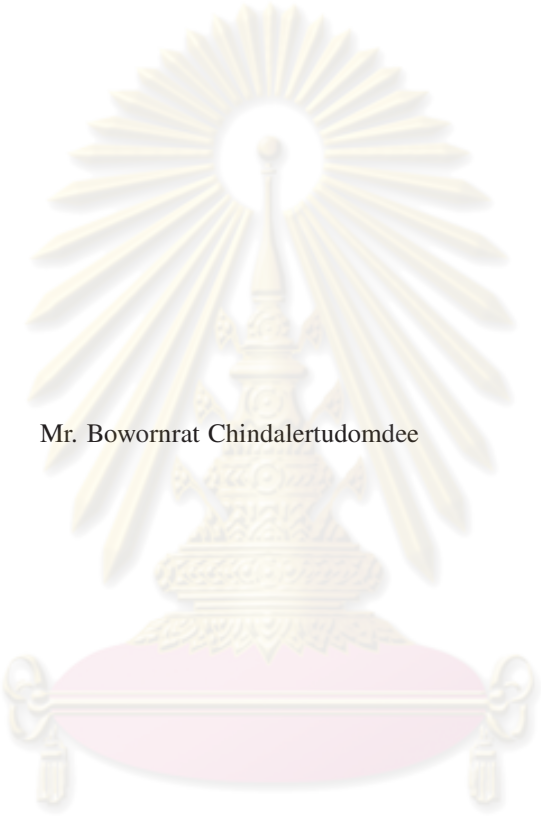
การใช้ทฤษฎีเกมเพื่อวิเคราะห์การจัดเส้นทางแบบเฟ้นสุ่มในโครงข่ายไร้สายแบบเมช ที่มีการรบกวนและการดักฟังสัญญาณ

นายบวรรัตน์ จินดาเลิศอุดมดี

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2552

GAME THEORETICAL ANALYSIS OF STOCHASTIC ROUTING IN WIRELESS MESH NETWORK WITH JAMMING AND EAVESDROPPING

Mr. Bowornrat Chindalertudomdee



A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Electrical Engineering
Department of Electrical Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2009

หัวข้อวิทยานิพนธ์	การใช้ทฤษฎีเกมเพื่อวิเคราะห์การจัดเส้นทางแบบเฟ้นสุ่มในโครงข่ายไร้สายแบบเมชที่มีการรบกวนและการดักฟังสัญญาณ
โดย	นายบวรรัตน์ จินดาเลิศอุดมดี
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.เชาวน์ดิศ อัศวกุล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. ทับทิม อ่างแก้ว)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.เชาวน์ดิศ อัศวกุล)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. ชัยเชษฐ์ สายวิจิตร)

..... กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร. ภูมิพัฒ แสงอุดมเลิศ)

บวรรัตน์ จินดาเลิศอุดมดี: การใช้ทฤษฎีเกมเพื่อวิเคราะห์การจัดเส้นทางแบบเฟ้นสุ่มในโครงข่ายไร้สายแบบเมชที่มีการรบกวนและการดักฟังสัญญาณ (GAME THEORETICAL ANALYSIS OF STOCHASTIC ROUTING IN WIRELESS MESH NETWORK WITH JAMMING AND EAVESDROPPING), อ. ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ.ดร. เชาวน์ดิศ อัศวกุล, 52 หน้า

ปัจจุบันโครงข่ายไร้สายแบบเมชได้รับความสนใจเป็นอย่างมากเนื่องจากข้อดีของโครงข่ายที่มีหลายประการ ทั้งการติดตั้งที่ง่าย รวดเร็วและประหยัดต้นทุน แต่การสื่อสารผ่านตัวกลางไร้สายทำให้ข้อมูลสำคัญถูกดักฟังได้ง่าย ในขณะที่การตรวจจับการดักฟังข้อมูลกระทำได้ยาก นอกจากนี้การสื่อสารผ่านตัวกลางไร้สายยังเสี่ยงต่อการถูกส่งสัญญาณรบกวนการรับส่งข้อมูลของโนดในโครงข่ายอีกด้วย

ในวิทยานิพนธ์ฉบับนี้ได้นำเสนอระเบียบวิธีใหม่ในการวิเคราะห์ และหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดโดยใช้ทฤษฎีเกมซึ่งสามารถป้องกันการดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมชต่าง ๆ ภายในระเบียบวิธีที่นำเสนอได้มีการปรับปรุงวิธีการจำลองการโจมตีให้สอดคล้องกับการส่งข้อมูลแบบไร้สายมากขึ้นโดยคำนึงถึงตำแหน่งซึ่งเหมาะสมที่สุดของผู้โจมตี นอกจากนั้นระเบียบวิธีที่นำเสนอยังสามารถวิเคราะห์หาค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตี (expected number of secure sessions, ESS) ขั้นต่ำที่พึงได้ในโครงข่ายไร้สายแบบเมช ผลการทดสอบแสดงให้เห็นถึงผลกระทบที่แตกต่างกันของการโจมตีทั้งสองแบบในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงผ่านตัวชี้วัด ESS นอกจากนั้นการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดจากระเบียบวิธีที่นำเสนอ สามารถป้องกันการดักฟังข้อมูลและการส่งสัญญาณรบกวนในกรณีร้ายแรงที่สุด และรับประกันจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีขั้นต่ำให้กับโครงข่ายไร้สายแบบเมชได้ รวมถึงระเบียบวิธีที่นำเสนอยังสามารถใช้วิเคราะห์ผลกระทบของการเพิ่มจำนวนเกตเวย์ในรูปแบบต่าง ๆ ซึ่งจะเป็นประโยชน์แก่การออกแบบโครงข่ายไร้สายแบบเมชให้มีระดับความปลอดภัยที่สูงขึ้นได้ในอนาคต

ภาควิชา วิศวกรรมไฟฟ้า	**ลายมือชื่อนิสิต** .....
สาขาวิชา วิศวกรรมไฟฟ้า	**ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก** .....
ปีการศึกษา 2552	

##5070575421: MAJOR ELECTRICAL ENGINEERING

KEYWORDS: WIRELESS MESH NETWORKS (WMNs) / EAVESDROPPING / JAMMING / POSITION BASED ATTACKING / STOCHASTIC ROUTING / GAME THEORY

BOWORNRAT CHINDALERTUDOMDEE : GAME THEORETICAL ANALYSIS OF STOCHASTIC ROUTING IN WIRELESS MESH NETWORK WITH JAMMING AND EAVESDROPPING, THESIS ADVISOR: CHAODIT ASWAKUL, Ph.D., 52 pp.

Nowadays, Wireless Mesh Network (WMN) has gained a lot of attention due to many advantages such as fast, easy and low-cost deployment. However, wireless transmission causes important data to be eavesdropped easily but eavesdropping is hard to detect. Using wireless medium, moreover, is prone to node jamming with radio interference.

In this thesis, we propose a new framework with game theory for analysing and finding optimal stochastic routing which can protect data from eavesdropping and jamming in wireless mesh networks. In the proposed framework, a new attacking model suitable for wireless data transmission has been formulated in terms of optimal attacker's position. Moreover, the proposed methodology can be applied to analyze for a lower bound of expected number of secure sessions (or ESS) in a wireless mesh network. Experimental results can clearly distinguish the security level indicated by ESS between uplink and downlink communications. Furthermore, optimal stochastic routing from the proposed framework can protect data from both eavesdropper and jammer in the worst case scenario. Also, this optimal stochastic routing can guarantee a lower bound for the number of secure sessions. Furthermore, the proposed framework can analyze the effect of gateway increasing in different patterns, which will be beneficial to the design of secure wireless mesh network in the future.

Department: Electrical Engineering
Field of Study: Electrical Engineering
Academic year: 2009

Student's Signature Bowornrat
Advisor's Signature C. Aswakul

กิตติกรรมประกาศ

อันดับแรกผมขอขอบคุณบิดา มารดา รวมทั้งน้องสาวของผมที่คอยให้กำลังใจ และจะอยู่เคียงข้างผมเสมอ โดยเฉพาะบิดาที่เป็นทั้งต้นแบบและเป็นผู้แนะนำให้ผมเรียนต่อซึ่งผมได้เรียนรู้หลายสิ่งหลายอย่างที่เป็นประโยชน์อย่างมาก

ขอขอบคุณ อ.เชาวน์ดิศ อัศวกุล อย่างสูงที่ให้โอกาสผมเป็นลูกศิษย์ในที่ปรึกษาซึ่งตลอดเวลาอาจารย์ได้ให้คำแนะนำต่าง ๆ ที่มากกว่าการทำวิจัย ฝึกการพรีเซนต์ รวมทั้งจัดกิจกรรมต่าง ๆ ทำให้ผมได้พัฒนาตนเองอย่างมาก นอกจากนั้นอาจารย์ยังเป็นบุคคลที่ทำให้ผมตั้งใจอยากทำงานวิจัยของตนเองออกมาดีที่สุดเท่าที่ผมจะทำได้อีกด้วย

ขอขอบคุณคณะกรรมการสอบทุกท่าน (อ.ทับทิม อ่างแก้ว อ.ชัยเชษฐ์ สายวิจิตร และอ.ภูมิพัฒ แสง-อุดมเลิศ) ที่แนะนำในประเด็นต่าง ๆ ซึ่งผมได้ใช้เป็นแนวทางในการทำวิจัยและทำให้วิทยานิพนธ์ฉบับนี้มีความสมบูรณ์ยิ่งขึ้น

ขอขอบคุณพี่มิ๊งค์ (กลิกา สุขสมบูรณ์) ตลอดเวลาที่ผ่านมาพี่มิ๊งค์พร้อมที่จะให้ทั้งคำปรึกษาที่เป็นประโยชน์กับงานวิจัยและกำลังใจที่ให้ในเวลาที่ผมรู้สึกท้อเสมอ และขอขอบคุณ อ.เป็ก (ภัทรชาติ โกมลกิติ) ที่ให้คำแนะนำที่เป็นประโยชน์กับวิทยานิพนธ์ฉบับนี้อย่างยิ่ง

ขอขอบคุณปอ เป้ที่ช่วยเหลือหลายสิ่งหลายอย่างรวมถึงเป็นเพื่อนที่ดีของผม ขอขอบคุณพี่ยอด พี่ช้าง พี่มด พี่โอ๋ พี่แน็ท ที่ให้ผมได้ร่วมทีมฟุตบอลรวมทั้งยังเป็นพี่ชายที่คอยให้กำลังใจและเสียงหัวเราะกับผมเสมอมา ขอขอบคุณพี่โบว์ พี่ตู้ พี่ตี่ พี่ต้น บิ๊ก เอื้อ ปุ๊ก เบียร์ น้องตั้ม น้องไนซ์ น้องขวัญ สัญญา รวมทั้งบุคคลอื่น ๆ ที่อาจไม่ได้พูดถึงซึ่งรวมกันเป็นสังคมที่อบอุ่น แสนดี และจะเป็นสังคมที่ผมจะรู้สึกดีที่นึกถึงตลอดไป

สารบัญ

หน้า

บทที่ หน้า

สารบัญภาพ

หน้า

หน้า

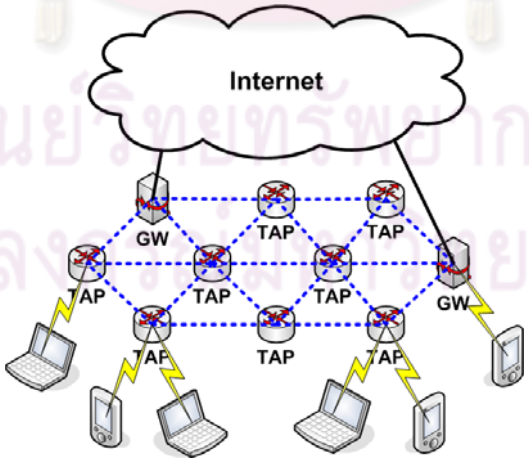
บทที่ 1

บทนำ

1.1 ความเป็นมา

โครงข่ายไร้สายแบบเมช (Wireless Mesh Network, WMN) เป็นโครงข่ายที่กำลังได้รับความสนใจอย่างมากจากทั้งผู้ให้บริการโครงข่ายและกลุ่มนักวิจัย เนื่องจากข้อได้เปรียบของโครงข่ายลักษณะนี้มีหลายประการเมื่อเทียบกับโครงข่ายไร้สายชนิดอื่น [1] โครงข่ายไร้สายแบบเมชประกอบไปด้วยโนดที่ต่อถึงกันแบบเมชผ่านตัวกลางไร้สาย การสื่อสารระหว่างโนดทำได้โดยตรงหรือส่งข้อมูลผ่านโนดข้างเคียง (neighbor node) ในลักษณะหลายช่วงเชื่อมต่อ (multi-hop) จึงทำให้โครงข่ายไร้สายแบบเมชไม่ต้องการการควบคุมจากส่วนกลาง และสามารถจัดโครงข่ายนี้เป็นกรณีเฉพาะของโครงข่ายแอดฮ็อก (ad hoc networks) ที่โนดทั้งหมดไม่มีการเคลื่อนที่ได้

การประยุกต์ใช้งานของโครงข่ายไร้สายแบบเมชสามารถทำได้หลากหลาย เช่น การให้บริการการเชื่อมต่ออินเทอร์เน็ตแบบไร้สายแก่ผู้ใช้งานที่มีการเคลื่อนที่ซึ่งเป็นการประยุกต์ใช้งานหลักของโครงข่ายนี้ [2] ถ้าหากเปรียบเทียบโครงข่ายไร้สายแบบเมชกับโครงข่าย WiFi ซึ่งให้บริการเชื่อมต่ออินเทอร์เน็ตไร้สายเช่นกัน พบว่าโครงข่ายไร้สายแบบเมชเปลี่ยนการสื่อสารจากช่วงเชื่อมต่อเดียว (single hop) มาเป็นหลายช่วงเชื่อมต่อ ทำให้โครงข่ายไร้สายแบบเมชต้องการโนดเพียงบางโนดที่ต่อกับโครงข่ายอินเทอร์เน็ตผ่านสายสื่อสาร (wired line) และโนดเพียงบางโนดนั้นจึงทำหน้าที่เป็นเกตเวย์ (Gateway, GW) ให้กับโนดที่เหลือซึ่งเรียกว่า จุดเชื่อมต่อผ่าน (Transit Access Point, TAP) ดังแสดงในรูปที่ 1.1



รูปที่ 1.1: โครงข่ายไร้สายแบบเมชเพื่อให้บริการเชื่อมต่อระบบอินเทอร์เน็ตแบบไร้สาย

ด้วยหลักการสื่อสารแบบแอดฮ็อกซึ่งใช้ตัวกลางไร้สายเป็นหลักในการรับส่งข้อมูล ทำให้การติดตั้งโครงข่ายไร้สายแบบเมชทำได้ง่าย รวดเร็ว รวมทั้งประหยัดต้นทุนในการวางสายสื่อสารอย่างมาก นอก

จากนี้การเชื่อมต่อถึงกันแบบเมชของโนดในโครงข่าย ทำให้แต่ละโนดมีเส้นทางให้เลือกใช้ในการส่งข้อมูลมากขึ้น โครงข่ายจึงมีความเชื่อถือได้ (reliability) สูงอีกด้วย ยิ่งไปกว่านั้นโครงข่ายไร้สายแบบเมชยังมีข้อได้เปรียบอีกหลายประการ เช่น ความสามารถในการขยายขนาดได้ง่าย (scalability) ความเข้ากันได้กับเทคโนโลยีที่มีมาก่อน เช่น IEEE 802.11, IEEE 802.16 เป็นต้น ทำให้ผู้ให้บริการโครงข่ายให้ความสนใจกับการประยุกต์ใช้โครงข่ายไร้สายแบบเมชกันมาก [3] เช่น โครงข่ายเชื่อมต่อภายในชุมชน (community networking), โครงข่ายบรอดแบนด์ภายในบ้าน (broadband home networking), โครงข่ายภายในองค์กร (enterprise networking) และโครงข่ายของระบบอัตโนมัติในอาคาร (building automation) เป็นต้น นอกจากการเชื่อมต่ออินเทอร์เน็ตแบบไร้สายแล้ว โครงข่ายไร้สายแบบเมชสามารถนำมาใช้งานในลักษณะแบบแยกเดี่ยว (stand alone) เนื่องจากใช้ระยะเวลาในการติดตั้งไม่นานจึงเหมาะสมกับการใช้งานในสถานการณ์ฉุกเฉินต่าง ๆ เช่น การช่วยเหลือผู้ประสบภัย (disaster recovery) การใช้งานเป็นโครงข่ายทางทหารทั้งการรบภาคสนามและการซ้อมรบ เป็นต้น

