมตีแบบหลุมดำ โพรโทคอลการค้นหาเส้นทาง CAODV จะมีการเพิ่มภาระงานในการจัดการเส้นทาง เพื่อป้องกันการโจมตีแบบหลุมดำ โดยค่าภาระงานเพิ่มขึ้นดังรูปที่ 4.12 การทำงานของโพรโทคอลการค้นหาเส้นทาง CAODV จะเพิ่มค่าภาระงานขึ้นร้อยละ 11.2 เพื่อใช้ในการจัดการกับการโจมตีแบบหลุมดำ

4.3 สรุปผลการทดสอบ

เมื่อทดสอบเครือข่ายไร้สายแบบ Ad hoc โดยทำการเปรียบเทียบระหว่างโพรโทคอลการค้นหาเส้นทาง AODV และ CAODV เมื่อเครือข่ายทำงานปกติและเครือข่ายที่มีการโจมตีแบบหลุมดำ โดยประเมินจากการวัดค่าสมรรถนะของเครือข่ายและค่าภาระงานของเครือข่าย ซึ่งเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง AODV เมื่อมีการโจมตีแบบหลุมดำ ค่าสมรรถนะของเครือข่ายจะลดลงร้อยละ 54.82 แต่เมื่อมีการโจมตีแบบหลุมดำในเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV ค่าสมรรถนะของเครือข่ายลดลงเพียงร้อยละ 3.86 เท่านั้น แต่เมื่อพิจารณา

ด้านภาระงานของเครือข่ายที่เพิ่มขึ้นเมื่อเครือข่ายใช้โพรโทคอลการค้นหาเส้นทาง CAODV โดยเปรียบเทียบกับโพรโทคอลการค้นหาเส้นทาง AODV ค่าภาระงานเพิ่มขึ้นโดยจะขึ้นอยู่กับความหนาแน่นของเครือข่าย โดยค่าภาระงานเพิ่มขึ้นโดยเฉลี่ยร้อยละ 14.7 แต่เมื่อเปรียบเทียบค่าสมรรถนะของเครือข่ายแบบ Ad hoc ที่ถูกโจมตีแบบหลุมดำ ซึ่งเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV จะมีค่าสมรรถนะสูงกว่าโพรโทคอลการค้นหาเส้นทาง AODV ถึงร้อยละ 112

บทที่ 5
บทสรุป ปัญหาและข้อเสนอแนะ

5.1 บทนำ

ในบทนี้จะกล่าวถึงบทสรุปและข้อเสนอแนะของการทำวิทยานิพนธ์ ปัญหาและอุปสรรคต่างๆ ที่เกิดขึ้นในขณะที่ทำวิทยานิพนธ์ และท้ายที่สุดจะกล่าวถึงรายละเอียดและข้อเสนอแนะแก่ผู้ที่สนใจที่จะนำวิทยานิพนธ์ชุดนี้ไปพัฒนาต่อไป

5.2 บทสรุปของการทำวิทยานิพนธ์

เครือข่ายไร้สายแบบ Ad hoc มีหลายปัจจัยที่ส่งผลต่อค่าสมรรถนะของเครือข่าย เช่น การจัดการเส้นทางการสื่อสารของโหนด การรักษาความปลอดภัยของเครือข่าย ข้อจำกัดทางด้านทรัพยากรของโหนด ความหนาแน่นของเครือข่าย และการเคลื่อนที่ของโหนด เป็นต้น ซึ่งปัจจัยข้างต้น การจัดการเส้นทางการสื่อสารถือเป็นเรื่องที่สำคัญที่สุดที่ส่งผลต่อค่าสมรรถนะของเครือข่ายโดยตรง เพราะโหนดจะไม่สามารถส่งข้อมูลไปยังปลายทางได้ ถ้าไม่มีการจัดการเส้นทางการสื่อสารอย่างมีประสิทธิภาพ ประกอบกับการจัดการเส้นทางการสื่อสารที่ดีจะสามารถเพิ่มประสิทธิภาพในการจัดการด้านความปลอดภัยด้วย ซึ่งโพรโทคอลการค้นหาเส้นทาง AODV มีสมรรถนะที่ดีในการจัดการเส้นทาง แต่ยังคงมีจุดอ่อนในด้านการจัดการด้านความปลอดภัย จึงมีจุดอ่อนให้เกิดการโจมตีแบบหลุมดำได้ง่าย วิทยานิพนธ์นี้จึงนำเสนอการโจมตีแบบหลุมดำในเครือข่ายไร้สายแบบ Ad hoc ที่มีการใช้โพรโทคอลการค้นหาเส้นทาง AODV โดยแสดงผลกระทบและความรุนแรงของการโจมตีแบบหลุมดำ และนำเสนอโพรโทคอลการค้นหาเส้นทาง CAODV ที่ใช้ค่าความน่าเชื่อถือในการตรวจสอบ และจัดการกับการโจมตีแบบหลุมดำ

เมื่อเปรียบเทียบโพรโทคอลการค้นหาเส้นทาง CAODV กับกระบวนการต่างๆ ทั้ง 5 วิธี ที่มีข้อดีและข้อเสียแตกต่างกัน ได้แก่ (1)การใช้ศูนย์กลางในการจัดการเส้นทางการสื่อสารอย่าง FRIMM นั้นถือว่าง่ายต่อการควบคุมและจัดการ แต่อย่างไรก็ตามการใช้ศูนย์กลางในการจัดการข้อมูลต่างๆ จะไม่ตรงกับจุดประสงค์ของการออกแบบเครือข่ายไร้สายแบบ Ad hoc ที่ทุกโหนดในเครือข่ายสามารถจัดการเส้นทางการสื่อสารของตนเองได้โดยที่ไม่จำเป็นต้องมีสถานีฐาน (2) การใช้กระบวนการด้านการเข้ารหัส ซึ่งกระบวนการนี้เป็นที่นิยมอย่างมากในการจัดการด้านความปลอดภัย สามารักษาความปลอดภัยของข้อมูล รวมไปถึงการยืนยันตัวตน ซึ่งในเครือข่ายไร้