อย่างไรก็ตามโครงข่ายไร้สายแบบเมชยังมีข้อเสียอยู่หลายประการ [2]-[3] เช่น ปัญหาขีดจำกัดของความจุในการส่งข้อมูล (capacity constraint) ปัญหาค่าเวลาประวิงของการส่งข้อมูล (delay constraint) อันเนื่องมาจากการสื่อสารผ่านตัวกลางไร้สายเป็นส่วนใหญ่ แต่ปัญหาหลักที่เป็นอุปสรรคทำให้โครงข่ายไม่ได้ถูกใช้งานอย่างแพร่หลายเท่าที่ควรในทุกวันนี้ คือ ปัญหาด้านความปลอดภัย โดยปกติแล้วการติดต่อผ่านตัวกลางไร้สายจะมีความทนทานต่อการถูกโจมตีต่ำกว่าโครงข่ายที่ใช้สายสื่อสาร (wired network) เมื่อพิจารณาโครงข่ายไร้สายแบบเมชซึ่งมีโครงข่ายแกนกลาง (backbone network) เป็นตัวกลางไร้สายทั้งหมดจึงทำให้ข้อมูลสำคัญต่าง ๆ ของผู้ใช้งานโครงข่าย เช่น รหัสเครดิตการ์ด รหัสอีเมลล์ หรือข้อมูลสำคัญที่เป็นความลับอื่น ๆ ซึ่งล้วนถูกส่งผ่านตัวกลางไร้สายนั้นจะถูกผู้โจมตีดักฟัง (eavesdropping) ได้ง่าย ถ้าหากการโจมตีนี้ผู้โจมตีดักฟังข้อมูลโดยไม่มีการเปลี่ยนแปลงเนื้อหาในกลุ่มข้อมูล (packet) แล้ว การตรวจจับการโจมตีจะกระทำได้ยาก [4] ยิ่งไปกว่านั้นการดักฟังข้อมูลยังอาจสร้างความเสียหายให้กับโครงข่ายมากขึ้นโดยนำไปสู่การโจมตีชนิดอื่นซึ่งขึ้นกับเนื้อหาในกลุ่มข้อมูลที่ถูกดักฟังได้อีกด้วย นอกจากการดักฟังข้อมูลแล้ว การที่มีโครงข่ายแกนกลางเป็นตัวกลางไร้สายยังทำให้โครงข่ายไร้สายแบบเมชง่ายต่อการถูกโจมตีโดยการส่งสัญญาณรบกวน (jamming) การโจมตีนี้จะทำให้การรับส่งข้อมูลของโนดที่อยู่ภายในพื้นที่ซึ่งถูกรบกวน (jamming area) นั้นไม่สามารถดำเนินการตามปกติ และนำไปสู่ภาวะที่ผู้ใช้งานไม่สามารถใช้บริการติดต่อสื่อสารผ่านโครงข่ายได้ (Denial of Service, DoS) ยิ่งไปกว่านั้นผู้โจมตีอาจส่งสัญญาณรบกวนให้มีลักษณะคล้ายกับสัญญาณรบกวนที่มาจากปัจจัยอื่น เช่น การรบกวนกันเองระหว่างโนดในโครงข่าย หรือการขาดหายของสัญญาณที่เกิดขึ้นตามปกติในการสื่อสารผ่านตัวกลางไร้สาย ทำให้การตรวจจับการโจมตีโดยการส่งสัญญาณรบกวนกระทำได้ยากขึ้นและเป็นช่องทางให้ผู้โจมตีสร้างความเสียหายให้กับโครงข่ายได้มากขึ้น ดังนั้นปัญหาที่เกิดจากทั้งการถูกดักฟังข้อมูลและการส่งสัญญาณรบกวนจากผู้โจมตีจึงเป็นปัญหาที่ไม่อาจมองข้ามและต้องการมาตรการป้องกันที่เหมาะสมกับโครงข่ายไร้สายแบบเมช

ปัญหาที่เกิดจากการถูกดักฟังข้อมูลซึ่งเป็นปัญหาแรกที่พิจารณาในวิทยานิพนธ์นี้ โดยทั่วไปสามารถป้องกันได้หลายวิธี การเข้ารหัสลับ (encryption) เป็นหนึ่งในวิธีที่มีประสิทธิภาพและถูกนำมาใช้อย่าง

แพร่หลาย [4] โดยวิธีนี้จะมีระดับความปลอดภัยที่สูงขึ้นตามความยาวของกุญแจ (key) ที่ใช้ในการเข้า/ถอดรหัส แต่เมื่อพิจารณาลักษณะของโครงข่ายไร้สายแบบเมชซึ่งมีโครงข่ายแกนกลางเป็นตัวกลางไร้สาย การเข้ารหัสทุกกลุ่มข้อมูลต้องใช้ระยะเวลาในการคำนวณสูง ซึ่งจะส่งผลให้ปัญหาขีดจำกัดของความจุและค่าเวลาประวิงในการส่งข้อมูลในโครงข่ายเพิ่มมากขึ้น อีกทั้งการเข้ารหัสลับยังเป็นวิธีที่วางใจกุญแจที่ใช้ในการเข้า/ถอดรหัสอย่างมาก แต่ในขณะเดียวกันโนดของโครงข่ายไร้สายแบบเมชนั้นกลับเข้าถึงได้ง่ายและไม่มีการป้องกันที่เพียงพอ [2] โดยเฉพาะจุดเชื่อมต่อผ่าน ผู้โจมตีสามารถขโมยกุญแจจากโนดนั้น ๆ ได้ไม่ยาก และทำให้การเข้ารหัสลับมีความเสี่ยงสูงต่อปัญหาการถูกขโมยกุญแจ (stolen key problem) ได้

ด้วยเหตุผลดังกล่าวทำให้การจัดเส้นทางแบบเฟ้นสุ่ม (stochastic routing) ถูกนำเสนอขึ้นเพื่อนำมาใช้ป้องกันการดักฟังข้อมูลในโครงข่ายไร้สายแบบเมช โดยการจัดเส้นทางชนิดนี้โนดในโครงข่ายจะเลือกเส้นทางเพื่อใช้เชื่อมต่อกับปลายทางอย่างสุ่ม (ตามการแจกแจงความน่าจะเป็นที่เหมาะสม) การจัดเส้นทางแบบเฟ้นสุ่ม จึงเป็นการลดโอกาสที่ผู้โจมตีจะเลือกจู่โจมเส้นทางที่ใช้ส่งข้อมูลได้ถูกต้องและจำนวนกลุ่มข้อมูลที่ถูกดักฟังนั้นมีจำนวนลดลง ทำให้ระดับความปลอดภัยของโครงข่ายมีมากขึ้น วิธีดังกล่าวนี้เมื่อเทียบกับวิธีการเข้ารหัสลับแล้ว เป็นวิธีที่ไม่ได้วางใจส่วนใดส่วนหนึ่งของกระบวนการป้องกันมากจนเกินไปอีกด้วย

เพื่อให้การจัดเส้นทางแบบเฟ้นสุ่มสามารถป้องกันการโจมตีกรณีร้ายแรงที่สุดได้ ทฤษฎีเกม (game theory) จึงถูกนำมาเป็นเครื่องมือในการวิเคราะห์ปัญหา [5]-[11] รวมทั้งใช้ในการหาการแจกแจงความน่าจะเป็นในการจัดเส้นทางที่เหมาะสม (optimal routing probability distribution) ดังนั้นการจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมจึงเป็นการป้องกันการโจมตีในลักษณะป้องกันไว้ก่อน (proactive protection) ที่สามารถรับประกันค่าประสิทธิภาพต่ำสุดที่พึงได้ของโครงข่ายภายใต้การโจมตีในกรณีร้ายแรงที่สุด ดังเช่นที่มีงานวิจัยที่มุ่งศึกษาการจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเพื่อแก้ปัญหาต่าง ๆ เช่น ใช้เพื่อลดความเสี่ยงที่ข้อมูลจะสูญหายเนื่องจากอุปกรณ์โครงข่ายได้รับความเสียหายดังในงานวิจัย [5]-[6], ประเมินสภาพการจราจรที่อาจเกิดจากการเกิดอุบัติเหตุในโครงข่ายท้องถนน [7] รวมทั้งใช้แก้ปัญหาการโจมตีต่าง ๆ ซึ่งจะกล่าวถึงในภายหลัง

ในส่วนปัญหาที่สองที่พิจารณาในวิทยานิพนธ์ฉบับนี้ คือ ปัญหาที่เกิดจากการส่งสัญญาณรบกวน นั้นสามารถแบ่งวิธีการป้องกันออกเป็น 3 วิธีหลัก [12] ได้ดังนี้

1. การพัฒนาด้านตรวจจับการโจมตี
   - งานวิจัยในส่วนนี้จะวิเคราะห์ความแตกต่างระหว่างสัญญาณรบกวนที่เกิดขึ้นตามปกติในการสื่อสารผ่านตัวกลางไร้สายกับสัญญาณที่ถูกส่งเพื่อรบกวนอย่างจงใจโดยผู้โจมตี [13]
2. การป้องกันในลักษณะแข่งขันกับผู้โจมตี
   - งานวิจัยในส่วนนี้เมื่อมีการส่งสัญญาณรบกวนจะใช้กลยุทธ์เพื่อให้สัญญาณรบกวนจากผู้โจมตีมีผลน้อยลง ซึ่งทำได้ทั้งการเพิ่มกำลังการส่ง (transmission power) หรือ การปรับรหัสระบุความผิดพลาด (error correction code) ให้มีความทนทานต่อสัญญาณรบกวนจากผู้โจมตีให้มากขึ้น [14] เป็นต้น เมื่อพิจารณางานวิจัยในส่วนนี้จะเห็นว่าทุกวิธีต้องคำนึงถึงผู้โจมตีซึ่งสามารถเพิ่มระดับ

สัญญาณรบกวนได้เช่นกัน ทำให้วิธีป้องกันทั้งหมดในส่วนนี้มีลักษณะแข่งขันกับผู้โจมตีนั่นเอง

3. การหนีหรือหลีกเลี่ยงผู้โจมตี

- งานวิจัยในส่วนนี้เป็นการป้องกันในลักษณะหลีกหนีสัญญาณรบกวนจากผู้โจมตีโดยสามารถทำได้ทั้งเลือกเส้นทางหนีพื้นที่ที่ถูกสัญญาณรบกวนอยู่ (spatial retreat) เลือกช่องสัญญาณที่ยังไม่ถูกรบกวนจากผู้โจมตี (channel surfing) [15] รวมทั้งการสลับใช้เทคโนโลยีที่แตกต่างกัน (mechanism hopping) [16] เป็นต้น

จากวิธีทั้งหมดที่กล่าวมาข้างต้น การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมสามารถจัดเป็นส่วนหนึ่งในวิธีที่ 3 คือ การหนีพื้นที่ที่ถูกสัญญาณรบกวนอยู่ เพียงแต่การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเป็นลักษณะการป้องกันไว้ก่อนการโจมตีจะเกิดขึ้นดังที่เคยกล่าวมาแล้ว ดังนั้นวิธีดังกล่าวจึงสามารถป้องกันโครงข่ายด้วยมาตรการลดผลกระทบจากการโจมตีทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวนได้ โดยมีงานวิจัยที่เกี่ยวข้องดังนี้

ในงานวิจัย [8]-[9] ใช้การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเพื่อแก้ปัญหาการดักฟังข้อมูล ซึ่งกำหนดให้ผู้โจมตีจะโจมตีโครงข่ายอย่างร้ายแรงที่สุด นั่นคือ ดักฟังข้อมูลของผู้ใช้งานโครงข่ายให้มากที่สุดเท่าที่จะทำได้ นอกจากนี้ในงานดังกล่าวยังใช้การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเพื่อลดความเสี่ยงที่ข้อมูลจะสูญหายเนื่องจากอุปกรณ์โครงข่ายได้รับความเสียหายอีกด้วย อย่างไรก็ตามในงานวิจัยนี้เป็นการศึกษาปัญหาในโครงข่ายที่ใช้สายสื่อสารซึ่งมีลักษณะการดักฟังข้อมูลของผู้โจมตี คือ การใช้เครื่องมือเพื่อวิเคราะห์ทราฟฟิกที่ถูกส่งผ่านข่ายเชื่อมโยงหนึ่ง ๆ ในโครงข่าย จึงมองได้ว่าผู้โจมตีจะดักฟังข้อมูลจากข่ายเชื่อมโยง แตกต่างกับการดักฟังข้อมูลในของโครงข่ายไร้สายซึ่งข้อมูลจะถูกส่งออกมาผ่านตัวกลางไร้สาย ผู้โจมตีที่ดักฟังข้อมูลโดยตรงจากตัวกลางไร้สายจึงมีโอกาสดักฟังการรับส่งข้อมูลได้หลายคู่สื่อสารพร้อมกัน ทั้งนี้ขึ้นกับตำแหน่งของผู้โจมตีว่าอยู่ในพื้นที่ครอบคลุมของโนดใดบ้าง ด้วยเหตุผลจากสภาพแวดล้อมที่แตกต่างกันระหว่างโครงข่ายที่ใช้สายสื่อสารกับโครงข่ายไร้สายแบบเมช ทำให้การจัดเส้นทางแบบเฟ้นสุ่มที่ศึกษาในโครงข่ายที่ใช้สายสื่อสาร ไม่สามารถนำมาใช้ป้องกันการดักฟังข้อมูลในโครงข่ายไร้สายแบบเมชได้โดยตรง

ในงานวิจัย [10] พิจารณาปัญหาที่เกิดจากการดักฟังข้อมูลและการส่งกลุ่มข้อมูลเพิ่มเข้าไปเพื่อก่อกวนระบบ (packet inserting attack) ในโครงข่ายไร้สายแบบเมช ซึ่งงานวิจัยดังกล่าวใช้การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมร่วมกับการจัดกำหนดการในการส่งกลุ่มข้อมูล (packet scheduling) เพื่อแก้ปัญหาการโจมตีทั้งสองแบบ แต่อย่างไรก็ตามภายใต้สมมุติฐานของการดักฟังข้อมูลในงานนี้ ผู้โจมตียังคงเลือกดักฟังข้อมูลจากข่ายเชื่อมโยงหนึ่ง ๆ ซึ่งเป็นลักษณะการดักฟังข้อมูลในโครงข่ายที่ใช้สายสื่อสาร นอกจากนี้งานดังกล่าวยังไม่ได้พิจารณาความแตกต่างระหว่างการส่งข้อมูลฝั่งขาขึ้น (uplink communication) และการส่งข้อมูลฝั่งขาลง (downlink communication) ของโครงข่ายไร้สายแบบเมช ซึ่งการส่งข้อมูลทั้งสองทิศทางต้องการการป้องกันโดยการจัดเส้นทางแบบเฟ้นสุ่มที่แตกต่างกัน

ดังนั้นในวิทยานิพนธ์ฉบับนี้ได้ศึกษาการจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเพื่อแก้ปัญหาที่เกิดจากทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมช โดยได้นำเสนอสมการในการ

วิเคราะห์ปัญหา พร้อมทั้งแยกพิจารณาการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงออกจากกันเพื่อให้ได้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมกับการส่งข้อมูลในแต่ละทิศทาง นอกจากนั้นเพื่อให้ลักษณะการโจมตีสอดคล้องกับสถานการณ์ใช้งานจริงกับโครงข่ายแบบไร้สาย ในวิทยานิพนธ์นี้ได้จำลองลักษณะการโจมตีโดยให้ขึ้นกับตำแหน่งของผู้โจมตีว่าอยู่ในพื้นที่ที่สามารถโจมตีโนดใดในโครงข่าย รวมทั้งวิทยานิพนธ์นี้ได้ชี้ให้เห็นถึงความสัมพันธ์และความแตกต่างของการโจมตีทั้งสองแบบ คือ การดักฟังข้อมูลและการส่งสัญญาณรบกวน เพื่อให้ได้การจัดเส้นทางที่เหมาะสมกับการป้องกันการโจมตีในแต่ละแบบ

1.2 วัตถุประสงค์

เสนอระเบียบวิธีการคำนวณหารูปแบบการจัดเส้นทางการส่งข้อมูลที่เหมาะสมสำหรับ การส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่ายไร้สายแบบเมช เพื่อป้องกันการดักฟังข้อมูลและการส่งสัญญาณรบกวน โดยประยุกต์ทฤษฎีเกมเข้ากับวิธีการจัดเส้นทางแบบเฟ้นสุ่ม ทั้งนี้โดยการปรับปรุงลักษณะการโจมตีให้มีความเหมาะสมและสอดคล้องกับโครงข่ายไร้สายซึ่งมีลักษณะการโจมตีที่ขึ้นกับตำแหน่งของผู้โจมตี

1.3 ขอบเขตของวิทยานิพนธ์

วิทยานิพนธ์นี้ได้ศึกษาปัญหาที่เกิดจากการดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมชโดยมีขอบเขตงานวิจัยดังนี้

1. โครงข่ายไร้สายแบบเมชที่นำมาพิจารณาเป็นโครงข่ายเพื่อการให้บริการเชื่อมต่ออินเทอร์เน็ตเท่านั้น ในวิทยานิพนธ์นี้ไม่ได้พิจารณาโครงข่ายไร้สายแบบเมชที่ถูกใช้ในลักษณะแยกเดี่ยว ซึ่งโนดในโครงข่ายลักษณะนี้ทำหน้าที่เหมือนกันทั้งหมด ไม่ได้ถูกแบ่งหน้าที่ออกเป็นสองชนิด คือ เกตเวย์และจุดเชื่อมต่อผ่าน
2. ในวิทยานิพนธ์นี้ไม่ได้พิจารณากรณีที่จุดเชื่อมต่อผ่านมีการระบุการเชื่อมต่อกับเกตเวย์ใดเกตเวย์หนึ่งโดยเฉพาะ
3. ระเบียบวิธีการคำนวณหารูปแบบการป้องกันที่เหมาะสมที่ได้นำเสนอนั้น สามารถนำไปใช้ในกรณีที่มีจำนวนผู้โจมตีมากกว่าหนึ่งคนได้ แต่ในวิทยานิพนธ์นี้จะศึกษาเฉพาะกรณีที่มีผู้โจมตีเพียงหนึ่งคนเท่านั้น

1.4 ขั้นตอนการดำเนินงาน

1. ศึกษางานวิจัยที่เกี่ยวข้องและทฤษฎีเกม
2. สร้างแบบจำลองทางคณิตศาสตร์สำหรับแก้ปัญหาที่พิจารณา
3. จำลองสถานการณ์ที่ใช้ศึกษาด้วยโปรแกรม MATLAB โดยใช้การคำนวณแบบกระจาย (distributed computing) บนคอมพิวเตอร์แบบคลัสเตอร์เพื่อใช้ทดสอบระเบียบวิธีที่เสนอ

4. สรุปผลการทดลองและวิเคราะห์ผล
5. เขียนบทความทางวิชาการและส่งตีพิมพ์
6. จัดทำวิทยานิพนธ์ฉบับสมบูรณ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

จากระเบียบวิธีที่ได้นำเสนอ ทำให้โครงข่ายไร้สายแบบเมชสามารถป้องกันทั้งปัญหาการดักฟังข้อมูลและการส่งสัญญาณรบกวนด้วยการจัดเส้นทางแบบเฟ้นสุ่มที่ถูกต้องเหมาะสมกับโครงข่ายมากขึ้น อีกทั้งวิธีป้องกันดังกล่าว ยังสามารถรับประกันค่าต่ำสุดของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีให้กับโครงข่ายไร้สายแบบเมชได้ นอกจากนี้วิทยานิพนธ์ได้ศึกษาลักษณะการโจมตีแต่ละแบบ ทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวน เพื่อให้รู้เบื้องต้นถึงพื้นที่ภายในโครงข่ายที่เสี่ยงต่อการถูกโจมตีซึ่งเป็นประโยชน์ต่อการศึกษาพฤติกรรมของผู้โจมตีโดยเฉพาะการดักฟังข้อมูล ซึ่งเป็นการโจมตีที่ไม่สามารถตรวจจับได้อีกด้วย

บทที่ 2

ทฤษฎีและความรู้พื้นฐาน

2.1 ทฤษฎีเกม

ทฤษฎีเกม [17] คือ ทฤษฎีที่กล่าวถึงผลได้เสียของการแข่งขัน ซึ่งผู้เล่นอาจเป็นบุคคลหรือกลุ่มบุคคลตั้งแต่ 2 กลุ่มขึ้นไปมาแข่งขันกัน โดยผลลัพธ์ของการแข่งขันจะมาจากการตัดสินใจเลือกแผนการเล่นของผู้เล่นทุกฝ่าย ในทุกรอบของการแข่งขันผู้เล่นจะตัดสินใจโดยคิดตามหลักเหตุผล (rational thinking) เพื่อให้ได้แผนการเล่นที่สามารถให้ผลประโยชน์กับตนเองมากที่สุด

หลักการเลือกแผนการเล่น มี 2 ลักษณะ คือ

1. แผนการเล่นแบบบริสุทธิ์ (pure strategy) คือ กลยุทธ์ที่ในแต่ละรอบของการแข่งขัน ผู้เล่นตัดสินใจเลือกแผนการเล่นใดแผนการเล่นหนึ่งเพื่อมาใช้เล่น และจะยังใช้แผนการเล่นเดิมในการเล่นรอบต่อไปโดยไม่เปลี่ยนแผน

2. แผนการเล่นแบบผสม (mixed strategies) คือ กลยุทธ์ที่ในแต่ละรอบของการแข่งขัน ผู้เล่นตัดสินใจเลือกแผนการเล่นใดแผนการเล่นหนึ่งอย่างสุ่มเพื่อมาใช้เล่น โดยขึ้นกับการแจกแจงความน่าจะเป็นนั่นคือในเกมนี้ ผู้เล่นจะเลือกใช้แผนการเล่นมากกว่าหนึ่งแผนตามความน่าจะเป็นที่แผนการเล่นนั้นจะถูกเลือก

2.1.1 เกมในรูปแบบปกติ (normal form) หรือ เกมในรูปแบบมาตรฐาน (strategic form)

ทฤษฎีเกมนั้นศึกษาสถานการณ์โดยอาศัยการวิเคราะห์ทางคณิตศาสตร์เข้ามาช่วย ดังนั้นจึงได้มีการนิยามรูปแบบให้เหมาะสมกับแต่ละสถานการณ์ที่จะศึกษาเพื่อให้ง่ายต่อการวิเคราะห์

เกมในรูปแบบปกติ หรือ รูปแบบมาตรฐานนั้น กล่าวถึงสถานการณ์ที่ผู้เล่นเลือกแผนการเล่นพร้อมกัน ผู้เล่นแต่ละคนไม่ทราบการเลือกแผนการเล่นของผู้เล่นคนอื่นล่วงหน้า รูปแบบดังกล่าวประกอบไปด้วยองค์ประกอบหลัก ดังนี้

1. เซตของแผนการเล่นของผู้เล่นแต่ละคน

2. ค่าของเกมซึ่งมาจากการตัดสินใจเลือกแผนการเล่นของผู้เล่นทุกคน

2.1.2 เกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์ (two-person zero-sum game)

เป็นเกมที่มีการแข่งขันกันระหว่างผู้เล่นสองฝ่าย โดยคำว่าผลรวมเป็นศูนย์หมายถึง ผู้เล่นทั้งสองฝ่ายจะได้รับผลประโยชน์รวมกันเป็นศูนย์เสมอสำหรับการตัดสินใจเลือกแผนการเล่นแต่ละแบบ หรือกล่าวอีกนัยหนึ่งคือ ผลประโยชน์ที่ผู้เล่นฝ่ายที่ชนะจะได้นั้น มาจากผลประโยชน์ที่ผู้เล่นฝ่ายที่แพ้จะเสียนั่นเอง

เกมลักษณะนี้แสดงให้เห็นถึงความขัดแย้งระหว่างผู้เล่นอย่างชัดเจน จึงไม่มีการเล่นเกมเกมนี้อย่างร่วมมือกัน ตัวอย่างของเกมลักษณะนี้ ได้แก่ เกมโยนเหรียญ เกมหมากรุก เป็นต้น

โดยปกติแล้ว เกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์ (two-person zero-sum game) นั้น จะแสดงผลได้ผลเสียด้วยตาราง ซึ่งเรียกว่า ตารางผลได้ผลเสีย (payoff table) ดังตัวอย่าง

		ผู้เล่น 2	
		a	b
ผู้เล่น 1	x	-2	0
	y	2	10

รูปที่ 2.1: ตัวอย่างตารางผลได้ผลเสีย

จากรูปที่ 2.1 แสดงถึง รูปแบบของการเล่นเกมและผลได้ผลเสีย โดยในตารางนี้ ผู้เล่นแนวแถว (ผู้เล่น 1) มีแผนการเล่น 2 แผน คือ x และ y ผู้เล่นแนวหลัก (ผู้เล่น 2) มีแผนการเล่น 2 แผนเช่นกันคือ a และ b ส่วนค่าในตารางหมายถึง ค่าผลได้ผลเสียของผู้เล่นแนวแถว ตัวอย่างเช่น หากผู้เล่น 1 เลือก แผน y และผู้เล่น 2 เลือกแผน a จะได้ค่าผลได้ผลเสียเท่ากับ 2 หมายถึง ผู้เล่น 1 จะได้ผลประโยชน์ 2 หน่วย ผู้เล่น 2 จะเสียประโยชน์ 2 หน่วย หากผู้เล่น 1 เลือกแผน x ในขณะที่ผู้เล่น 2 เลือกแผน a จะได้ค่าเท่ากับ -2 ผู้เล่น 1 จะเสียผลประโยชน์ 2 หน่วย ผลเล่น 2 จะได้ผลประโยชน์ 2 หน่วย เป็นต้น

2.1.3 ทฤษฎีมินิแมกซ์ (minimax theorem)

ในเกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์นั้น หากผู้เล่นทั้งสองคนมีเซตของแผนการเล่นที่เป็นเซตจำกัดแล้ว จะเรียกเกมประเภทนี้ว่า เกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์แบบจำกัด (finite two-person zero-sum game) ซึ่งเกมประเภทนี้สามารถใช้ทฤษฎีมินิแมกซ์ในการหาจุดสมดุลย์ของเกมได้ โดยทฤษฎีกล่าวไว้ดังนี้

สำหรับเกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์แบบจำกัด

1. จะมีค่า V ซึ่งเป็นค่าของเกม (value of game) โดยค่าของเกมนี้เป็นค่าที่ผู้เล่นทั้งสองพอใจและเป็นค่าที่รับประกันผู้เล่นทั้งสองฝ่ายว่า ในการเล่นทั้งหมดโดยเฉลี่ยแล้วจะได้รับค่าที่จ่ายจากเกมไม่ต่ำไปกว่าค่านี้

2. จะมีแผนการเล่นแบบผสมสำหรับผู้เล่น 1 ซึ่งทำให้ผู้เล่น 1 ได้รับประโยชน์โดยเฉลี่ยอย่างน้อยที่สุดเท่ากับค่า V ไม่ว่าผู้เล่น 2 จะเลือกใช้แผนการเล่นใดก็ตาม ซึ่งแผนของผู้เล่น 1 เป็นการหาค่ามากที่สุดจากผลได้น้อยที่สุด (maximize the minimum gain)

3. จะมีแผนการเล่นแบบผสมสำหรับผู้เล่น 2 ซึ่งทำให้ผู้เล่น 2 เสียผลประโยชน์โดยเฉลี่ยอย่างมากที่สุดเท่ากับค่า V ไม่ว่าผู้เล่น 1 จะเลือกใช้แผนการเล่นใดก็ตาม ซึ่งแผนของผู้เล่น 2 เป็นการหาค่าน้อยที่สุดจากผลเสียที่มากที่สุด (minimize the maximum loss)

จากทฤษฎีมินิแมกซ์ที่กล่าวไว้ข้างต้น จะเห็นว่าเกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์แบบจำกัดทุกเกม ผู้เล่น 1 และ 2 จะมีแผนการเล่นที่สอดคล้องกับค่าของเกมที่ทำให้ผู้เล่นทั้งคู่พอใจในผลได้เสียของการแข่งขัน โดยแผนที่ทั้งคู่นำมาเล่นนี้เรียกว่าแผนการเล่นแบบมินิแมกซ์ หรือ แผนการเล่นที่เหมาะสมที่สุด (optimal strategy)

2.1.4 กลยุทธ์เด่น (dominant strategy)

จากนิยามกล่าวว่า แผนการเล่น S เด่นกว่าแผนการเล่น T ถ้าทุก ๆ ค่าของผลได้ผลเสียใน S ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้ามมีค่าผลได้ผลเสียที่ดีกว่าหรือเท่ากับค่าของผลได้ผลเสียใน T ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้าม ซึ่งกลยุทธ์เด่นนั้นสามารถแบ่งออกเป็น 2 รูปแบบ คือ

1. กลยุทธ์เด่นอย่างชัดเจน (strictly dominant)

   - หากแผนการเล่น S เด่นกว่าแผนการเล่น T อย่างชัดเจนแล้ว ทุก ๆ ค่าของผลได้ผลเสียใน S ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้ามจะมีค่าผลได้ผลเสียที่ดีกว่าค่าของผลได้ผลเสียใน T ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้าม

2. กลยุทธ์ไม่ด้อยกว่า (weakly dominant)

   - หากแผนการเล่น S ไม่ด้อยกว่าแผนการเล่น T แล้ว จะมีอย่างน้อยหนึ่งค่าของผลได้ผลเสียใน S ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้ามมีค่าผลได้ผลเสียที่ดีกว่าค่าของผลได้ผลเสียใน T ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้าม และค่าของผลได้ผลเสียใน S ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้ามที่เหลือมีค่าผลได้ผลเสียเท่ากับค่าของผลได้ผลเสียใน T ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้าม

เพื่อความชัดเจนจึงขออธิบายโดยการยกตัวอย่างตารางผลได้ผลเสียดังรูปที่ 2.2

		ผู้เล่น 2			
		a	b	c	d
ผู้เล่น 1	w	1	2	3	4
	x	2	3	4	5
	y	2	4	4	5
	z	1	4	5	2

รูปที่ 2.2: ตัวอย่างตารางผลได้ผลเสียเพื่อแสดงกลยุทธเด่นของผู้เล่นทั้งสองคน

เนื่องจากค่าในตารางเป็นค่าผลได้ผลเสียของผู้เล่นแนวแถว (ผู้เล่น 1) ดังนั้นค่าผลได้ผลเสียที่ดีกว่าสำหรับผู้เล่น 1 จะหมายถึง ค่าผลได้ผลเสียที่มากกว่านั่นเอง จากตัวอย่างจะเห็นว่าแผนการเล่น x นั้นเป็นแผนการเล่นที่เด่นกว่าแผนการเล่น w อย่างชัดเจน เนื่องจากค่าผลได้ผลเสียทุกค่าของแผน x มีค่ามาก

กว่าค่าผลได้ผลเสียของแผนการเล่น w ในทุกกรณี ในขณะที่แผนการ y นั้นเป็นแผนการเล่นที่ไม่ด้อยกว่าแผนการเล่น x เนื่องจากมีอย่างน้อยหนึ่งค่าของแผนการเล่น y ที่ให้ค่าผลได้ผลเสียที่มากกว่าแผนการเล่น x นั่นคือ ค่าผลได้ผลเสียในกรณีที่ผู้เล่น 2 เลือกแผนการเล่น b ส่วนค่าผลได้ผลเสียในกรณีที่เหลือที่ผู้เล่น 2 เลือกนั้นแผนการเล่น x และ y มีค่าผลได้ผลเสียเท่ากัน

สำหรับผู้เล่น 2 เนื่องจากค่าในตารางเป็นค่าผลได้ผลเสียของผู้เล่น 1 ดังนั้นค่าผลได้ผลเสียที่ดีกว่าสำหรับผู้เล่น 2 จะหมายถึง ค่าผลได้ผลเสียที่น้อยกว่า และจากตัวอย่างจะเห็นว่าแผนการเล่น a เป็นแผนการเล่นที่เด่นกว่าแผนการเล่น d อย่างชัดเจนเนื่องจากค่าผลได้ผลเสียทุกค่าของแผน a มีค่าน้อยกว่าค่าผลได้ผลเสียของแผน d ไม่กว่าผู้เล่น 1 จะเลือกแผนการเล่นใด เป็นต้น

จากหลักการของกลยุทธ์เด่น ทำให้สามารถลดความซับซ้อนในการหาผลเฉลยได้เนื่องจากผู้เล่นที่มีเหตุมีผล (rational) นั้นจะไม่เลือกกลยุทธ์ที่ด้อยกว่าเพื่อมาใช้เล่น ทำให้สามารถตัดกลยุทธ์ที่ด้อยกว่าออกก่อนหาผลเฉลยได้โดยค่าของเกมที่ได้จะไม่เปลี่ยนแปลง

2.2 การส่งข้อมูลหลายวิถี (multi path routing)

เมื่อโนดหนึ่งต้องการส่งข้อมูลผ่านโครงข่ายไปยังโนดอื่น โครงข่ายจำเป็นต้องมีกระบวนการจัดหาเส้นทางการส่งข้อมูล (routing) เพื่อให้ข้อมูลถูกส่งไปในเส้นทางที่ดีที่สุด โดยกระบวนการจัดหาเส้นทางที่ใช้กันตามปกตินั้น จะส่งข้อมูลไปตามเส้นทางเพียงเส้นทางเดียวจากต้นทางไปยังปลายทาง (single path routing) ดังนั้นหากมีผู้โจมตีลักลอบดักฟังข้อมูลหรือลักลอบส่งสัญญาณรบกวนอยู่ระหว่างทาง การส่งข้อมูลไปตามเส้นทางที่ได้จากกระบวนการจัดหาเส้นทางที่ใช้กันตามปกติจะทำให้ผู้โจมตีคาดเดาเส้นทางการส่งได้ง่ายและทำให้ข้อมูลที่ส่งไปตามเส้นทางดังกล่าวไม่ปลอดภัย จึงเกิดแนวคิดในการใช้เส้นทางมากกว่า 1 เส้นทางขึ้น (multi path routing) เพื่อแก้ปัญหาดังกล่าวซึ่งทำได้หลายลักษณะดังนี้

2.2.1 การกระจายทุกทิศทาง (flooding)

การกระจายทุกทิศทางเป็นวิธีที่ง่ายที่สุดของการส่งข้อมูลแบบหลายวิถี คือ การส่งข้อมูลไปในทุกเส้นทางที่เป็นไปได้ทั้งหมด จะเห็นว่าการส่งข้อมูลลักษณะเช่นนี้เป็นวิธีที่ดีที่สุดสำหรับการส่งข้อมูลเพื่อหลีกเลี่ยงความเสียหายของอุปกรณ์โครงข่ายซึ่งอาจจะเป็นข่ายเชื่อมโยงหรือโนด แต่เมื่อพิจารณาในด้านของการดักฟังข้อมูลแล้วการส่งข้อมูลด้วยวิธีดังกล่าวเป็นการเพิ่มความเสี่ยงที่จะถูกดักฟังข้อมูลได้โดยง่าย นอกจากนั้นการส่งแบบกระจายทุกทิศทางยังทำให้สิ้นเปลืองทรัพยากรโครงข่ายเป็นอย่างมากอีกด้วย

2.2.2 การจัดเส้นทางแบบเฟ้นสุ่ม (stochastic routing)

การจัดเส้นทางแบบเฟ้นสุ่ม เป็นวิธีการส่งข้อมูลโดยเลือกเส้นทางที่จะใช้ในการส่งข้อมูลมาหนึ่งเส้นทางอย่างสุ่ม ซึ่งวิธีนี้ช่วยให้ข้อมูลที่ถูกส่งไปตามเส้นทางดังกล่าวมีความปลอดภัยมากขึ้น เนื่องจากการเลือกเส้นทางอย่างสุ่ม ทำให้ผู้โจมตีคาดเดาเส้นทางที่ใช้ส่งข้อมูลได้ยากขึ้นหรือเป็นการบังคับให้ผู้โจมตีดักข้อมูลในทุกเส้นทางที่เป็นอิสระต่อกัน (independent path) อีกทั้งวิธีดังกล่าวยังไม่เป็นการสิ้นเปลือง

ทรัพยากรของโครงข่ายมากนัก

โดยวิทยานิพนธ์ฉบับนี้ ได้วิเคราะห์ปัญหาทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมช ซึ่งสถานการณ์ระหว่างโครงข่ายกับผู้โจมตีนั้นมีความขัดแย้งกันอย่างชัดเจน ปัญหาที่สนใจจึงถูกจำลองเป็นเกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์ที่กล่าวมาข้างต้น โดยที่โครงข่ายจะใช้การจัดเส้นทางแบบเฟ้นสุ่มเพื่อป้องกันการโจมตีทั้งสองแบบ รวมทั้งวิทยานิพนธ์นี้ได้จำลองระดับความปลอดภัยเป็นค่าของเกมเกมนี้ ทำให้การป้องกันด้วยการจัดเส้นทางแบบเฟ้นสุ่มสามารถรับประกันระดับความปลอดภัยขั้นต่ำให้แก่โครงข่ายไร้สายแบบเมชได้ ตามความหมายค่าของเกมจากทฤษฎีมินิแมกซ์อีกด้วย โดยแบบจำลองของเกมการรับส่งข้อมูลและระเบียบวิธีที่นำเสนอในวิทยานิพนธ์นี้จะถูกกล่าวถึงโดยละเอียดในบทต่อไป