สายแบบ Ad hoc อย่างเช่นโพรโทคอลการค้นหาเส้นทาง SAODV นำการเข้ารหัสมาใช้ แต่อย่างไรก็ตามการจัดการด้านการเข้ารหัสจำเป็นต้องมีระบบการประมวลผลที่ซับซ้อน และต้องมีการจัดการกับกุญแจที่ใช้ในการเข้ารหัสเป็นอย่างดี ซึ่งการจัดการในการแจกกุญแจ หรือการตรวจสอบความถูกต้องของกุญแจเป็นเรื่องที่ยุ่งยากในเครือข่ายไร้สายแบบ Ad hoc ที่ไม่มีศูนย์กลางในการจัดการด้านความปลอดภัย รวมไปถึงการสูญเสียพลังงานกับการประมวลผลในการเข้ารหัส ซึ่งแตกต่างกับโพรโทคอลการค้นหาเส้นทาง CAODV ที่ไม่จำเป็นต้องมีศูนย์กลางในการจัดการ โหนดสามารถตรวจสอบโหนดเพื่อนบ้านได้ด้วนตนเอง และไม่จำเป็นต้องมีการประมวณผลที่ซับซ้อน (3) การตรวจสอบการส่งข่อมูลต่อของโหนดเพื่อนบ้าน เช่น การใช้กระบวนการ Watchdog โหนดในเครือข่ายจำเป็นต้องพร้อมในการรับข้อมูลอยู่เสมอ โดยจะทำการฟังโหนดเพื่อนบ้านในการส่งข้อมูลต่อ โหนดจะต้องสูญเสียพลังงานและทรัพยากรในการจัดการกับทุกๆข้อมูลที่มีการส่ง ซึ่งแตกต่างกับโพรโทคอลการค้นหาเส้นทาง CAODV ที่จะทำการตรวจสอบเส้นทางโดยการส่งข้อความควบคุมจากโหนดปลายทางกลับมายังเส้นทางการสื่อสารเท่านั้น จึงทำให้การใช้พลังงานน้อยกว่ากระบวนการ Watchdog และข้อจำกัดของกระบวนการ Watchdog คือไม่สามารถตรวจสอบการส่งต่อได้เมื่อเกิดการชนกันของข้อมูล (4) การตรวจนับและตรวจสอบจำนวนการส่งข้อมูล อย่างโพรโทคอล HSAM และ E-HSAM ได้ใช้การนับจำนวนข้อมูลที่ส่งแล้วนำมาเปรียบเทียบกับข้อมูลที่ตอบกลับจากโหนดปลายทาง กระบวนการทั้ง 2 กำหนดอัตราการสูญหายไว้ที่ร้อยละ 20 แต่อย่างไรก็ตามกระบวนการนี้ไม่สามารถระบุได้ว่าโหนดใดเป็นโหนดหลุมดำ เพราะค่าที่ทำการนับทำการนับจากโหนดต้นทาง และตอบกลับจากโหนดปลายทางเท่านั้น ดังนั้นโหนดระหว่างทางจึงไม่มีส่วนในการจัดการเส้นทาง ซึ่งแตกต่างกับโพรโทคอลการค้นหาเส้นทาง CAODV ที่สามารถระบุโหนดที่ทำการโจมตีได้โดยทุกโหนดในเส้นทางจะทำการตรวจสอบโหนดถัดไปที่ส่งข้อมูลด้วยตนเอง โดยใช้ระบบความน่าเชื่อถือในการตัดสินใจ (5) การส่งข้อความจากโหนดปลายทางอย่าง โพรโทคอลการค้นหาเส้นทาง RAODV มีการจัดการก็ต่อเมื่อโหนดได้รับข้อความควบคุม RREP มากกว่า 1 ข้อความ ซึ่งโหนดจะทำการตรวจสอบเส้นทางเพื่อหาเส้นทางที่น่าเชื่อถือ โดยการส่งข้อความควบคุม RRDU ไปยังโหนดปลายทาง ถ้าเส้นทางใดมีการตอบกลับ RRDU-Reply ที่มาจากโหนดปลายทางนั้นมีความน่าเชื่อถือ เมื่อพิจารณาข้อจำกัดของโพรโทคอลการค้นหาเส้นทา RAODV มีข้อจำกัดอย่างมากในการตรวจสอบเส้นทางเพียงเส้นทางเดียว ซึ่งในกรณีของโพรโทคอลการค้นหาเส้นทาง CAODV จะสามารถตรวจสอบ แม้จะมีเส้นทางการสื่อสารจากโหนดหลุมดำ และ (6) การจัดเก็บข้อมูลจากข้อความควบคุม RREP กระบวนการนี้จะทำการเก็บข้อมูลต่างๆ จากข้อความ RREP เมื่อได้รับข้อความควบคุม RREP จากโหนดหลุมดำ จะมีข้อมูลแตกต่างไปจาก RREP ที่เคยได้รับจึงทำการปฏิเสธข้อความควบคุม RREP ของโหนดหลุมดำ เมื่อ

พิจารณากระบวนการนี้มีข้อจำกัดโดยเฉพาะในกรณีที่เริ่มต้นสร้างเครือข่าย ซึ่งจะทำให้โหนดไม่มีข้อมูลจาก RREP นำไปพิจารณา ซึ่งในกรณีนี้ไม่ส่งผลต่อโพรโทคอลการค้นหาเส้นทาง CAODV ที่สามารถทำการตรวจสอบได้

เมื่อเปรียบเทียบกับกระบวนการต่างๆ โพรโทคอลการค้นหาเส้นทาง CAODV สามารถจัดการกับการโจมตีแบบหลุมดำได้ ทั้งในกรณีที่ เริ่มสร้างเครือข่ายไร้สายแบบ Ad hoc รวมไปถึงการตรวจสอบในขณะที่มีการส่งข้อมูล และไม่มีข้อจำกัดในการตรวจสอบเส้นทาง แม้จะมีเพียงเส้นทางการสื่อสารให้เลือกเพียงเส้นทางเดียว ประกอบกับการใช้พลังงานและทรัพยากรของโหนดที่ใช้เพิ่มเติมจากโพรโทคอลการค้นหาเส้นทาง มีเพียงการจัดการกับความน่าเชื่อถือในเส้นทางการสื่อสารเท่านั้น ซึ่งแตกต่างกับกระบวนการที่ทำการตรวจสอบโหนดเพื่อนบ้านอยู่ตลอดเวลาอย่างกระบวนการ Watchdog และได้ทำการทดสอบโพรโทคอลการค้นหาเส้นทาง CAODV ด้วยการจำลองด้วยโปรแกรมจำลองเครือข่าย NS-2

เมื่อทำการทดสอบวัดผลกระทบจากการโจมตีแบบหลุมดำในเครือข่ายที่ใช้โพร-โทคอลการค้นหาเส้นทาง AODV การโจมตีแบบหลุมดำลดค่าสมรรถนะของเครือข่ายถึงร้อยละ 54.82 แต่ในเครือข่ายที่ใช้โพรโทคอลการค้นหาเส้นทาง CAODV ผลกระทบจากการโจมตีแบบหลุมดำส่งผลทำให้ค่าสมรรถนะของเครือข่ายลดลงเพียงร้อยละ 3.86 เท่านั้น แต่อย่างไรก็ตามการจัดการด้านความน่าเชื่อถือของโพรโทคอลการค้นหาเส้นทาง CAODV เพิ่มภาระงานให้แก่เครือข่ายเฉลี่ยร้อยละ 14.7 ดังนั้นโพรโทคอลการค้นหาเส้นทาง CAODV จึงเหมาะสมกับเครือข่ายไร้สายแบบ Ad hoc ในการจัดการกับการโจมตีแบบหลุมดำ

5.3 ปัญหาและอุปสรรคของการทำวิทยานิพนธ์

ปัญหาของเครือข่ายไร้สายแบบ Ad hoc คือการกำหนดและควบคุม ตัวแปรที่ส่งผลต่อค่าสมรรถนะของเครือข่าย จึงทำให้เป็นเรื่องที่ยุ่งยากในการกำหนดค่าตัวแปรต่างๆที่ใช้ในการทดสอบการโจมตีแบบหลุมดำ

5.4 ข้อเสนอแนะ

งานวิทยานิพนธ์นี้มุ่งเน้นทดสอบและแสดงผลลัพธ์จากการโจมตีแบบหลุมดำ โดยพยายามที่จะลดผลกระทบจากตัวแปรอื่น ดังนั้นจึงสามารถนำไปทดสอบต่อในกรณีที่โหนดมีการเคลื่อนที่หรือมีปัจจัยอื่นเข้ามาเกี่ยวข้อง เพื่อพัฒนาโพรโทคอลการค้นหาเส้นทาง AODV ต่อไป

บรรณานุกรม

[1] M. I. Chlamtac, M. Conti, and J. J.-N. Liu, “Mobile Ad Hoc Networking: Imperatives and Challenges,” *Ad Hoc Networks*, Vol. 1, No. 1, pp. 13–64, 2003.

[2] H. Bakht, “Survey of Routing Protocols for Mobile Ad-hoc Network,” Int. J. of Information and Communication Technology Research, Vol. 1, No. 6, pp. 258-270, 2011.

[3] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destinaion-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” *ACM SIG-COMM*, 1994.

[4] C. E. Perkins, E. M. Belding-Royer and S. R. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561, 2003.

[5] H. Deng, W. Li and D. P. Agrawal, “Routing Security in Wireless Ad Hoc Networks, *IEEE Communications Magazine*”, pp. 70-75, 2002.

[6] K. Lakhani, H. Bathla and R. Yadav, “A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET,” *Int. Journal of Computer Science and Network Security*, Vol. 10, No. 5, pp. 40-45, 2010.

[7] M. Raza and S. I. Hyder, “A Forced Routing Information Modification Model for Preventing Black Hole Attacks in Wireless Ad Hoc Network,” *Proc. of 2012 9th Int. Bhurban Conf. on Applied Sciences & Technology (IBCAST),* pp. 418-422, 2012.

[8] IEEE 802.16 Wireless Man, IEEE Standard, 2002.

[9] IEEE 802.11 Wireless Lan, IEEE Standard, 2003.

[10] M. G. Zapata, “Secure Ad hoc On-Demand Distance Vector Routing,” Mobile Computing and Communications Review, Vol. 6, No. 3, pp. 106-107, 2006.

[11] K. Lakhani, H. Bathla and R. Yadav, “A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET,” *IJCSNS Int. J. of Computer Science and Network Security*, Vol. 10, No. 5, May 2010.

[12] P. K. Singh and G. Sharma, “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET,” *IEEE 11th Int. Conf. on Trust, Security and Privacy in Computing and Communications*, pp. 902-906, 2012.

[13] G. S. Mamatha and S. C. Sharma, "A Highly Secured Approach against Attacks in MANETs", *Int. J. of Computer Theory and Engineering*, Vol. 2, No. 5, 2010.

[14] M. S. Obaidat, I. Woungang , S. K. Dhuramdher and V. Koo, "Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad Hoc Networks," *2012 Int. Conf. on Computer, Information and Telecommunication Systems (CITS)*, pp. 1-5, 2012.

[15] S. Khurana, N. Gupta, and N. Aneja, "Reliable Ad-hoc On-demand Distance Vector Routing Protocol," *Int. Conf. on Systems and Int. Conf. on Mobile Communications and Learning*, pp. 98-103, 2006.

[16] S. S. Ramaswami and S. Upadhyaya, "Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing," *2006 IEEE Information Assurance Workshop*, pp. 253-260, 2006.

[17] N. Mistry, D. Jinwala and M. Zaveri, "Improving AODV Protocol against Blackhole Attacks," *Proc. Int. Multi Conf. of Engineers and Computer Scientists*, Vol.11, pp.1034-1039, 2010.

[18] T. Camp, J. Boleng and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *Wireless Communication & Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking*: Research, Trends and Applications, Vol. 2, No. 5, pp. 483-502, 2002.