บทที่ 3

ระเบียบวิธีที่นำเสนอในการหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะที่สุด

เนื้อหาบทนี้จะกล่าวถึงระเบียบวิธีที่นำเสนอเป็นลำดับ โดยหัวข้อที่ 3.1 กล่าวถึง แบบจำลองของโครงข่ายไร้สายแบบเมชที่พิจารณาในวิทยานิพนธ์ฉบับนี้ รวมทั้งอธิบายความแตกต่างของการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่ายไร้สายแบบเมช นอกจากนั้นหัวข้อนี้ได้อธิบายผลกระทบเมื่อเกิดการโจมตีแต่ละแบบ คือ การดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่าย

หัวข้อที่ 3.2 กล่าวถึง การจำลองสถานการณ์ในรูปแบบของเกมการรับส่งข้อมูลในโครงข่ายระหว่างผู้เล่นคนที่หนึ่ง คือ ผู้เล่นฝั่งป้องกันซึ่งใช้การจัดเส้นทางแบบเฟ้นสุ่มในการป้องกันผู้เล่นอีกคนหนึ่ง คือ ผู้เล่นฝั่งโจมตีที่จะเลือกตำแหน่งที่เหมาะสมที่สุดในการโจมตี และในตอนท้ายของหัวข้อนี้จะเป็นการอธิบายถึงตัวชี้วัดระดับความปลอดภัยที่ถูกนำเสนอขึ้นโดยวิทยานิพนธ์ฉบับนี้

หัวข้อที่ 3.3 กล่าวถึง สัญญาณพื้นฐานซึ่งถูกนิยามขึ้น และหัวข้อที่ 3.4 ซึ่งเป็นหัวข้อสุดท้ายของบทกล่าวถึง ขั้นตอนการหาผลเฉลยของเกมที่ถูกนำมาใช้ในวิทยานิพนธ์ฉบับนี้

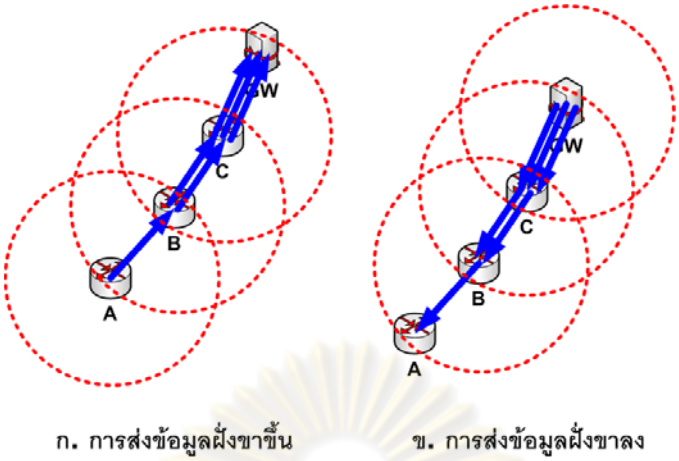
3.1 แบบจำลองโครงข่าย

โครงข่ายไร้สายแบบเมชซึ่งให้บริการเชื่อมต่ออินเทอร์เน็ตไร้สายประกอบไปด้วยโนดสองชนิด โนดชนิดแรก คือ เกตเวย์ซึ่งเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตผ่านสายสื่อสาร และโนดอีกชนิดหนึ่ง คือ จุดเชื่อมต่อผ่านซึ่งเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตโดยสร้างเซสชั่นผ่านเกตเวย์ในลักษณะหลายช่วงเชื่อมต่อ เนื่องจากโครงข่ายไร้สายแบบเมชที่นำมาพิจารณาเป็นโครงข่ายที่ให้บริการเชื่อมต่ออินเทอร์เน็ตเท่านั้น วิทยานิพนธ์ฉบับนี้จึงพิจารณาเฉพาะเซสชั่นที่เชื่อมต่อระหว่างจุดเชื่อมต่อผ่านกับเกตเวย์ และจะไม่พิจารณาเซสชั่นที่เชื่อมต่อระหว่างจุดเชื่อมต่อผ่านด้วยกัน

นอกจากนั้นโครงข่ายที่พิจารณาจะตกอยู่ภายใต้การโจมตีในกรณีร้ายแรงที่สุดสองแบบ คือ การดักฟังข้อมูลและอีกกรณีหนึ่ง คือ การส่งสัญญาณรบกวน การโจมตีทั้งสองแบบนี้ผู้โจมตีจะเลือกตำแหน่งภายในพื้นที่ที่โครงข่ายไร้สายแบบเมชติดตั้งอยู่เพื่อใช้ในการโจมตีเซสชั่นให้ได้มากที่สุด และโครงข่ายจะใช้การจัดเส้นทางแบบเฟ้นสุ่มเพื่อป้องกันการโจมตีทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวน โดยจุดเชื่อมต่อผ่านที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ตจะสร้างเซสชั่นเชื่อมต่อกับเกตเวย์อย่างสุ่มเพื่อให้ ผู้โจมตีคาดเดาเส้นทางที่ใช้ส่งข้อมูลได้ยาก และทำให้ได้จำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีมากที่สุด

3.1.1 ความแตกต่างของการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่าย

การส่งข้อมูลฝั่งขาขึ้นสู่เกตเวย์และฝั่งขาลงจากเกตเวย์ในโครงข่ายไร้สายแบบเมชนั้น มีความแตกต่างกันดังนี้ การส่งข้อมูลฝั่งขาขึ้น เป็นการส่งข้อมูลจากจุดเชื่อมต่อผ่านไปยังเกตเวย์ผ่านช่องสัญญาณไร้สาย จากนั้นจะส่งข้อมูลไปยังโครงข่ายอินเทอร์เน็ตที่เชื่อมต่อผ่านสายสื่อสาร ดังนั้นข้อมูลจะถูกส่งต่อผ่าน



ก. การส่งข้อมูลฝั่งขาขึ้น ข. การส่งข้อมูลฝั่งขาลง

รูปที่ 3.1: ความแตกต่างของการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

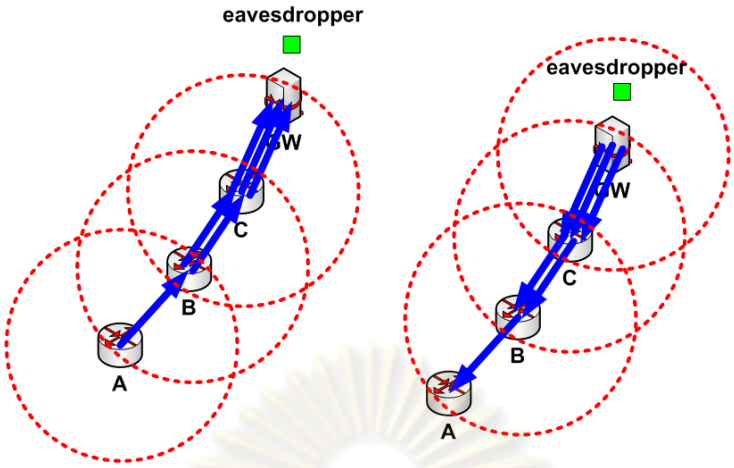
ช่องสัญญาณไร้สายในช่วงเชื่อมต่อทุกช่วงยกเว้น ณ จุดสุดท้ายคือ เกตเวย์ ซึ่งข้อมูลจะถูกส่งผ่านทางสายสื่อสารดังรูปที่ 3.1 ก. เป็นตัวอย่างการส่งข้อมูลฝั่งขาขึ้นของเซสชั่น 3 เซสชั่น คือ เซสชั่นระหว่างจุดเชื่อมต่อผ่าน A กับเกตเวย์ เซสชั่นระหว่างจุดเชื่อมต่อผ่าน B กับเกตเวย์และเซสชั่นระหว่างจุดเชื่อมต่อผ่าน C กับเกตเวย์ โดยทั้งสามเซสชั่นนี้มีเกตเวย์เป็นโนดสุดท้ายของเส้นทางและเกตเวย์ไม่ได้ส่งข้อมูลออกมาผ่านตัวกลางไร้สาย

ลักษณะเดียวกันกับการส่งข้อมูลฝั่งขาลง ซึ่งเป็นการส่งข้อมูลจากโครงข่ายอินเทอร์เน็ตผ่านเกตเวย์ไปยังจุดเชื่อมต่อผ่านผ่านช่องสัญญาณไร้สาย ณ จุดสุดท้ายคือ จุดเชื่อมต่อผ่านที่เป็นโนดปลายทาง (destination node) ก็จะไม่ส่งข้อมูลของตนเองออกมาผ่านตัวกลางไร้สายเช่นกัน ดังรูปที่ 3.1 ข. เป็นตัวอย่างการส่งข้อมูลฝั่งขาลงของเซสชั่น 3 เซสชั่น คือ เซสชั่นระหว่างจุดเชื่อมต่อผ่าน A กับเกตเวย์ เซสชั่นระหว่างจุดเชื่อมต่อผ่าน B กับเกตเวย์และเซสชั่นระหว่างจุดเชื่อมต่อผ่าน C กับเกตเวย์ โดยทั้งสามเซสชั่นนี้จุดเชื่อมต่อผ่านซึ่งเป็นเจ้าของข้อมูลในเซสชั่นนั้นไม่ได้ส่งต่อข้อมูลของตนเองออกมาผ่านตัวกลางไร้สาย เป็นต้น

3.1.2 ผลกระทบของการโจมตีโดยการดักฟังข้อมูลและการส่งสัญญาณรบกวน

การโจมตีทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวนนั้น ผู้โจมตีจะเลือกตำแหน่งเพื่อใช้ในการโจมตี แต่การโจมตีทั้งสองแบบนั้นมีความแตกต่างกัน โดยการดักฟังข้อมูล ผู้โจมตีต้องคำนึงถึงตำแหน่งที่เลือกว่าอยู่ในพื้นที่ครอบคลุมของโนดใดบ้าง นอกจากนั้นโนดที่ผู้โจมตีเลือกดักฟังข้อมูลอยู่ต้องส่งข้อมูลออกมาผ่านตัวกลางไร้สายด้วย ผู้โจมตีจึงจะสามารถดักฟังข้อมูลในโครงข่ายได้ดังแสดงในรูปที่ 3.2 ก. ผู้โจมตีเลือกดักฟังข้อมูลบริเวณพื้นที่ครอบคลุมของเกตเวย์ แต่ในการส่งข้อมูลฝั่งขาขึ้นนั้นเกตเวย์ไม่ได้ส่งข้อมูลใดผ่านตัวกลางไร้สาย ทำให้ผู้โจมตีซึ่งถึงแม้จะอยู่ในบริเวณพื้นที่ครอบคลุมของเกตเวย์ดังกล่าวก็ไม่สามารถดักฟังเซสชั่นใดได้ตามตัวอย่างในกรณีนี้

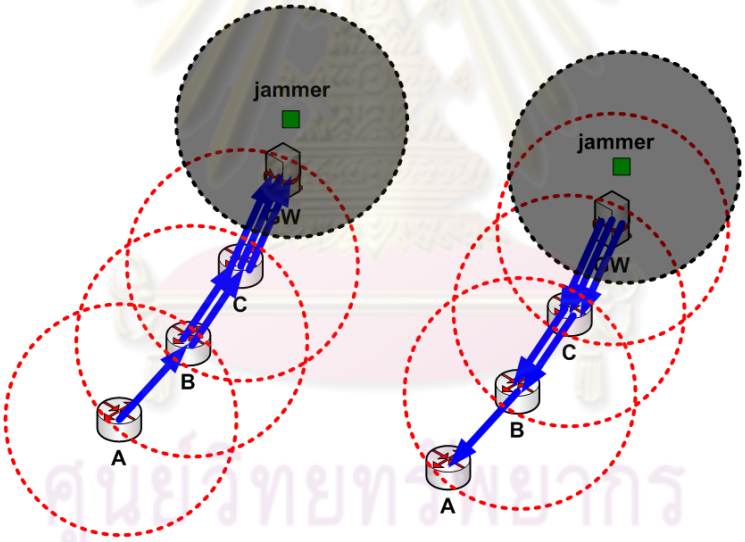
แต่กรณีการส่งข้อมูลฝั่งขาลงดังแสดงในรูปที่ 3.2 ข. หากผู้โจมตีเลือกดักฟังข้อมูลในบริเวณดังกล่าวจะสามารถดักฟังได้ทุกเซสชั่นเนื่องจากการส่งข้อมูลฝั่งขาลง เกตเวย์ต้องส่งข้อมูลของจุดเชื่อมต่อ



ก. การส่งข้อมูลฝั่งขาขึ้น ข. การส่งข้อมูลฝั่งขาลง

รูปที่ 3.2: การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

ผ่านทุกโนดออกมาผ่านตัวกลางไร้สายนั่นเอง



ก. การส่งข้อมูลฝั่งขาขึ้น ข. การส่งข้อมูลฝั่งขาลง

รูปที่ 3.3: การส่งสัญญาณรบกวนการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

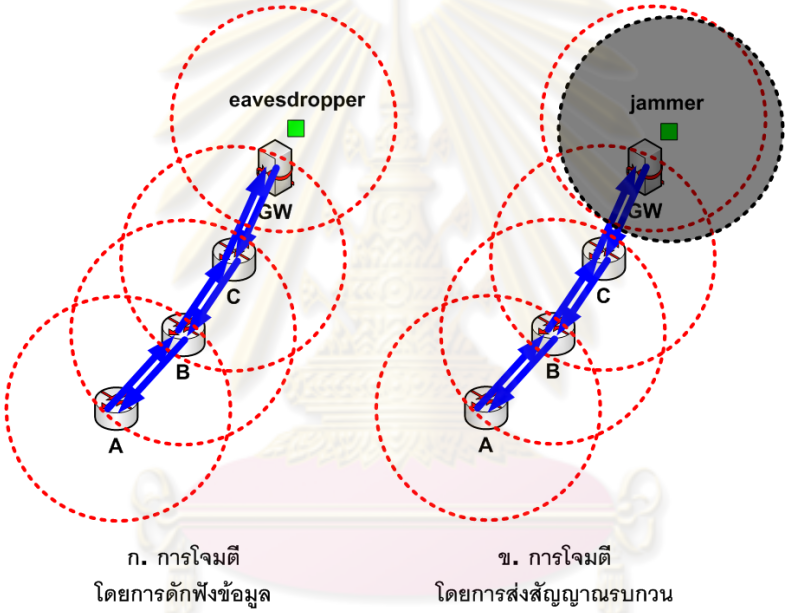
ในขณะที่การโจมตีโดยการส่งสัญญาณรบกวนนั้น ผู้โจมตีไม่จำเป็นต้องคำนึงถึงตำแหน่งที่เลือกว่าอยู่ในพื้นที่ครอบคลุมของโนดใดบ้าง แต่ต้องคำนึงว่ามีโนดใดบ้างที่อยู่ภายในพื้นที่ครอบคลุมของผู้โจมตีและทำให้ผู้โจมตีสามารถส่งสัญญาณรบกวนโนดเหล่านั้นได้ ความแตกต่างของการส่งข้อมูลในแต่ละทิศทางจึงไม่มีผลและโนดทั้งหมดที่อยู่ในพื้นที่ครอบคลุมของผู้โจมตีจะไม่สามารถรับหรือส่งข้อมูลใด ๆ ได้ ดังที่แสดงในรูปที่ 3.3 ก. ซึ่งเป็นการส่งข้อมูลฝั่งขาขึ้น เกตเวย์ไม่สามารถรับสัญญาณจากโนดใด ๆ ได้เพราะอยู่ในพื้นที่ครอบคลุมของผู้โจมตีซึ่งส่งสัญญาณรบกวนอยู่ ดังนั้นทั้งสามเซสชั่นในตัวอย่างจึงเป็นเซสชั่นที่ถูก

โจมตีทั้งหมด ในขณะที่การส่งข้อมูลฝั่งขาลง รูปที่ 3.3 ข. เกตเวย์ไม่สามารถส่งข้อมูลไปให้กับโนดใด ๆ ได้เนื่องจากการส่งข้อมูลตามปกตินั้นจะต้องมีการตอบรับ (acknowledgement) รวมอยู่ด้วย ดังนั้นโนดใดที่อยู่ในพื้นที่ครอบคลุมของผู้โจมตีซึ่งส่งสัญญาณรบกวนอยู่จะไม่สามารถรับหรือส่งข้อมูลใด ๆ ได้

นอกจากลักษณะการโจมตีทั้งสองแบบซึ่งมีลักษณะแตกต่างกันจะทำให้การนับเซสชั่นที่ถูกโจมตีแตกต่างกันแล้ว ในกรณีการส่งสัญญาณรบกวนผู้โจมตียังสามารถเพิ่มระยะการส่งสัญญาณรบกวนได้อย่างอิสระอีกด้วย

3.1.3 ความสัมพันธ์กันระหว่างการดักฟังข้อมูลและการส่งสัญญาณรบกวน

ถึงแม้ว่าการโจมตีทั้งสองแบบจะมีความแตกต่างกัน แต่บางกรณีการโจมตีทั้งสองแบบนี้มีผลกระทบต่อโครงข่ายเหมือนกันดังนี้



รูปที่ 3.4: ความสัมพันธ์กันระหว่างการดักฟังข้อมูลและการส่งสัญญาณรบกวน

สำหรับโครงข่ายไร้สายแบบเมชที่โนดทั้งหมดมีรัศมีการส่งสัญญาณไร้สายเท่ากัน และโนดทุกโนดติดตั้งสายอากาศแบบรอบทิศทาง (omni directional antenna) รวมถึงกรณีที่การโจมตีคือ การส่งสัญญาณรบกวน ผู้โจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับรัศมีการส่งสัญญาณไร้สายของโนดนั้น หากโครงข่ายใช้เส้นทางในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงเป็นเส้นทางเดียวกันและนับว่าเซสชั่นที่เกิดขึ้นในทั้งสองทิศทางนี้เป็นส่วนหนึ่งของเซสชั่นเดียวกันระหว่างคู่โนดนั้น ๆ แล้ว การโจมตีทั้งสอบแบบ คือ การดักฟังข้อมูลและการส่งสัญญาณรบกวนจะให้ผลเหมือนกัน เพื่อความชัดเจนจึงขอยกตัวอย่างเพื่ออธิบายดังรูปที่ 3.4 เป็นการส่งข้อมูลของจุดเชื่อมต่อผ่าน A เป็นเกตเวย์ซึ่งใช้เส้นทางในการส่งข้อมูลในฝั่งขาขึ้นและฝั่งขาลงเป็นเส้นทางเดียวกันและนับเซสชั่นที่เกิดขึ้นนี้เป็นเซสชั่นเดียวกันจะพบว่า เซสชั่นนี้ในกรณีของการดักฟังข้อมูลถือว่าเป็นเซสชั่นที่ถูกดักฟัง เช่นเดียวกันกับกรณีของการส่งสัญญาณรบกวนซึ่งนับเซสชั่นดังกล่าวนี้เป็นเซสชั่นที่ถูกสัญญาณรบกวนเช่นกัน

3.2 เกมของการรับส่งข้อมูลในโครงข่าย

จากปัญหาการโจมตีซึ่งเกิดขึ้นระหว่างโครงข่ายกับผู้โจมตีมีลักษณะความขัดแย้งกัน สถานการณ์ดังกล่าว จึงสามารถจำลองในรูปแบบของเกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์ ซึ่งมีผู้เล่นคนหนึ่งเป็นผู้เล่นฝั่งป้องกัน และผู้เล่นอีกคนหนึ่งเป็นผู้เล่นฝั่งโจมตี โดยหลังจากนี้ วิทยานิพนธ์จะเรียกฝั่งป้องกันและฝั่งโจมตีเป็นผู้เล่นฝั่งป้องกันและผู้เล่นฝั่งโจมตีตามลำดับ รายละเอียดทั้งหมดสามารถอธิบายได้ด้วยเกมในรูปแบบปกติประกอบไปด้วยแผนของผู้เล่นทั้งสองฝั่งและค่าของเกมดังนี้

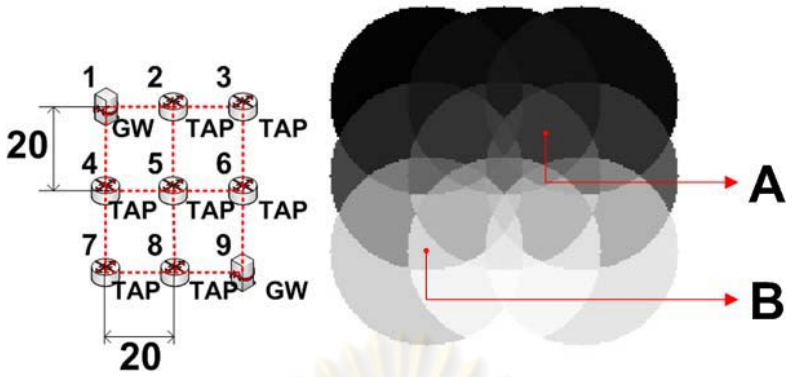
3.2.1 ผู้เล่น 1: ผู้เล่นฝั่งป้องกัน

ผู้เล่น 1 คือ ผู้เล่นฝั่งป้องกัน (โนดทั้งหมดในโครงข่ายไร้สายแบบเมช) โดยผู้เล่นนี้จะสร้างเซสชั่นระหว่างจุดเชื่อมต่อผ่านที่ต้องการรับส่งข้อมูลทั้งหมดกับเกตเวย์อย่างสุ่มเพื่อให้มีจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีมากที่สุด และด้วยการส่งข้อมูลแบบแอดฮ็อกซึ่งผู้ส่งใช้โนดข้างเคียงในการส่งข้อมูลของตนเองไปที่ปลายทาง รวมทั้งเส้นทางที่มีลักษณะเป็นลูป (loop) ย่อมเพิ่มความเสี่ยงในการถูกโจมตีมากขึ้น ดังนั้นผู้เล่นฝั่งป้องกันจึงควรใช้แผนการเล่นเป็น การเลือกส่งข้อมูลอย่างสุ่มในลักษณะของทรี (tree) ซึ่งมีรากอยู่ที่เกตเวย์และเชื่อมต่อกับจุดเชื่อมต่อผ่านทุกโนดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต

3.2.2 ผู้เล่น 2: ผู้เล่นฝั่งโจมตี

ผู้เล่น 2 คือ ผู้เล่นฝั่งโจมตี (ผู้โจมตี) โดยผู้เล่นนี้มีเป้าหมาย คือ การเลือกตำแหน่งในโครงข่ายเพื่อโจมตีเซสชั่นระหว่างจุดเชื่อมต่อผ่านที่ต้องการรับส่งข้อมูลทั้งหมดกับเกตเวย์ให้ได้มากที่สุด ดังนั้นแผนการเล่นของผู้เล่นฝั่งโจมตีจึงเป็น เซตของตำแหน่งที่เป็นไปได้ทั้งหมดในพื้นที่ที่โครงข่ายไร้สายแบบเมชติดตั้งอยู่ ซึ่งเซตที่ได้เป็นเซตอนันต์ เพื่อหลีกเลี่ยงปัญหาดังกล่าวที่ทำให้ผู้เล่นเกมเกมนี้มีแผนการเล่นให้เลือกเป็นเซตอนันต์ จึงจำเป็นต้องพิจารณาแผนการเล่นของผู้เล่นฝั่งโจมตีโดยจัดกลุ่มภายในเซตของตำแหน่งที่เป็นไปได้ทั้งหมดใหม่ และนิยามเป็นเซตของพื้นที่โจมตีซึ่งหากผู้เล่นฝั่งโจมตีเลือกพื้นที่ดังกล่าวเพื่อโจมตีแล้ว จะสามารถโจมตีเซตของโนดได้เป็นเซตเดียวกัน การพิจารณาแผนการเล่นของผู้เล่นฝั่งโจมตีใหม่นี้ทำให้แผนการเล่นของผู้เล่นฝั่งโจมตีเป็นเซตจำกัด และส่งผลให้เกมนี้สามารถหาผลเฉลยได้เสมอตามทฤษฎีมินิแมกซ์ เพื่อความเข้าใจจึงขอยกตัวอย่างเพื่ออธิบายดังรูปที่ 3.5

โครงข่ายในตัวอย่างรูปที่ 3.5 กำหนดให้มีระยะห่างระหว่างโนดเท่ากับ 20 หน่วยของระยะทางทั้งในแนวแกนตั้งและแนวแกนนอน โดยโนดทั้งหมดมีรัศมีการส่งสัญญาณไร้สายเท่ากัน คือ 25 หน่วย ส่วนกรณีที่การโจมตี คือ การส่งสัญญาณรบกวนกำหนดให้ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับ 25 หน่วย ในตัวอย่างนี้หากผู้เล่นฝั่งโจมตีเลือกพื้นที่ A เพื่อใช้โจมตีแล้ว ผู้เล่นฝั่งโจมตีจะสามารถดักฟังข้อมูลหรือส่งสัญญาณรบกวนโนดหมายเลข 2, 3, 5 และ 6 ได้ หรือในกรณีที่ผู้เล่นฝั่งโจมตีเลือกพื้นที่ B เพื่อใช้โจมตี ผู้เล่นฝั่งโจมตีจะสามารถดักฟังข้อมูลหรือส่งสัญญาณรบกวนโนดหมายเลข 4, 7 และ 8 ได้ เป็นต้น



รูปที่ 3.5: การเปลี่ยนเซตของตำแหน่งมาเป็นเซตของพื้นที่โจมตีที่เป็นไปได้ทั้งหมด

3.2.3 ค่าของเกม

เมื่อเปรียบเทียบความเร็วของการส่งข้อมูลของโครงข่าย กับความเร็วในการเคลื่อนที่ของผู้เล่นฝั่งโจมตีแล้ว พบว่าการส่งข้อมูลมีความเร็วมากกว่าผู้เล่นฝั่งโจมตีมาก ดังนั้นผู้เล่นฝั่งโจมตีจะเห็นการเชื่อมต่อระหว่างจุดเชื่อมต่อผ่านกับเกตเวย์ทุกเซสชั่นเกิดขึ้นพร้อม ๆ กัน โดยไม่สามารถเคลื่อนที่ไปดักฟังข้อมูลที่เหลือ หรือเคลื่อนที่ไปเพื่อส่งสัญญาณรบกวนการรับส่งข้อมูลอื่นได้ทัน ดังนั้นค่าของเกมจึงนิยามเป็น จำนวนเซสชั่นระหว่างจุดเชื่อมต่อผ่านที่ต้องการรับส่งข้อมูลกับเกตเวย์ที่ปลอดภัยจากการถูกโจมตี โดยเซสชั่นที่ถูกโจมตีสามารถอธิบายได้ดังนี้

1. กรณีที่การโจมตี คือ การดักฟังข้อมูล เซสชั่นที่ถูกโจมตีหรือเซสชั่นที่ถูกดักฟังจะหมายถึง เซสชั่นที่มีโนดที่ถูกดักฟังอยู่เป็นส่วนหนึ่งในเส้นทางบนทรีของการส่งข้อมูลที่เลือกใช้ และเซสชั่นดังกล่าวใช้โนดนั้นส่งข้อมูลออกมาผ่านตัวกลางไร้สาย
2. กรณีที่การโจมตี คือ การส่งสัญญาณรบกวน เซสชั่นที่ถูกโจมตีหรือเซสชั่นที่ถูกสัญญาณรบกวนจะหมายถึง เซสชั่นที่มีโนดที่ถูกสัญญาณรบกวนอยู่เป็นส่วนหนึ่งในเส้นทางบนทรีของการส่งข้อมูลที่เลือกใช้

ความหมายของเซสชั่นที่ถูกโจมตีที่แตกต่างกันตามชนิดของการโจมตีนี้ มีผลทำให้การนับว่าเซสชั่นใดเป็นเซสชั่นที่ปลอดภัยจากการถูกโจมตีรวมถึงการเลือกแผนการเล่นเพื่อป้องกันของผู้เล่นฝั่งป้องกันและการเลือกแผนการเล่นเพื่อโจมตีของผู้เล่นฝั่งโจมตีมีความแตกต่างกันด้วย แต่ลักษณะของเกมยังคงมีความเหมือนกัน คือ ผู้เล่นฝั่งป้องกันต้องการให้มีจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีมากที่สุด ในขณะที่ผู้เล่นฝั่งโจมตีต้องการให้มีจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีน้อยที่สุดอยู่เช่นเดิม

หลังจากการนิยามสถานการณ์ดังกล่าวในรูปแบบของเกมการรับส่งข้อมูลในโครงข่ายแล้ว ค่าของเกมในที่นี้จะนิยามเป็นค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตี (expected number of secure sessions, ESS) ซึ่งสามารถคำนวณได้จากการแจกแจงความน่าจะเป็นในการเลือกแผนการเล่นหลังจากการหาผลเฉลยที่เหมาะสมที่สุดของผู้เล่นทั้งสองฝั่ง ในทางปฏิบัติค่า ESS ที่ได้จะหมายถึง จำนวนเซสชั่นขั้นต่ำที่สุดโดยเฉลี่ยที่พึงได้ปลอดภัยจากการโจมตีเมื่อโครงข่ายใช้รูปแบบการรับส่งข้อ

มูลอย่างเหมาะสมที่สุด ดังนั้นค่า ESS จึงสามารถบ่งชี้ระดับความปลอดภัยขั้นต่ำที่พึงได้ของโครงข่ายและเป็นมาตรวัดที่เหมาะสมสำหรับการวิจัยในอนาคต เกี่ยวกับการออกแบบโครงข่ายไร้สายแบบเมชที่ทนทานต่อการโจมตีต่าง ๆ ได้

3.3 สัญลักษณ์พื้นฐาน

สำหรับการตั้งโจทย์ปัญหาด้วยวิธีการของเกมในโครงข่ายไร้สายแบบเมช วิทยานิพนธ์นี้จะใช้นิยามของตัวแปรต่าง ๆ ดังนี้

M : แทนจำนวนรูปแบบการเลือกรับส่งข้อมูลในลักษณะของทรี (tree) ซึ่งมีรากอยู่ที่เกตเวย์และเชื่อมต่อกับจุดเชื่อมต่อผ่านทุกโนดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ตที่เป็นไปได้ทั้งหมด

N : แทนจำนวนรูปแบบพื้นที่โจมตีที่เป็นไปได้ทั้งหมด

i : แทนหมายเลขของรูปแบบการเลือกรับส่งข้อมูลในลักษณะของทรีซึ่งมีรากอยู่ที่เกตเวย์และเชื่อมต่อกับจุดเชื่อมต่อผ่านทุกโนดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต

j : แทนหมายเลขรูปแบบพื้นที่โจมตีที่เป็นไปได้

p_i : แทนความน่าจะเป็นที่ผู้เล่นฝั่งป้องกันจะเลือกทรีรูปแบบที่ i ในการรับส่งข้อมูลระหว่างเกตเวย์และจุดเชื่อมต่อผ่านทุกโนดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต

P : การแจกแจงความน่าจะเป็นในการเลือกรูปแบบการรับส่งข้อมูลของผู้เล่นฝั่งป้องกัน

q_j : แทนความน่าจะเป็นที่ผู้เล่นฝั่งโจมตีจะเลือกอยู่ในพื้นที่โจมตีรูปแบบที่ j

Q : การแจกแจงความน่าจะเป็นในการเลือกรูปแบบพื้นที่โจมตีของผู้เล่นฝั่งโจมตี

$s_{i,j}$: จำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีเมื่อผู้เล่นฝั่งป้องกันเลือกทรีรูปแบบที่ i ในการรับส่งข้อมูล และผู้เล่นฝั่งโจมตีเลือกอยู่ในพื้นที่โจมตีรูปแบบที่ j

x_i : ตัวแปรช่วย

y_j : ตัวแปรช่วย

n : แทนรอบของการเล่นเกม

3.4 การวิเคราะห์และแก้ปัญหาโดยกรรมวิธี MSA (Method of Successive Average)

การหาผลเฉลยในวิทยานิพนธ์นี้จะใช้หลักการโต้ตอบที่ดีที่สุด (best response) ร่วมกับกระบวนการปรับปรุงความน่าจะเป็นด้วย MSA ซึ่งเป็นกระบวนการที่เป็นที่รู้จักและถูกใช้ในงานวิจัยซึ่งศึกษาการจัดเส้นทางแบบเฟ้นสุ่ม เช่น [5]-[7] นอกจากนี้กระบวนการปรับปรุงความน่าจะเป็นด้วย MSA ยังสามารถแก้ปัญหาได้ทั้งกรณีปัญหาเชิงสถิต (static) และเชิงพลวัต (dynamic) โดยจำลองเหตุการณ์ให้ผู้เล่นทั้งสองฝั่งเลือกและเรียนรู้ในการปรับปรุงแผนการเล่นอย่างดีที่สุด สอดคล้องกับการจำลองเหตุการณ์จริงในวิทยานิพนธ์ฉบับนี้ และ MSA ยังรับประกันการลู่เข้าของผลเฉลยได้อีกด้วย [18] วิธีการวิเคราะห์และแก้ปัญหาด้วยวิธีดังกล่าวมีขั้นตอนดังนี้

1. กำหนดค่าความน่าจะเป็นเริ่มต้นในการเลือกแผนการเล่นของผู้เล่นทั้งสองฝั่ง ให้แต่ละแผนมีความเท่าเทียมกัน โดยความน่าจะเป็นที่ผู้เล่นฝั่งป้องกันจะเลือกทรีรูปแบบที่ i (p_i) และความน่าจะเป็นที่ผู้เล่นฝั่งโจมตีจะเลือกอยู่ในพื้นที่โจมตีรูปแบบที่ j (q_j) มีค่าเริ่มต้นเป็น

$$p_i = \frac{1}{M}, \quad \text{สำหรับทุกค่า} \quad i$$

$$q_j = \frac{1}{N}, \quad \text{สำหรับทุกค่า} \quad j$$

พร้อมทั้งกำหนดรอบของการเล่นเกมเริ่มแรกเป็นรอบที่ 1 $(n = 1)$

2. คำนวณค่า ESS ที่ผู้เล่นฝั่งป้องกันจะได้สำหรับกรณีที่ผู้เล่นฝั่งป้องกันเลือกแผนการเล่น i (i= 1, 2, …, M)

$$ESS_i = \sum_{j=1}^{N} [q_j s_{i,j}]$$

3. คำนวณค่า ESS ที่ผู้เล่นฝั่งโจมตีจะได้สำหรับกรณีที่ผู้เล่นฝั่งโจมตีเลือกแผนการเล่น j (j= 1, 2, …, N)

$$ESS_j = \sum_{i=1}^{M} [p_i s_{i,j}]$$

4. ผู้เล่นฝั่งป้องกันเลือกแผนการเล่นโต้ตอบที่ดีที่สุด $\hat{i}$ ซึ่งทำให้ค่า ESS_i มีค่าสูงที่สุด

$$\hat{i} = \arg\max_i \{ESS_i\}$$

5. ผู้เล่นฝั่งโจมตีเลือกแผนการเล่นโต้ตอบที่ดีที่สุด $\hat{j}$ ซึ่งทำให้ค่า ESS_j มีค่าต่ำที่สุด

$$\hat{j} = \arg\min_j \{ESS_j\}$$

6. ผู้เล่นฝั่งป้องกันปรับการแจกแจงความน่าจะเป็นในการเลือกแผนการเล่น P โดยเพิ่มความน่าจะเป็นที่รูปแบบการรับส่งข้อมูลรูปแบบที่ได้เลือกไว้ในขั้นตอนที่ 4 โดยใช้สมการในการปรับค่าตามระเบียบวิธี MSA ดังสมการ

$$p_i \leftarrow \left(\frac{1}{n}\right) x_i + \left(\frac{n-1}{n}\right) p_i$$

โดยที่ค่าตัวแปรช่วย x_i จะมีค่าเท่ากับ 1 เมื่อ $i = \hat{i}$ และมีค่าเป็น 0 เมื่อ $i \neq \hat{i}$