[19] J. Haas, "A new routing protocol for the reconfigurable wireless networks", *Proc. of IEEE 6th Int. Conf. on Universal Personal Communications*, pp. 562–566, 1997.

[20] L.Zhou and Z. J.Haas, "Securing Ad Hoc Networks," *IEEE network*, special issue on network security, 1999.

[21] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Networks* 3, pp. 69-89, 2005.

[22] H. Yang, H. Lua and F. Ye, "Security in Mobile Ad hoc Network: Challenges and Solution", *IEEE communications*, 2004.

[23] B. Kannhavong, H. Nakayama, Y. Nemoto and N. Kato, "A Survey of Routing Attack in Mobile Ad hoc Networks," *Wireless Communications*, IEEE 14, No. 5, pp.85-91, 2007.

[24] G. Peng and Z. Chuanyun, “Routing Attacks and Solutions in Mobile Ad hoc Networks,” in *Communication Technology*, 2006.

[25] L.Abusalah, A. Khokhar and M. Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols,” *IEEE Communication Survey & Tutorials*, Vol. 10, No. 4, 2008.

[26] P. Yi, Z. Dai, S. Zhang and Y. Zhong, “A New Routing Attack in Mobile Ad Hoc Networks,” *Int. J. Information Technology*, Vol. 11, No. 2, 2005.

[27] A. Bala, R. Kumari and J. Singh, “Investigation of Blackhole Attack on AODV in MANET,” *Journal of Emerging Technologies in Web Intellingence*, Vol. 2, No. 2, pp. 96-100, 2010.

[28] Y. C. Hu, A. Perrig, and D. Johnson, “Wormhole Attacks in Wireless Networks,” *IEEE JSAC*, Vol. 24, No. 2, 2006.

[29] C. Adjih, D. Raffo, and P. Muhlethaler, “Attacks Against OLSR: Distributed Key Management for Security,” *2nd OLSR Workshop*, 2005.

[30] N. Uushona and W. T. Penzhorn, “Towards the Security of Routing in Ad Hoc Networks,” *IEEE ISIE 2005*, 2005.

[31] I. Aad, J. P. Hubaux and E. W. Knightly, “Denial of Service Resilience in Ad Hoc Networks,” *Proceedings of the 10th annual Int. Conf. on Mobile computing and networking*, pp. 202-215, 2004.

[32] R. Mahmood and A. I. Khan, “A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks,” in *High Capacity Optical Networks and Enabling Technologies*, 2007.

[33] M. Allman, V. Paxson and W. Stevens, “TCP Congestion Control,” RFC 2581, 1999.

[34] N. C. Valler, B. Aditya, H. Thong, M. Faloutsos and C.Faloutsos, “Epidemic Spread in Mobile Ad Hoc Networks Determining the Tipping Point,” *10th Int. IFIP TC 6 Networking Conf.*, pp. 266-280, 2011.

อภิธานศัพท์

ตาราง ก-1 อภิธานศัพท์

ศัพท์เดิม	**อภิธานศัพท์**
Wireless networks	เครือข่ายการสื่อสารไร้สาย
Base station	สถานีฐาน
Ad hoc networks	เครือข่ายไร้สายแบบ Ad hoc
Peer to peer	สื่อสารกันได้โดยตรง
Source node	โหนดต้นทาง
Destination node	โหนดปลายทาง
Routing protocol	โพรโทคอลการค้นหาเส้นทาง
Throughput	ค่าสมรรถนะของเครือข่าย
Credit	ความน่าเชื่อถือ
Hidden node	ปัญหาโหนดที่มองไม่เห็น
Wake up	สภาวะตื่น
Destination sequence number	ค่าเลขลำดับปลายทาง
Denial of service	ขัดขวางการให้บริการ
Dynamic	พลศาสตร์
Bandwidth	ช่องสัญญาณการสื่อสาร
Overhead	ภาระงาน
Control message	ข้อความควบคุม
Routing discovery	กระบวนการค้นหาเส้นทาง
Routing maintenance	กระบวนการบำรุงรักษาเส้นทาง
Broadcast	การส่งกระจาย
Loop	การวน
Unicast	การส่งแบบโดยตรง
Sleep	สภาวะหลับ
Local repair	กระบวนการซ่อมแซมเฉพาะที่
Availability	ความสามารถให้บริการ

ตาราง ก-1 อภิธานศัพท์ (ต่อ)