7. ผู้เล่นฝั่งโจมตีปรับการแจกแจงความน่าจะเป็นในการเลือกแผนการเล่น Q โดยเพิ่มความน่าจะเป็นที่รูปแบบพื้นที่โจมตีรูปแบบที่ได้เลือกไว้ในขั้นตอนที่ 5 โดยใช้สมการในการปรับค่าตามระเบียบวิธี MSA ดังสมการ

$$q_j \leftarrow \left(\frac{1}{n}\right) y_j + \left(\frac{n-1}{n}\right) q_j$$

โดยที่ค่าตัวแปรช่วย y_j จะมีค่าเท่ากับ 1 เมื่อ $j = \hat{j}$ และมีค่าเป็น 0 เมื่อ $j \neq \hat{j}$

8. หาค่า ESS ของระบบจากสมการ

$$ESS = \sum_{i=1}^{M} \sum_{j=1}^{N} p_i q_j s_{i,j}$$

9. ปรับค่ารอบของการเล่น $n \leftarrow n+1$ และกลับไปทำขั้นตอนที่ 2-8 ใหม่จนกระทั่งเกิดการลู่เข้าของค่า ESS

สำหรับการวิเคราะห์ในทางปฏิบัติพบว่าปัญหาที่พิจารณา ณ จุดสมดุลของเกมอาจมีคำตอบที่เหมาะสมที่สุดหลายคำตอบได้ แต่จากทฤษฎีเกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์กล่าวว่า ในทุกคำตอบนั้นจะให้ค่าของเกม ESS เท่ากันเสมอ ดังนั้นแต่ละคำตอบที่ได้จึงไม่มีผลกระทบต่อการชี้วัดระดับความปลอดภัยด้วยตัวชี้วัด ESS ที่นำเสนอ รวมทั้งคำตอบที่เหมาะสมที่สุดซึ่งในที่นี้ คือ การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดนั้น โครงข่ายสามารถเลือกใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดจากหนึ่งคำตอบในหลายคำตอบนี้เพื่อใช้ป้องกันการโจมตีทั้งสองแบบได้

โดยทั่วไปการวิเคราะห์ปัญหาเกมการรับส่งข้อมูลในโครงข่ายจะมีอุปสรรค คือ ความซับซ้อนในการหาผลเฉลย ซึ่งวิทยานิพนธ์ฉบับนี้ได้แก้ปัญหาดังกล่าว โดยใช้หลักการของกลยุทธเด่นเพื่อตัดแผนที่ด้อยกว่าของผู้เล่นทั้งสองฝ่ายออกก่อนการหาผลเฉลยด้วยกรรมวิธี MSA นอกจากนั้น แผนการเล่นของผู้เล่นที่มีความเท่าเทียมกันซึ่งหมายถึง แผนการเล่นซึ่งหากวิเคราะห์จากตารางผลได้ผลเสียแล้ว แผนการเล่นเหล่านั้นให้ค่าผลได้ผลเสียเท่ากันในทุกกรณี โดยวิทยานิพนธ์ฉบับนี้จะเลือกแผนการเล่นจากแผนการเล่นที่เท่าเทียมกันเหล่านั้นมาเพียงหนึ่งแผน เพื่อลดความซับซ้อนของการหาผลเฉลย และหลังจากการหาผลเฉลยเสร็จสิ้น หากแผนการเล่นเพียงหนึ่งแผนนั้นถูกเลือกด้วยค่าความน่าจะเป็นค่าหนึ่ง ในวิทยานิพนธ์นี้จะแบ่งความน่าจะเป็นค่านั้นไปยังทุกแผนการเล่นที่เท่าเทียมกันนั้น ๆ ทั้งหมดอย่างเท่าเทียมกัน

หลังจากการวิเคราะห์ปัญหาและจำลองโครงข่ายไร้สายแบบเมชซึ่งตกอยู่ภายใต้การโจมตีโดยการดักฟังข้อมูลและการส่งสัญญาณรบกวนแล้ว โนดในโครงข่ายจะใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดจากกระบวนการหาผลเฉลยโดยกรรมวิธี MSA ที่กล่าวไว้ข้างต้นเพื่อใช้ป้องกันการโจมตีทั้งสองแบบ โดยระเบียบวิธีที่นำเสนอซึ่งสามารถใช้หาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดได้นั้น จะถูกทดสอบและเปรียบเทียบกับระเบียบวิธีอื่นในด้านต่าง ๆ ผ่านตัวชี้วัด ESS ในบทต่อไป

บทที่ 4

ผลการทดสอบ

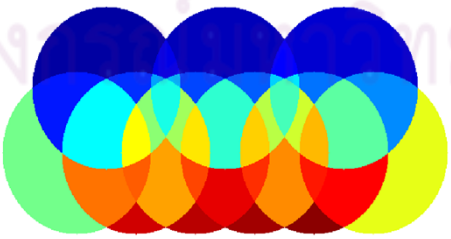
เนื้อหาบทนี้จะเป็นการทดสอบระเบียบวิธีที่นำเสนอในการหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุด รวมทั้งศึกษาผลกระทบจากการโจมตีทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมช ซึ่งการทดสอบแบ่งออกเป็น 5 หัวข้อดังนี้

หัวข้อที่ 4.1 เป็นการทดสอบผลกระทบจากการโจมตีทั้งสองแบบที่เกิดขึ้นในการส่งข้อมูลแต่ละทิศทางในโครงข่ายอย่างง่าย หัวข้อที่ 4.2 เป็นการทดสอบผลกระทบจากการโจมตีทั้งสองแบบเมื่อโครงข่ายมีขนาดใหญ่ขึ้น นอกจากนั้นภายในหัวข้อนี้ยังได้เปรียบเทียบระเบียบวิธีที่นำเสนอในการหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดกับระเบียบวิธีอื่น หัวข้อที่ 4.3 เป็นการทดสอบผลกระทบเมื่อโนดในโครงข่ายมีรัศมีการส่งสัญญาณไร้สายเพิ่มขึ้น หลังจากนั้นในหัวข้อที่ 4.4 เป็นการทดสอบผลกระทบจากการโจมตีเมื่อมีการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายในรูปแบบที่แตกต่างกัน และหัวข้อที่ 4.5 ซึ่งเป็นหัวข้อสุดท้าย เป็นการทดสอบผลกระทบจากการโจมตีทั้งสองแบบในกรณีที่ผู้เล่นฝั่งโจมตีไม่สามารถเลือกพื้นที่เพื่อโจมตีเกตเวย์ได้

ในการทดสอบทั้งหมด วิทยานิพนธ์ฉบับนี้ใช้โปรแกรม MATLAB จำลองสถานการณ์และใช้การคำนวณแบบกระจาย (distributed computing) บนเครื่องคอมพิวเตอร์แบบคลัสเตอร์

4.1 ผลการทดสอบในโครงข่ายอย่างง่าย

ก. โครงข่ายอย่างง่าย



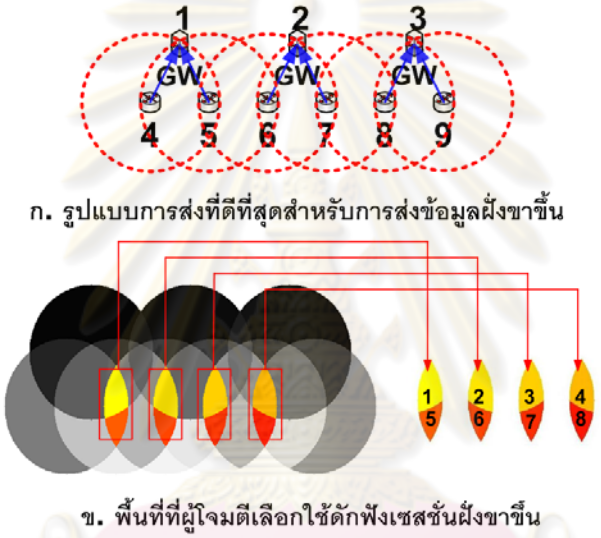
ข. พื้นที่โจมตีที่เป็นไปได้ทั้งหมด

รูปที่ 4.1: โครงข่ายไร้สายแบบเมชอย่างง่ายและพื้นที่โจมตีที่เป็นไปได้ทั้งหมด

การทดสอบนี้เป็นการเปรียบเทียบระดับความปลอดภัยของโครงข่ายไร้สายแบบเมชเมื่อมีการดักฟัง

ข้อมูลและการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงด้วยตัวชี้วัด ESS โครงข่ายไร้สายแบบเมชที่นำมาทดสอบเป็นโครงข่ายอย่างง่ายซึ่งมีพื้นที่โจมตีที่เป็นไปได้ทั้งหมดดังแสดงในรูปที่ 4.1 โดยโครงข่ายประกอบไปด้วยเกตเวย์ 3 โนดวางห่างกัน 20 หน่วยของระยะทางในแนวแกนนอนและจุดเชื่อมต่อผ่าน 6 โนดวางห่างกัน 20 หน่วยในแนวแกนนอนและวางห่างกับเกตเวย์ 20 หน่วยในแนวแกนตั้ง กำหนดให้จุดเชื่อมต่อผ่านทั้งหมดมีรัศมีการส่งสัญญาณไร้สายเท่ากัน คือ 25 หน่วย และในกรณีที่การโจมตีเป็นการส่งสัญญาณรบกวน กำหนดให้ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับ 25 หน่วย ผลการทดสอบมีดังนี้

4.1.1 กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น



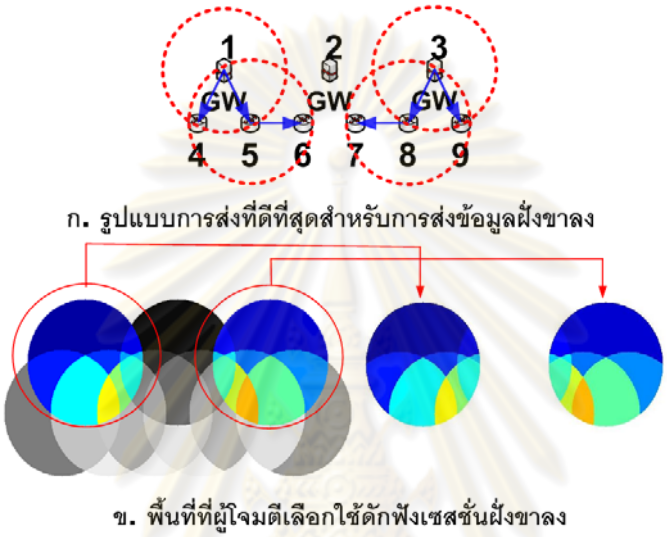
รูปที่ 4.2: ผลการทดสอบกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น

เมื่อทดสอบการจัดเส้นทางแบบเฟ้นสุ่มเพื่อป้องกันการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นพบว่าได้ค่า $ESS = 3$ ซึ่งมีความหมายคือ เมื่อโครงข่ายใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดแล้ว ในระยะยาวโครงข่ายจะได้จำนวนเซสชั่นระหว่างจุดเชื่อมต่อผ่านกับเกตเวย์ที่ไม่ถูกดักฟัง 3 เซสชั่นเป็นอย่างน้อย โดยการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดและลักษณะการดักฟังข้อมูลของผู้เล่นฝั่งโจมตีในกรณีร้ายแรงที่สุดในการส่งข้อมูลฝั่งขาขึ้นแสดงได้ดังรูปที่ 4.2

เนื่องจากการส่งข้อมูลฝั่งขาขึ้น เกตเวย์ทุกโนดจะไม่ส่งข้อมูลออกมาผ่านตัวกลางไร้สาย หากผู้เล่นฝั่งโจมตีเลือกพื้นที่โจมตีของเกตเวย์เพียงอย่างเดียวเพื่อดักฟังข้อมูลแล้ว ผู้เล่นฝั่งโจมตีจะไม่สามารถดักฟังเซสชั่นใด ๆ ได้ ดังนั้นผู้เล่นฝั่งโจมตีจึงเลือกดักฟังเซสชั่นในพื้นที่โจมตีของโนดข้างเคียงของเกตเวย์ที่ซ้อนทับกันพื้นที่ใดพื้นที่หนึ่งจาก 8 พื้นที่ดังรูปที่ 4.2 ข. ส่วนการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดสำหรับการส่งข้อมูลฝั่งขาขึ้นเป็นลักษณะการกระจายเส้นทางอย่างสมดุล (load balancing) ดังรูปที่ 4.2 ก. เพื่อความชัดเจนจึงขออธิบายด้วยการยกตัวอย่างดังต่อไปนี้ หากผู้เล่นฝั่งโจมตีเลือกพื้นที่โจมตีที่ 1 ดังรูปที่ 4.2 ข. ผู้เล่นฝั่งโจมตีจะสามารถดักฟังข้อมูลจากเกตเวย์ 1 และจุดเชื่อมต่อผ่าน 4, 5, 6 เมื่อโครงข่ายไร้สายแบบเมชใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดดังรูป

ที่ 4.2 ก. แล้วจะได้จำนวนเซสชั่นที่ไม่ถูกดักฟังเท่ากับ 3 เซสชั่น คือ เซสชั่นของจุดเชื่อมต่อผ่าน 7, 8, 9 กับเกตเวย์เพราะผู้เล่นฝั่งโจมตีสามารถดักฟังเซสชั่นของจุดเชื่อมต่อผ่าน 4, 5, 6 กับเกตเวย์ได้นั่นเอง นอกจากนี้จะเห็นได้ว่าการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดในกรณีนี้มีเพียงรูปแบบเดียวเนื่องจากโครงข่ายที่นำมาทดสอบนี้เป็นโครงข่ายที่มีขนาดเล็ก

4.1.2 กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง



ก. รูปแบบการส่งที่ดีที่สุดสำหรับการส่งข้อมูลฝั่งขาลง

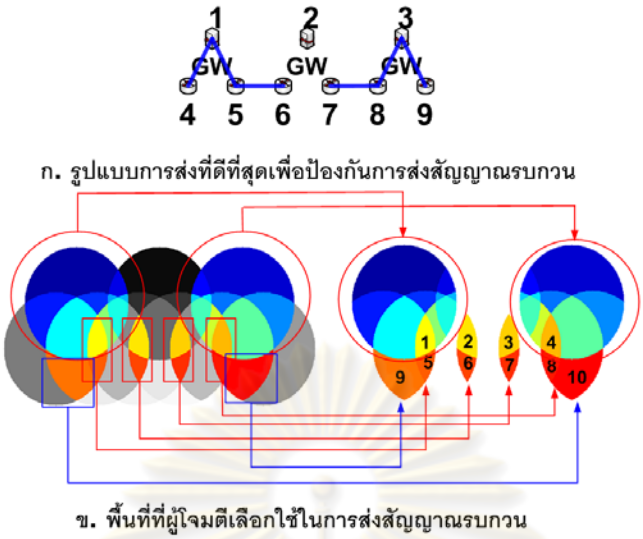
ข. พื้นที่ที่ผู้โจมตีเลือกใช้ดักฟังเซสชั่นฝั่งขาลง

รูปที่ 4.3: ผลการทดสอบกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง

เมื่อทดสอบการจัดเส้นทางแบบเฟ้นสุ่มเพื่อป้องกันการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงพบว่าได้ค่า $ESS = 3$ เช่นเดียวกันกับกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น แต่ความแตกต่างของการส่งข้อมูลในแต่ละทิศทางนั้นทำให้ลักษณะของการเลือกพื้นที่โจมตีเพื่อดักฟังข้อมูลของผู้เล่นฝั่งโจมตีแตกต่างกัน โดยการส่งข้อมูลฝั่งขาลง ผู้เล่นฝั่งโจมตีจะเลือกดักฟังเซสชั่นในพื้นที่โจมตีของเกตเวย์พื้นที่ใดพื้นที่หนึ่งดังรูปที่ 4.3 ข. เพราะการส่งข้อมูลฝั่งขาลงนั้นเกตเวย์จะต้องส่งข้อมูลของทุกเซสชั่นออกมาผ่านตัวกลางไร้สาย ดังนั้นโครงข่ายจึงต้องการการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดเพื่อป้องกันการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงที่ต่างกันออกไปดังรูปที่ 4.3 ก. โดยการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดเพื่อป้องกันการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง จะเป็นลักษณะการส่งข้อมูลโดยไม่ใช้เกตเวย์ที่มีพื้นที่โจมตีซ้อนทับกันอยู่เพื่อใช้ส่งพร้อมกันนั่นเอง นอกจากนี้จะเห็นได้ว่าการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดในกรณีนี้มีเพียงรูปแบบเดียวเช่นกัน

4.1.3 กรณีการส่งสัญญาณรบกวนในโครงข่าย

เมื่อทดสอบการจัดเส้นทางแบบเฟ้นสุ่มเพื่อป้องกันการส่งสัญญาณรบกวนพบว่าได้ $ESS = 3$ เช่นเดียวกับกรณีการดักฟังข้อมูลในการส่งข้อมูลทั้งสองทิศทางข้างต้น แต่พื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีสามารถเลือกใช้ส่งสัญญาณรบกวนนั้นมีมากกว่ากรณีการดักฟังข้อมูลดังแสดงในรูปที่ 4.4 ข. โดยพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีเลือกประกอบไปด้วยพื้นที่โจมตีของเกตเวย์ พื้นที่โจมตีของโนดข้างเคียงของเกตเวย์ที่ซ้อน