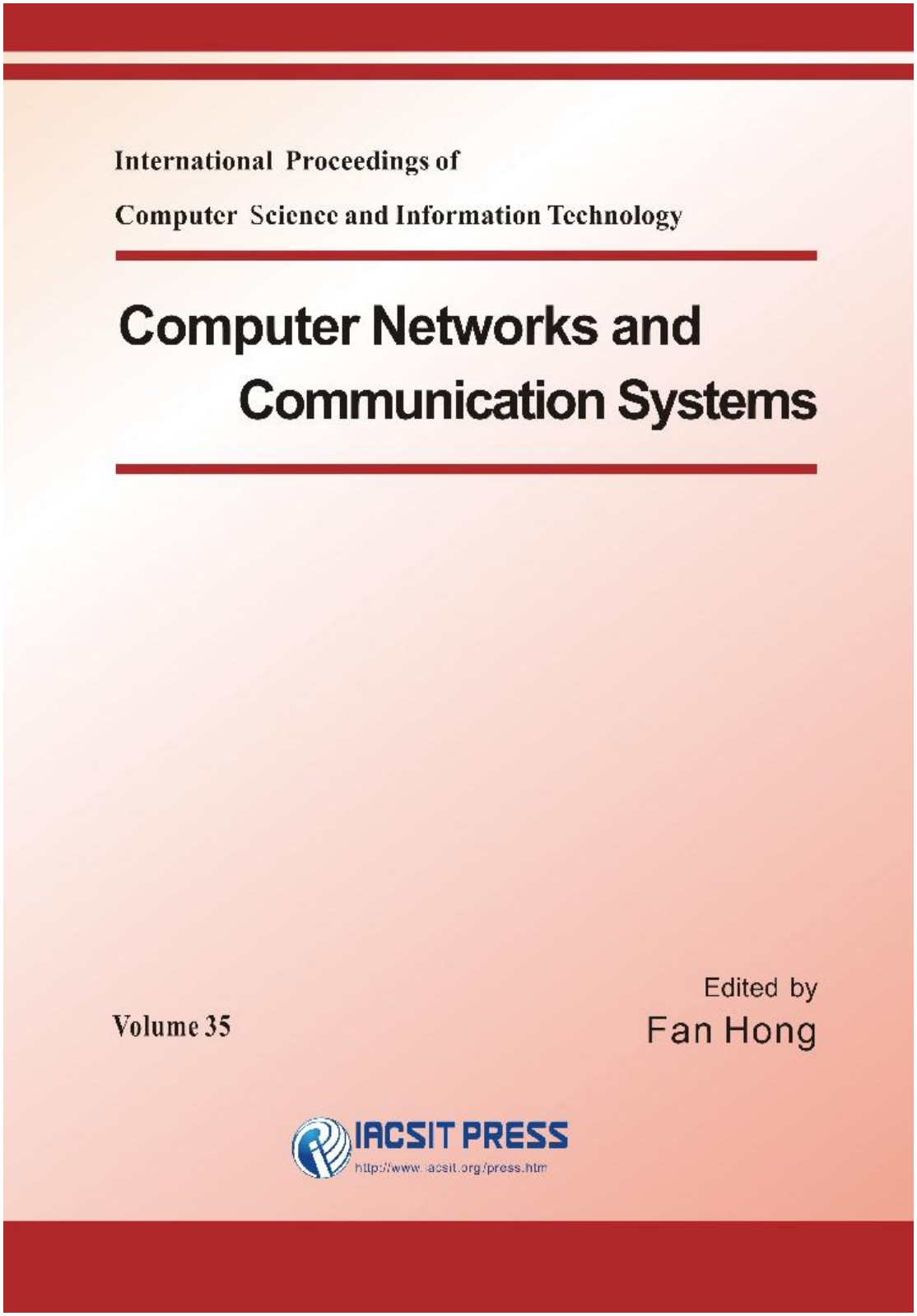
ศัพท์เดิม	**อภิธานศัพท์**
Integrity	ความถูกต้องสมบูรณ์
Confidential	การรักษาความลับ
Authentication	การพิสูจน์ตัวตน
Non-repudiation	การไม่สามารถปฏิเสธความรับผิดชอบ
Selfish node	โหนดเห็นแก่ตัว
Passive attack	การโจมตีแบบไม่แก้ไขข้อมูล
Active attack	การโจมตีแบบแก้ไขข้อมูล
Physical layer	ชั้นกายภาพ
Link layer	ชั้นเชื่อมโยง
Network layer	ชั้นเครือข่าย
Drop	การทิ้งข้อมูล
Transport layer	ชั้นขนส่ง
Application layer	ชั้นโปรแกรมประยุกต์
Blackhole attack	การโจมตีแบบหลุมดำ
Wormhole attack	การโจมตีแบบรูหนอน
Replay attack	การโจมตีแบบส่งซ้ำ
Information Disclosure attack	การโจมตีโดยไม่ปกปิดข้อมูล
Partition attack	การโจมตีโดยการแบ่งเครือข่าย
Blacklist	บัญชีดำ
Delay	เวลาหน่วง
Neighbor attack	การโจมตีโดยโหนดเพื่อนบ้าน
Blackhole node	โหนดหลุมดำ
Collision	การชนกันของข้อมูล
Packet	แพ็กเก็ต
Credit limit	ค่าจำกัดความน่าเชื่อถือ

ภาคผนวก

ภาคผนวก ก
การตีพิมพ์เผยแพร่วิทยานิพนธ์

CNCS 2012: 2012 International Conference on Computer Networks and Communication Systems

April 7-8 2012, at Kuala Lumpur, Malaysia


International Proceedings of
Computer Science and Information Technology
Computer Networks and Communication Systems
Volume 35
Edited by
Fan Hong
IACSIT PRESS
http://www.iacsit.org/press.htm

2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)
IPCSIT vol.35(2012) © (2012) IACSIT Press, Singapore

CAODV Free Blackhole Attack in Ad Hoc Networks

Watchara Saetang [1] and Sakuna Charoenpanyasak [2]

Center of Excellent in Wireless Sensor Networks (CoE-WSN)

Department of Computer Engineering, Faculty of Engineering

Prince of Songkla University, Hatyai, Songkhla, Thailand

[1] st_watchara@hotmail.com, [2] jsakuna@coe.psu.ac.th

Abstract. Ad hoc networks are the network that having no infrastructure or base station. A node communicates directly to the others with its transmission range. The essential requirement in ad hoc network is the security. The well-known attack is the black hole that having a malicious node advertised itself as a shortest path. This will decrease a throughput of network. In this paper, Credit based on Ad hoc On-demand Distance Vector (CAODV) routing protocol is proposed to detect and eliminate the blackhole attack. The NS-2 simulator has been used to analyze both CAODV and AODV when the blackhole attack is injected in the network. By using our proposed protocol, we can achieve the throughput improvement at about 47 percentages.

Keywords: Ad hoc networks, AODV, Blackhole attack and CAODV

1. Introduction

The infrastructureless is a major characteristic of the ad hoc networks. Each node has communicated as a peer to peer connection and having a direct connection with the neighbor nodes with in their transmission range. The network is a self-configuration that having abilities to discover and maintain the route without manual management. Moreover, ad hoc networks can also perform multi-hop wireless networks.

Currently, several efficient routing protocols have been proposed [1]. Ad hoc On-demand Distance Vector (AODV) [2] routing protocol is widely used in ad hoc networks. AODV is a reactive routing protocol that only requested a route when the node requests. Route discovery operation is used to discover the route by using Route Request (RREQ) and Route Reply (RREP) control messages. When a source node needs to send the data to the destination node, it will broadcast RREQ to the others. When a destination node receives RREQ, the RREP will be returned to the source node. Then, source node receives RREP and uses the information in RREP without checking the correctness of routing information. Therefore, during a route discovery in AODV, the blackhole attack can harm the network easily.

The blackhole attack has a high opportunity to occur in ad hoc networks, especially in the AODV [3]. The blackhole node is easily able to crash the network became each node assumes to be trusted. In the route discovery, the blackhole node replies the RREP with fake information back to the source node, as soon as the RREQ is received. In this case, the source node will take that information to select the route immediately. This leads to pass the data to the destination via the blackhole node. The blackhole attack is one of Denial of Services (DoS), therefore, it is powerful to decrease the throughput of the networks. The several detection blackhole attack methods have been proposed such as the anomaly-based detection techniques [4] and promiscuous monitoring approaches [5]. However, these methods have some weaknesses such as complicate computation and consuming the extra resources.

This paper proposes Credit based on AODV (CAODV) routing protocols to protect the network from blackhole attack. Our CAODV uses credit for checking the next hop node. CAODV will initial a credit to the

next hop node in the route discovery phase. When the existed node in the route table sends one packet, it will decrease one credit of the next hop node. The destination node will send Credit Acknowledge (CACK) to the source node as soon as it receives the data packet. The intermediate node receives CACK and increases a credit of the next hop if the next hop can be trusted. On the other hand, if the destination node cannot receive the data packet and nodes in the path cannot receive CACK, the credit will be decreased to zero. This means the next hop node cannot to be trusted and also be marked as a blacklist node.

The remaining of this paper is organized as follows. The AODV protocol is explained in Section 2. The blackhole attack is described in Section 3. Our proposed protocol named CAODV is introduced in Section 4. The simulation results using NS-2 are analyzed in Section 5 to show the comparison between AODV and CAODV. The last section is the conclusions.

2. Ad hoc On-demand Distance Vector (AODV) routing protocol

The AODV routing protocol is one kind of the reactive routing protocol. The route is thus requested only when needed. A source node broadcasts a RREQ when the data is required to send to a destination node. A route is created when each intermediate node receives RREQ if the intermediate node is not the destination node and never received this RREQ before, it will broadcast the RREQ. The RREP is unicast to the source node when the receiving node is the destination node. The source node will check and choose the shorted path when it receives more than one RREP. The route is only updated if the hop count in RREP is smaller than the existing route in route table. The route discovery operation in AODV shows in Fig. 1.

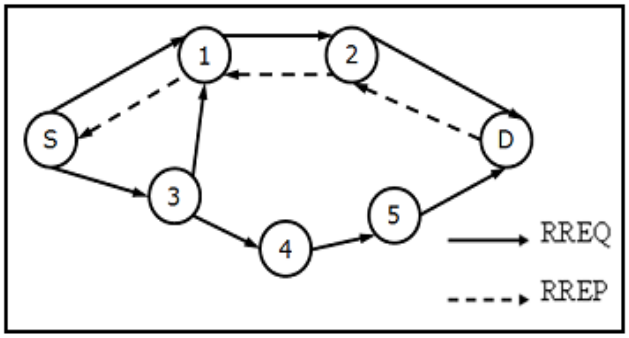


Fig. 1 Route discovery in AODV

From Fig. 1, the example of AODV route discovery is shown. Node S is a source node and node D is a destination node. In this scenario, node S needs to send the data to node D. Node S broadcasts RREQ to its neighbour (node 1 and node 3). Both node 1 and 3 do not have route to node D, therefore they broadcast to its neighbour immediately. This process has been repeated until node D receives RREQ. Node D will unicast RREP back to node S via node 2 and 1, respectively. When node S receives RREP, the communication path to destination is completed.

Another operation in AODV is route maintenance. Route Error (RERR) is used to notify to the source node when route is broken. Route discovery is invoked again. If the route is failed nearly the destination node, the local repair is deployed. AODV is a good routing protocol to manage or discovery the route in ad hoc networks; AODV has more vulnerable to attack. For example, the fake information can be found in RREP if a malicious node pretends to be a destination node and generates RREP to a source node. Because of AODV lacking a mechanism to handle or detect the false information in RRER, this kind of attack can easily occur in ad hoc networks.

3. Blackhole attack in AODV

The blackhole attack is easily to found in AODV routing protocol. The attack is occurred when a route discovery in AODV is used by a source node or a local repair is invoked. Therefore, a source or intermediate node starts to broadcast RREQ to its neighbor. When the malicious node receives RREQ, it sends the fake routing information back to the source node claiming that it is an optimum route. When the source node

receives RREP with the fake route information containing a smallest hop count, the source node will create invalid path to a malicious node. All data packets will be dropped by malicious node when the source node transmits the data. Therefore, a throughput of networks is greatly reduced because of the blackhole attack.

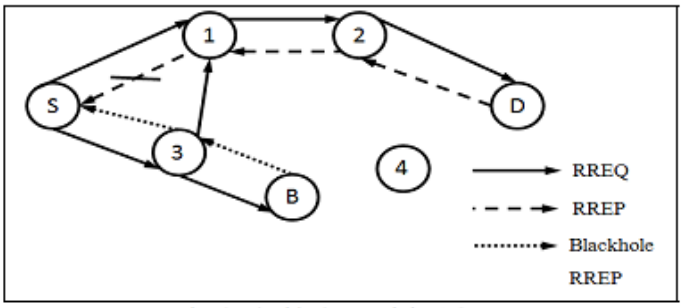


Fig. 2 Blackhole attack in AODV

Fig. 2 shows an example of blackhole attack on AODV in MANETs. Node S is a source node, node D is a destination node and node B is a blackhole node. Node S needs to send data to node D. Then AODV route discovery is used. Node S starts to broadcast RREQ to the neighbour nodes. When node B receives RREQ form node 3, it replies RREP with fake information to node S immediately. In this case, the hop count is equal to 1. When node S receives RREP, it will create the path to node B instead of the destination node. The RREP from node D will be dropped because the hop count of malicious node is smaller than node D. When node S starts to send the data packets to destination, all data will be dropped.

The routing control message in AODV has not been checked in ad hoc networks. Therefore, the blackhole attack is easily occurred and the performances of the ad hoc networks are reduced. H. A. Bala and et al. has studied the impact of blackhole attack in ad hoc networks based on AODV routing protocol. In their experiments, the network consist 20 mobile-nodes and one blackhole node. The result of blackhole attack shows that the packet is dropped up to 90 percentages [6].

Several algorithms to handle the blackhole attack have been proposed recently. For example, K. Lakhani et al. proposed the Watchdog algorithm to check the next hop node that sending the data packet by overhearing all of the packets [7]. By using their solution, the throughput was increased by 10-18 percentages. Unfortunately, nodes in the network have to wake up all-time. This consumed high power dissipation. This consumed both resource and power more than the original AODV. S. khurana proposed Reliable Ad hoc On-demand Distance Vector (RAODV) [8] using Reliable Route Discovery Unit (RRDU). This mechanism was deployed when source node received the multiple RREPs. When a destination receives RRDU, RRDU-reply was replied to the source node. The source node selected the path that having the RRDU-reply. Unfortunately, RAODV cannot detect the blackhole attack when there was only one route to destination. N. Mistry et al. proposed a source node to keep the multiple RREPs for checking information in RREP [9]. When the source node received RREP, the destination sequence number in RREP and the information threshold were compared. However, the blackhole attack can still occur when the destination sequence number and threshold was not different. As we can see, the some algorithms can detect and protect the blackhole but they took a lot of resources. Moreover, in some algorithms the blackhole cannot be solved. Thus, we propose CAODV to get rid of the blackhole attack without consuming the extra resources.

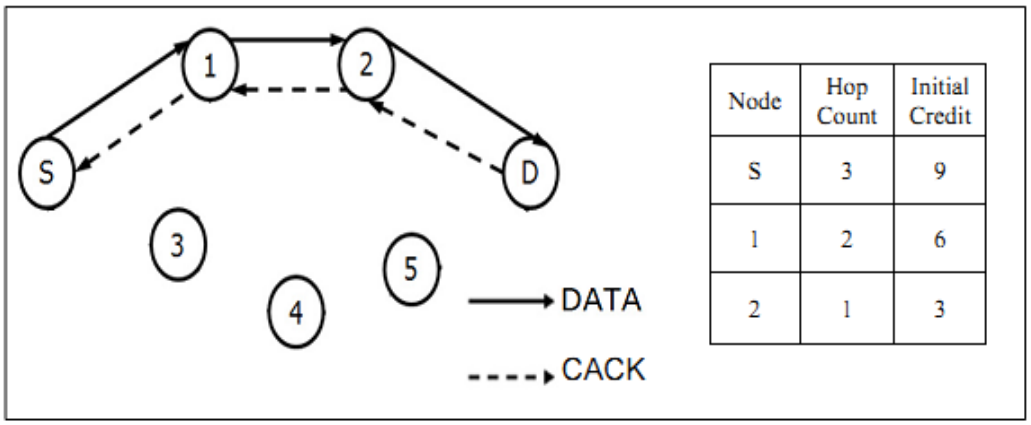
4. The proposed protocol – Credit based on AODV (CAODV)

To protect a blackhole attack in AODV, CAODV is therefore introduced in this paper. We deploy a credit mechanism to check the next hop whether it can be trusted or not. The credit is initiated in a route discovery phase. The credit is defined as followings:

$$\text{Credit} = \begin{cases} \text{Hop count}*3 & \text{; initial state} \\ \text{Credit}+2 & \text{; when destination node sends credit acknowledge} \\ \text{Credit}-1 & \text{; send 1 packet} \end{cases}$$

Note: $\text{Credit}_{\text{Max}} = 5*(\text{Hop count}+2)$

At the beginning, a source node broadcasts RREQ to other nodes until a destination node or node having a route to destination replies RREP back to source. The receiving node will assign a credit to the next hop node or who sent RREP. When a node in the path sends one packet, one credit is deducted from the next hop node. As soon as a destination node receives data packet, it will send Credit Acknowledge (CACK) back to a source node. A node within a way back will increase credit of the next hop by 2 to indicate a higher trust level of the next hop. On the other hand, credit will be decreased if a node cannot receive CACK. The node will be untrusted and marked as a blacklist, when a credit reaches zero.



Node	Hop Count	Initial Credit
S	3	9
1	2	6
2	1	3

Fig. 3 Example of CAODV routing protocol

Fig. 3 shows an example of a credit mechanism in CAODV. Node S is a source node that sends data to node D. In this scenario, the route discovery is used and the path contains node S, node 1, node 2 and node D. The credit is initialled by using a hop count multiplied by 3. Thus node 1 is the next hop of node S having 9 credits at the beginning. The credit in node 1 and 2 is decreased by 1 when the data is transmitted to node D. Node D will return CACK back by using the reserved path to source node when the data is received. Node with the path will increase a credit after it receives CACK. Finally, node S adds 2 credits to node 1, when it can receive the data packet. This made the credit of node 1 to be 10 credits. However, the credit has limited to the hop count multiplied 5 to limit the number of data packet when is a malicious node. However, the blackhole attack in CAODV is limited by credit of next hop. When nodes in the path cannot to receive CACK form the destination node, the credit of next hop will become zero. This means the next hop node is blackhole node. The next hop will be a blacklist node. Thus, the packets from a blacklist node will be dropped, eventually.

5. The Simulation Results

This section will show and describe the comparison results of the throughput between AODV and CAODV when the blackhole attack is injected to the networks. This experiment has been done on Networks Simulator2 (NS-2). We declare to use 30 nodes with 2 connections in the networks. In the first connection, there is no attack and start at 10 s. The second connection will have a blackhole attack and start at 20 s. The throughput results of both AODV and CAODV are shown in Fig. 4 and 5, respectively.

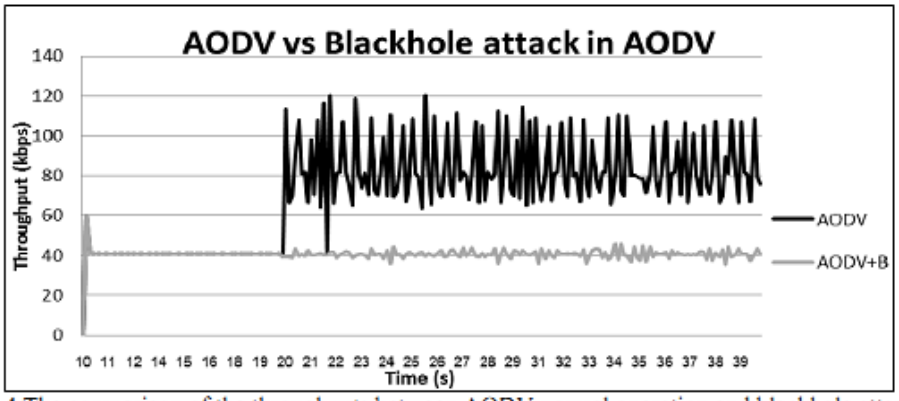


Fig. 4 The comparison of the throughputs between AODV normal operation and blackhole attack

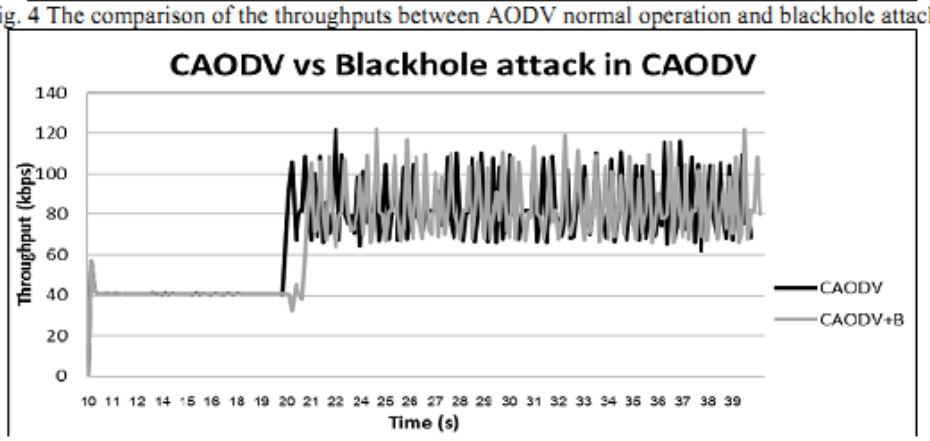


Fig. 5 The comparison of the throughputs between CAODV normal operation and blackhole attack

Fig. 4, the comparisons of the throughputs between AODV with normal operation and AODV with blackhole attack. The average throughput of AODV in normal operation is 70.51 kbps while the blackhole attack has a throughput at 40 kbps. In the scenario of CAODV, a throughput of CAODV with normal operation is 69.89 kbps and when it is attacked by blackhole attack, the average throughput is 69.15 kbps as shown in Fig. 5. From the result in Fig. 5 shows that the blackhole attack cannot harm the network when CAODV is employed. Meanwhile, the blackhole attacks the network that used AODV and decrease throughput at about 47 percentages.

6. Conclusions

According to the nature of AODV routing protocol in ad hoc networks, the blackhole attack is able to harm and decrease a throughput of network, especially in the route discovery phase. Therefore, CAODV has been proposed in this paper. By using a credit mechanism, we can detect and protect a malicious node before the blackhole attack is occurred. We have successful demonstrated that the blackhole cannot attack the networks when our CAODV is employed. In contrast with CAODV, we found the average throughput of the original AODV is decreased at about 40 percentages when the network is attacked by the blackhole.

7. References

[1] S. H. H. N. Ghazani, J. J. Lotf and R. M. Alguliev, "A New Survey of Routing Algorithm in Ad Hoc Networks," 2nd Int. Conf. on Computer Engineering and Technology, vol. 3, pp. 684-688, 2010.

[2] C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Mobile Computer Systems and Applications, pp. 90–100, 1999.

[3] H. Deng, W. Li and D. P. Agrawal, "Routing Security in Wireless Ad Hic Networks," IEEE Communications Magazine, pp. 70-75, 2002.

[4] Y. A. Huang and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," 7th Int. Symposium on Recent Advances in Intrusion Detection, pp. 125-145, 2005.

[5] R. A. R. Mahmood and A. I. Khan, "A Survey on Detecting Black Hole Attack in AODV based Mobile Ad Hoc Networks," Int. Symposium on High Capacity Optical Networks and Enabling Technologies, pp. 18-24, 2007.

[6] H. A. Bala, R. Kumari and J. Singh, "Investigation of Blackhole Attack on AODV in MANET," Journal of Emerging Technologies in Web Intellingence, vol. 2, no. 2, pp. 96-100, 2010.

[7] K. Lakhani, H. Bathla and R. Yadav, "A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET," Int. Journal of Computer Science and Network Security, vol. 10, pp. 40-45, 2010.

[8] S. Khurana, N. Gupta, and N. Aneja, "Reliable Ad-hoc On-demand Distance Vector Routing Protocol," Int. Conf. on Systems and Int. Conf. on Mobile Communications and Learning, pp. 98-103, 2006.

[9] N. Mistry, D. Jinwala and M. Zaveri, "Improving AODV Protocol against Blackhole Attacks," Proc. Int. Multi Conf. of Engineers and Computer Scientists, vol.11, pp.1034-1039, 2010.

ประวัติผู้เขียน

ชื่อ สกุล นายวัชระ แซ่ตั้ง

รหัสประจำตัวนักศึกษา 5310120073

วุฒิการศึกษา

วุฒิ	ชื่อสถาบัน	ปีที่สำเร็จการศึกษา
วิศวกรรมศาสตรบัณฑิต (วิศวกรรมคอมพิวเตอร์)	มหาวิทยาลัยสงขลานครินทร์	2552

ทุนการศึกษา (ที่ได้รับในระหว่างการศึกษา)

ทุนการศึกษาตรี-โท 5 ปี คณะวิศวกรรมศาสตร์

การตีพิมพ์เผยแพร่ผลงาน

W. Saetang and S. Charoenpanyasak, “CAODV Free Blackhole Attack in Ad hoc Networks,” *Int. Conf. on Computer Networks and Communication Systems (CNCS 2012)*, Vol. 35, pp. 63-68, April 2012.