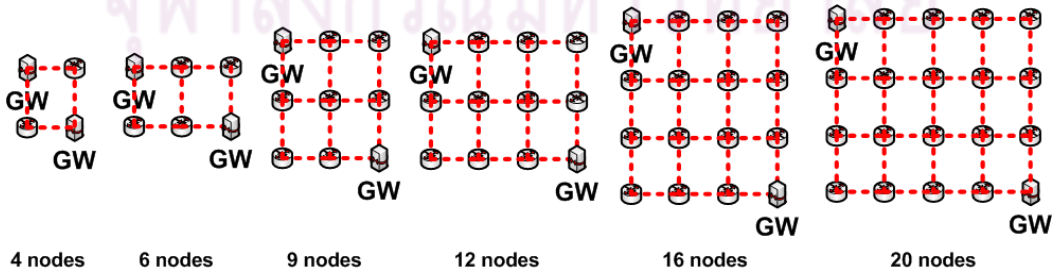


รูปที่ 4.4: ผลการทดสอบกรณีการส่งสัญญาณรบกวนในโครงข่าย

ทับกัน และพื้นที่หมายเลข 9 และ 10 จากรูป และการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดเพื่อป้องกันการส่งสัญญาณรบกวนแสดงได้ดังรูปที่ 4.4 ก. ซึ่งเป็นลักษณะการส่งข้อมูลโดยไม่ใช้เกตเวย์ที่มีพื้นที่โจมตีซ้อนทับกันอยู่ เพื่อใช้ส่งพร้อมกันเช่นเดียวกันกับการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดเพื่อป้องกันการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง เพราะผู้เล่นฝั่งโจมตีสามารถส่งสัญญาณรบกวนเกตเวย์ 2 โนดที่อยู่ติดกันได้พร้อมกัน

กล่าวโดยสรุปสำหรับการทดสอบในโครงข่ายไร้สายแบบเมชอย่างง่าย เมื่อมีการโจมตีโดยการดักฟังข้อมูลและการส่งสัญญาณรบกวน โดยผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับรัศมีการส่งสัญญาณไร้สายของโนด พบว่าได้ค่า ESS เท่ากัน คือ 3 แต่พื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีเลือกใช้รวมถึงการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดเพื่อใช้ป้องกันการโจมตีแต่ละแบบมีความแตกต่างกันขึ้นอยู่กับชนิดของการโจมตี รวมถึงกรณีการดักฟังข้อมูลซึ่งการป้องกันจะขึ้นอยู่กับทิศทางของการส่งข้อมูลในโครงข่ายไร้สายแบบเมชอีกด้วย

4.2 ผลกระทบของการเพิ่มขนาดของโครงข่าย

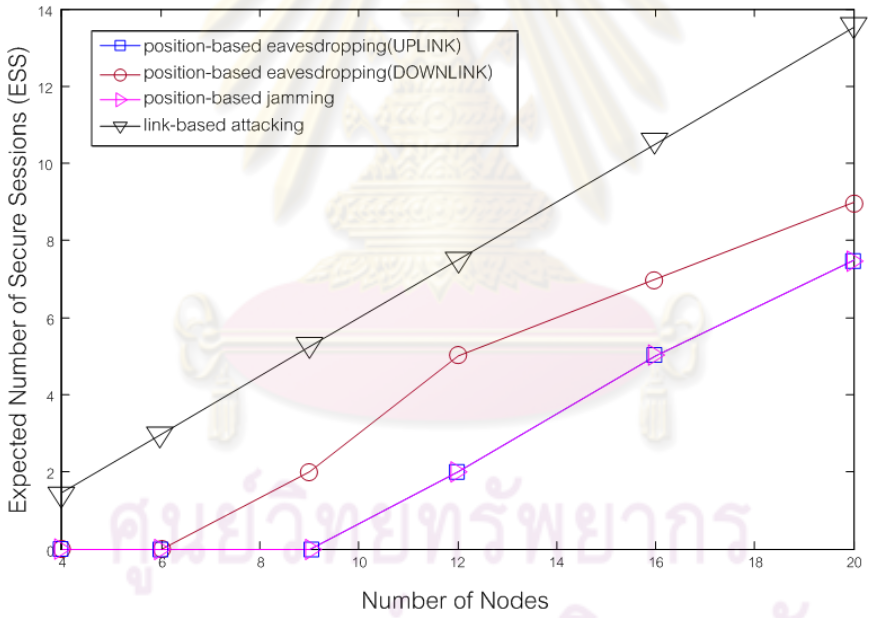


รูปที่ 4.5: การเพิ่มขนาดของโครงข่ายแบบตาราง

จากผลการทดสอบในหัวข้อที่ 4.1 ซึ่งทดสอบกับโครงข่ายอย่างง่าย จะเห็นว่าทุกกรณีได้ค่า ESS

เท่ากันเนื่องจากโครงข่ายดังกล่าวมีขนาดเล็ก ดังนั้นการทดสอบในหัวข้อนี้จึงมุ่งศึกษาผลกระทบจากการโจมตีทั้งสองแบบ คือ การดักฟังข้อมูลและการส่งสัญญาณรบกวนเมื่อโครงข่ายมีขนาดเพิ่มขึ้น โครงข่ายไร้สายแบบเมชที่นำมาทดสอบในหัวข้อนี้เป็นโครงข่ายแบบตาราง (grid network) ดังแสดงในรูปที่ 4.5 ซึ่งเป็นการเชื่อมต่ออย่างง่ายที่สามารถครอบคลุมพื้นที่ให้บริการได้ทั่วถึง โครงข่ายดังกล่าวประกอบด้วยเกตเวย์ 2 โนดติดตั้งอยู่ที่มุมซ้ายบนและมุมขวาล่างของโครงข่ายในทุกกรณี และโนดที่เหลือจะเป็นจุดเชื่อมต่อผ่านโนดทั้งหมดในโครงข่ายถูกวางห่างกันเท่ากับ 20 หน่วยทั้งในแนวแกนตั้งและแนวแกนนอน รัศมีในการส่งสัญญาณไร้สายของทุกโนด คือ 25 หน่วย กรณีการโจมตีคือการส่งสัญญาณรบกวนกำหนดให้ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับ 25 หน่วย

นอกจากนั้นการทดสอบในหัวข้อนี้จะเปรียบเทียบลักษณะการโจมตี 2 รูปแบบที่แตกต่างกัน รูปแบบแรก คือ ลักษณะการโจมตีที่ผู้เล่นฝั่งโจมตีมุ่งโจมตีที่ข่ายเชื่อมโยงของโครงข่าย (link-based attacking) ซึ่งเป็นลักษณะการโจมตีที่ใช้ในงานวิจัย [10], [11] กับรูปแบบที่สอง คือ ลักษณะการโจมตีที่คำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตีกับพื้นที่ที่โครงข่ายติดตั้งอยู่ (position-based attacking) ซึ่งเป็นลักษณะการโจมตีที่ถูกนำเสนอโดยวิทยานิพนธ์ฉบับนี้ ผลการทดสอบที่ได้แสดงดังรูปที่ 4.6



รูปที่ 4.6: ผลกระทบของการเพิ่มขนาดของโครงข่าย

จะเห็นว่าในทุกกรณีของลักษณะการโจมตีที่ข่ายเชื่อมโยงเมื่อเปรียบเทียบกับลักษณะการโจมตีที่คำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตีได้ค่า ESS สูงกว่าซึ่งหมายถึง ลักษณะการโจมตีที่คำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตีซึ่งเป็นลักษณะการโจมตีที่สอดคล้องกับโครงข่ายไร้สายมากกว่านั้นมีความรุนแรงกว่าลักษณะการโจมตีที่ข่ายเชื่อมโยง โดยเหตุผลที่เป็นเช่นนั้นสามารถอธิบายผลตามชนิดของการโจมตีดังนี้

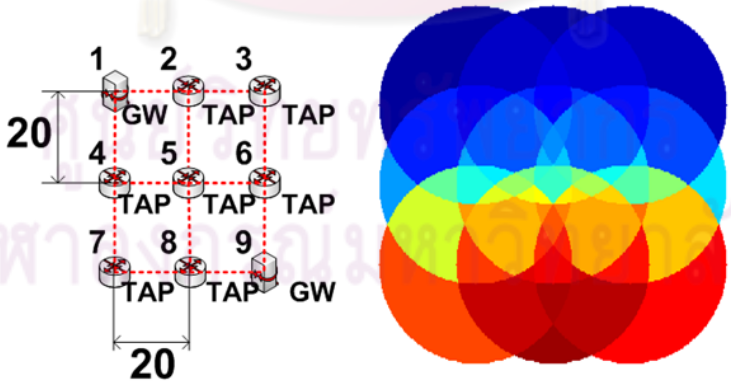
กรณีการดักฟังข้อมูลหากเป็นการโจมตีที่ข่ายเชื่อมโยงนั้นจะหมายความว่า ผู้เล่นฝั่งโจมตีเลือกดักฟังข้อมูลในข่ายเชื่อมโยงหนึ่งแล้วจะดักฟังข้อมูลจากข่ายเชื่อมโยงนั้นเพียงข่ายเชื่อมโยงเดียวโดยไม่มีการเปลี่ยนไปดักฟังข้อมูลจากข่ายเชื่อมโยงอื่นอีก แต่การดักฟังข้อมูลที่คำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตี

มีสมมุติฐานว่า ผู้เล่นฝั่งโจมตีสามารถดักฟังข้อมูลจากข่ายเชื่อมโยงหนึ่งแล้วสามารถเปลี่ยนมาดักฟังข้อมูลจากอีกข่ายเชื่อมโยงหนึ่งที่ผ่านตำแหน่งที่ผู้เล่นฝั่งโจมตีอยู่ได้ หรือแม้กระทั่งในกรณีที่ผู้เล่นฝั่งโจมตีมีความสามารถที่จะดักฟังข้อมูลจากทุกข่ายเชื่อมโยงที่ผ่านตำแหน่งที่ผู้เล่นฝั่งโจมตีอยู่ ดังนั้นการดักฟังข้อมูลโดยคำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตีจึงมีความรุนแรงมากกว่า เนื่องจากผู้เล่นฝั่งโจมตีสามารถดักฟังข้อมูลจากข่ายเชื่อมโยงหลายอันซึ่งผ่านตำแหน่งผู้เล่นฝั่งโจมตีอยู่ได้พร้อม ๆ กัน

กรณีการส่งสัญญาณรบกวนหากเป็นการโจมตีที่ข่ายเชื่อมโยงจะหมายถึง ผู้เล่นฝั่งโจมตีจะเลือกส่งสัญญาณรบกวนคู่สื่อสารได้เพียงหนึ่งคู่สื่อสารเท่านั้น แต่ความเป็นจริงการส่งสัญญาณรบกวนในโครงข่ายไร้สายนั้นมีผลกับคู่สื่อสารอื่นด้วย ขึ้นกับรัศมีในการส่งสัญญาณรบกวนของผู้เล่นฝั่งโจมตี ดังนั้นการส่งสัญญาณรบกวนโดยคำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตีจึงมีค่า ESS ที่ต่ำกว่าการส่งสัญญาณรบกวนที่ข่ายเชื่อมโยงซึ่งผู้เล่นฝั่งโจมตีหนึ่งคนจะส่งสัญญาณรบกวนคู่สื่อสารได้เพียงหนึ่งคู่สื่อสารเท่านั้น

นอกจากนี้เมื่อพิจารณาลักษณะการโจมตีที่ข่ายเชื่อมโยงแล้วจะพบว่า การดักฟังข้อมูลกับการส่งสัญญาณรบกวนให้ผลเหมือนกันซึ่งหมายถึง ระเบียบวิธีที่ใช้ลักษณะการโจมตีที่ข่ายเชื่อมโยงไม่สามารถแยกความแตกต่างของการโจมตีที่ต่างชนิดกันได้ รวมถึงลักษณะการโจมตีที่ข่ายเชื่อมโยงยังไม่สามารถแยกความแตกต่างของการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโคงข่ายไร้สายแบบเมชออกจากกันได้อีกด้วย

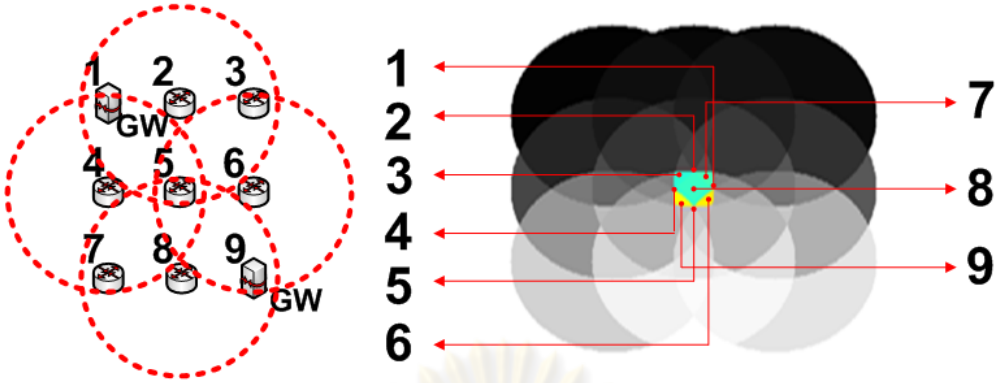
กรณีลักษณะการโจมตีที่คำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตีจากรูปที่ 4.6 จะเห็นว่า ลักษณะการโจมตีที่นำเสนอนั้น สามารถแยกความแตกต่างของผลกระทบจากการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและขาลงออกจากกันได้ โดยจะเห็นว่าการส่งข้อมูลในฝั่งขาลงได้ค่า ESS สูงกว่าการส่งข้อมูลฝั่งขาขึ้น รวมไปถึงการโจมตีที่คำนึงถึงตำแหน่งของผู้เล่นฝั่งโจมตียังสามารถแยกความแตกต่างระหว่างการดักฟังข้อมูลกับการส่งสัญญาณรบกวนออกจากกันได้ ซึ่งจะเห็นว่าการส่งสัญญาณรบกวนได้ค่า ESS ต่ำกว่ากรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงและได้ค่า ESS เท่ากับกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น



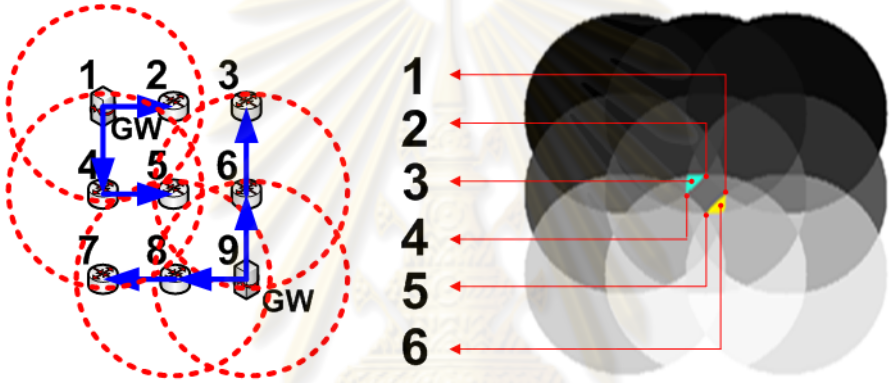
รูปที่ 4.7: โครงข่ายแบบตารางขนาด 9 โนดและพื้นที่โจมตีที่เป็นไปได้ทั้งหมด

เหตุผลที่แต่ละกรณีได้ค่า ESS ต่างกันนั้นจะขออธิบายด้วยการยกตัวอย่างกรณีโครงข่ายขนาด 9 โนดซึ่งมีพื้นที่โจมตีที่เป็นไปได้ทั้งหมดแสดงดังรูปที่ 4.7

กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นซึ่งได้ค่า $ESS = 0$ นั้นมีความหมายคือ ผู้เล่นฝั่งโจม



รูปที่ 4.8: รูปแบบการรับส่งข้อมูลและพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีเลือกใช้ดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นของโครงข่ายแบบตารางขนาด 9 โนด

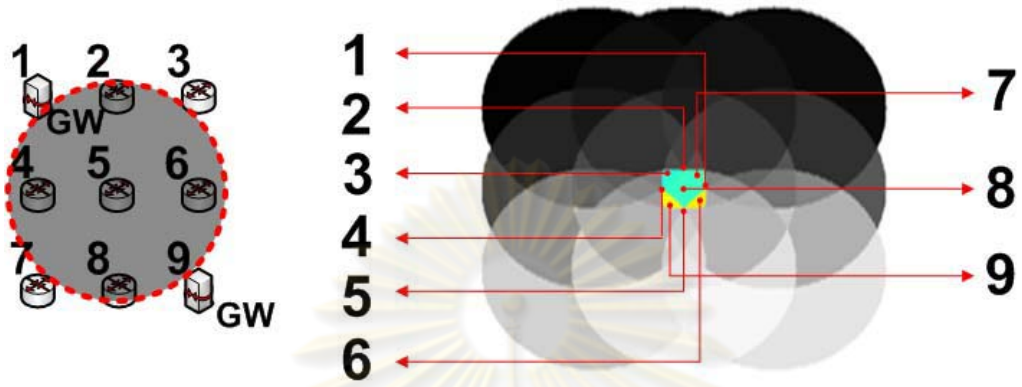


รูปที่ 4.9: รูปแบบการรับส่งข้อมูลและพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีเลือกใช้ดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงของโครงข่ายแบบตารางขนาด 9 โนด

ตีสามารถดักฟังข้อมูลในทุกเซสชั่นได้ ไม่ว่าผู้เล่นฝั่งป้องกันจะใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดรูปแบบใดก็ตาม หากพิจารณาโครงข่ายรูปที่ 4.7 จะเห็นว่าการจัดเส้นทางเพื่อใช้ส่งข้อมูลฝั่งขาขึ้นไม่ว่าจะเป็นรูปแบบใดจะต้องใช้จุดเชื่อมต่อผ่านที่ 2, 4, 6, 8 เพื่อส่งต่อข้อมูลเข้าสู่เกตเวย์เสมอ และจุดเชื่อมต่อผ่านเหล่านี้ต้องส่งข้อมูลผ่านตัวกลางไร้สายอีกด้วย ดังนั้นหากมีพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีสามารถดักฟังข้อมูลจากตัวกลางไร้สายของจุดเชื่อมต่อ 2, 4, 6, 8 ได้พร้อมกันแล้ว จะทำให้ผู้เล่นฝั่งโจมตีดักฟังข้อมูลได้ทุกเซสชั่น และจากผลการทดสอบพื้นที่ดังกล่าวนั้นคือ พื้นที่บริเวณตรงกลางของโครงข่ายดังแสดงในรูปที่ 4.8

กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงได้ค่า $ESS = 2$ หมายความว่า เมื่อผู้เล่นฝั่งป้องกันใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดแล้วจะได้เซสชั่นที่ไม่ถูกดักฟังข้อมูลจำนวน 2 เซสชั่น โดยผลการทดสอบการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดและพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีเลือกใช้ในการดักฟังแสดงดังรูปที่ 4.9 จะพบว่าพื้นที่ที่ผู้เล่นฝั่งโจมตีใช้ในการดักฟังข้อมูลคือ พื้นที่ที่สามารถดักฟังข้อมูลของเกตเวย์หนึ่งและสามารถดักฟังข้อมูลของจุดเชื่อมต่อข้างเคียงของอีกเกตเวย์หนึ่งพื้นที่ใดพื้นที่หนึ่ง ดังนั้นเมื่อโครงข่ายใช้การจัดเส้นทางที่เหมาะสมที่สุดดังแสดงในรูปที่ 4.9 แล้วจะได้เซสชั่นที่ปลอดภัยจากการถูกดักฟังของ 2 เซสชั่น นั่นคือ เซสชั่นของจุดเชื่อมต่อข้างเคียงของเกตเวย์ที่ไม่ถูกดักฟังนั่นเอง ยกตัวอย่าง

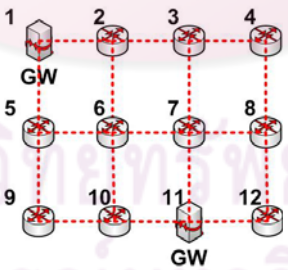
เช่น ผู้เล่นฝั่งโจมตีเลือกพื้นที่ที่ 1 ซึ่งอยู่ในพื้นที่ครอบคลุมของเกตเวย์ 9 และจุดเชื่อมต่อผ่าน 2, 4 โดย 2 เซสชั่นที่ไม่ถูกดักฟังข้อมูล คือ เซสชั่นของจุดเชื่อมต่อผ่าน 2, 4 เพราะฝั่งขาลงจุดเชื่อมต่อผ่าน 2, 4 ไม่ได้ส่งต่อข้อมูลของตนเองผ่านตัวกลางไร้สายออกมา เป็นต้น



รูปที่ 4.10: รูปแบบการรับส่งข้อมูลและพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีเลือกใช้ในการส่งสัญญาณรบกวนโนดในโครงข่ายแบบตารางขนาด 9 โนด

กรณีการส่งสัญญาณรบกวนซึ่งได้ค่า $ESS = 0$ หมายถึงผู้เล่นฝั่งโจมตีสามารถส่งสัญญาณรบกวนโจมตีทุกเซสชั่นในโครงข่ายนี้ได้ เนื่องจากผู้เล่นฝั่งโจมตีมีพื้นที่ที่สามารถโจมตีจุดเชื่อมต่อผ่าน 2, 4, 6, 8 ทำให้จุดเชื่อมต่อผ่านเหล่านี้ไม่สามารถรับและส่งข้อมูลได้ ซึ่งจากผลการทดสอบพื้นที่ดังกล่าวมี 9 พื้นที่ ดังรูปที่ 4.10

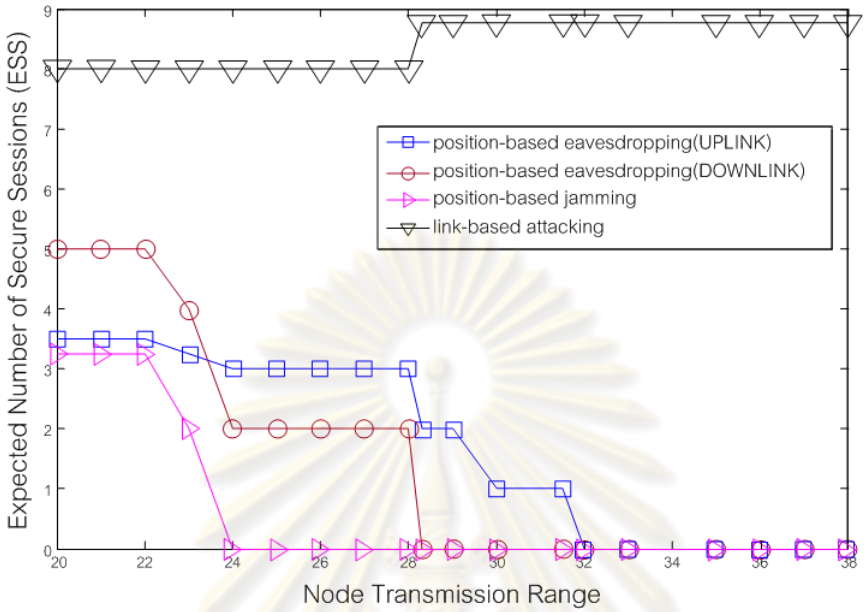
4.3 ผลกระทบของการเพิ่มรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่าย



รูปที่ 4.11: โครงข่ายแบบตารางขนาด 12 โนดที่ใช้ศึกษาผลกระทบของการเพิ่มรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่าย

การทดสอบในหัวข้อนี้ เป็นการศึกษาถึงผลกระทบเมื่อโนดในโครงข่ายไร้สายแบบเมช มีรัศมีการส่งสัญญาณไร้สายเพิ่มขึ้น รวมถึงศึกษากรณีที่ผู้เล่นฝั่งโจมตีส่งสัญญาณรบกวนด้วยรัศมีค่าต่าง ๆ โดยโครงข่ายที่นำมาใช้ทดสอบเป็นโครงข่ายแบบตารางซึ่งมีโนดที่ 1 และ 11 เป็นเกตเวย์ดังแสดงในรูปที่ 4.11 โนดที่เหลือทั้งหมดจำนวน 10 โนดเป็นจุดเชื่อมต่อผ่าน กำหนดให้ระยะห่างระหว่างโนดคือ 20 หน่วยทั้งในแนวแกนตั้งและแนวแกนนอน โดยที่โนดทุกโนดมีรัศมีการส่งสัญญาณไร้สายเท่ากันเริ่มต้นจาก 20 จนถึง 38 หน่วย กรณีการส่งสัญญาณรบกวนกำหนดให้ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเพิ่มขึ้นใน

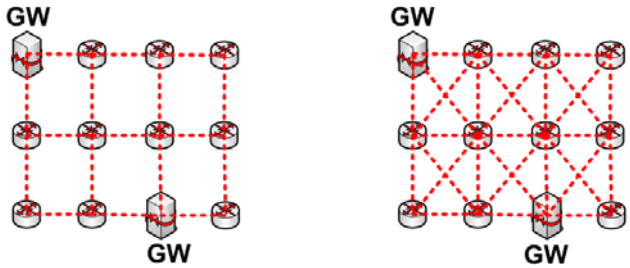
ลักษณะเดียวกันกับการเพิ่มรัศมีการส่งสัญญาณไร้สายของโนดคือเริ่มต้นจาก 20 จนถึง 38 หน่วย ผลการทดสอบที่ได้มีดังนี้



รูปที่ 4.12: ผลกระทบของการเพิ่มรัศมีในการส่งสัญญาณไร้สายของโนดในโครงข่าย

จากผลการทดสอบรูปที่ 4.12 พบว่าเมื่อทุกโนดมีรัศมีการส่งสัญญาณไร้สายเพิ่มขึ้น แนวโน้มของค่า ESS ซึ่งวิเคราะห์ด้วยระเบียบวิธีที่นำเสนอทั้ง 3 กรณี คือ การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง และการส่งสัญญาณรบกวนมีค่าลดลงจนกระทั่งมีค่าเท่ากับศูนย์ เหตุผลที่เป็นเช่นนั้นเนื่องจากการเพิ่มขึ้นของรัศมีการส่งสัญญาณไร้สายของทุกโนดทำให้ผู้เล่นฝั่งโจมตีมีพื้นที่ที่สามารถดักฟังข้อมูลได้หลายคู่สื่อสารมากขึ้น รวมทั้งกรณีการส่งสัญญาณรบกวนที่ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเพิ่มขึ้น จะทำให้ผู้เล่นฝั่งโจมตีสามารถส่งสัญญาณรบกวนได้หลายคู่สื่อสารมากขึ้นเช่นกัน นอกจากนี้การเปลี่ยนแปลงของค่า ESS ในแต่ละกรณีของการโจมตียังบ่งบอกได้ถึง พื้นที่โจมตีที่เปลี่ยนแปลงไปมีผลต่อการเลือกพื้นที่ของผู้เล่นฝั่งโจมตีซึ่งสามารถโจมตีการสื่อสารของคู่โนดได้มากขึ้น

ในขณะที่ระเบียบวิธีที่ใช้ลักษณะการโจมตีที่ข่ายเชื่อมโยงจากผลการทดสอบจะเห็นว่า ระเบียบวิธีดังกล่าวไม่สามารถวิเคราะห์กรณีใดที่มีการระบุรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่าย หรือมีการระบุรัศมีในการส่งสัญญาณรบกวนของผู้เล่นฝั่งโจมตีได้ เนื่องจากลักษณะการโจมตีที่ข่ายเชื่อมโยงผู้เล่นฝั่งโจมตีมีสมมุติฐานเป็นการเลือกข่ายเชื่อมโยงหนึ่งเพื่อโจมตี ดังนั้นไม่ว่าจะมีการระบุรัศมีการส่งสัญญาณไร้สายเป็นค่าใด ระเบียบวิธีที่ใช้ลักษณะการโจมตีที่ข่ายเชื่อมโยงจะให้ค่า ESS ที่คงที่ไม่มีการเปลี่ยนแปลงจนถึงจุดที่โครงข่ายมีรัศมีการส่งสัญญาณไร้สายของโนดเท่ากับ 28.3 ซึ่งเป็นจุดที่การต่อถึงกันของโนดที่เปลี่ยนไปดังแสดงในรูปที่ 4.13 การที่โครงข่ายมีจำนวนข่ายเชื่อมโยงมากขึ้นเนื่องจากการเพิ่มรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่าย ทำให้ผู้เล่นฝั่งป้องกันมีรูปแบบการจัดเส้นทางที่หลากหลายมากขึ้นในขณะที่ผู้เล่นฝั่งโจมตียังคงเลือกโจมตีข่ายเชื่อมโยงได้เพียงข่ายเชื่อมโยงเดียวเช่นเดิม ดังนั้นหากผู้



ก. การต่อถึงกันของโนดในโครงข่าย เมื่อรัศมีการส่งสัญญาณไร้สายมีค่าตั้งแต่ 20 จนถึง 28 หน่วย

ข. การต่อถึงกันของโนดในโครงข่าย เมื่อรัศมีการส่งสัญญาณไร้สายมีค่าตั้งแต่ 28.3 จนถึง 38 หน่วย

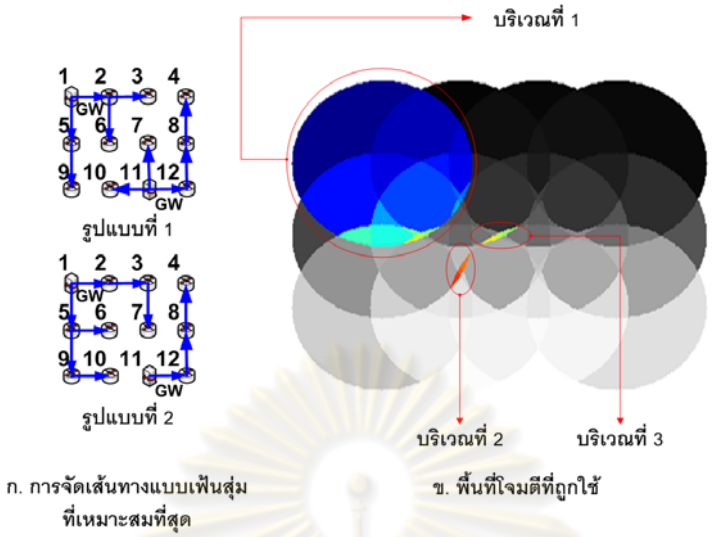
รูปที่ 4.13: การต่อถึงกันที่เปลี่ยนไปเมื่อโนดในโครงข่ายไร้สายแบบเมชมีรัศมีการส่งสัญญาณที่เพิ่มขึ้น

เล่นฝั่งป้องกันวิเคราะห์ปัญหาการดักฟังข้อมูลและการส่งสัญญาณรบกวน ด้วยระเบียบวิธีที่ใช้ลักษณะการโจมตีที่เชื่อมโยงแล้ว จะวิเคราะห์ได้ว่า เมื่อโนดในโครงข่ายมีรัศมีการส่งสัญญาณไร้สายเพิ่มขึ้น ผู้เล่นฝั่งโจมตีจะดักฟังข้อมูลได้น้อยลงและโครงข่ายจะมีระดับความปลอดภัยที่สูงขึ้น หรือกรณีการส่งสัญญาณรบกวนหากผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเพิ่มขึ้น โครงข่ายจะมีระดับความปลอดภัยที่สูงขึ้น ซึ่งแนวโน้มดังกล่าวไม่สอดคล้องกับสภาพของโครงข่ายไร้สายอย่างสิ้นเชิง

นอกจากนั้นผลการทดสอบเมื่อวิเคราะห์ด้วยระเบียบวิธีที่นำเสนอยังแสดงให้เห็นถึงผลที่แตกต่างกันจากการโจมตีทั้ง 3 กรณีคือ การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงและการส่งสัญญาณรบกวนได้ชัดเจนมากขึ้น โดยจะเห็นว่าค่า ESS กรณีการดักฟังข้อมูล ณ รัศมีการส่งสัญญาณไร้สายของโนดบางค่าจะให้ค่า ESS กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นมากกว่ากรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง แต่ ณ รัศมีการส่งสัญญาณไร้สายบางค่าให้ค่า ESS ที่น้อยกว่า ทั้งนี้ขึ้นอยู่กับตำแหน่งของเกตเวย์และจุดเชื่อมต่อผ่านรวมถึงรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่ายที่นำมาทดสอบ จึงสรุปได้ว่าไม่จำเป็นเสมอไปที่การดักฟังข้อมูลในทิศทางใดทิศทางหนึ่งจะมีความรุนแรงมากกว่าหรือน้อยกว่ากัน นอกจากนั้นผลการทดสอบยังแสดงให้เห็นถึงกรณีผลกระทบจากการส่งสัญญาณรบกวนเมื่อเปรียบเทียบกับกรณีการดักฟังข้อมูลทั้งสองทิศทางแล้ว จะมีความรุนแรงที่สุดเสมอในทุกกรณี เนื่องจากการส่งสัญญาณรบกวน ผู้เล่นฝั่งโจมตีสามารถรบกวนทั้งภาครับและภาคส่งของโนดที่อยู่ในรัศมีการรบกวน ขณะที่การดักฟังข้อมูล ผู้เล่นฝั่งโจมตีจะสามารถดักฟังข้อมูลได้เมื่อโนดที่ถูกดักฟังอยู่นั้นส่งข้อมูลออกมาผ่านตัวกลางไร้สายหรืออาจมองได้ว่าการดักฟังข้อมูลเป็นโจมตีได้เฉพาะภาคส่งของโนดในโครงข่ายเท่านั้น

เพื่อความชัดเจนในการเปรียบเทียบผลกระทบจากการโจมตีที่แตกต่างกันข้างต้น วิทยานิพนธ์นี้จึงขอยกตัวอย่างกรณีที่รัศมีการส่งสัญญาณไร้สายของโนดมีค่าเท่ากับ 23 หน่วยและกรณีที่ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับ 23 หน่วยดังนี้

กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงซึ่งผู้เล่นฝั่งโจมตีจะเลือกพื้นที่โจมตีของเกตเวย์ใดเกตเวย์หนึ่งเพื่อใช้ในการดักฟังข้อมูล และในกรณีที่รัศมีการส่งสัญญาณไร้สายของโนดมีค่าเท่ากับ 23 นี้ ผู้เล่นฝั่งโจมตีมีพื้นที่ซึ่งสามารถดักฟังข้อมูลจากโนดที่ 11 ที่เป็นเกตเวย์ ขณะเดียวกันผู้เล่นฝั่งโจมตียังสามารถ



รูปที่ 4.14: การป้องกันด้วยการจัดเส้นทางแบบเฟ้นสุ่มและพื้นที่โจมตีที่ถูกเลือกใช้ในการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง ณ รัศมีการส่งสัญญาณเท่ากับ 23 หน่วย

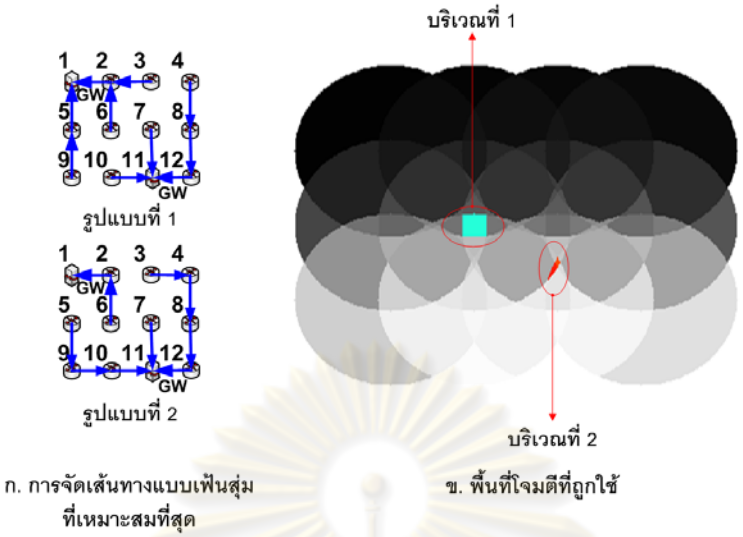
ดักฟังโนดข้างเคียงของอีกเกตเวย์หนึ่ง คือ โนดที่ 1 ได้อีกหนึ่งโนดพร้อม ๆ กันอีกด้วย ดังแสดงในรูปที่ 4.14 พื้นที่ดังกล่าว คือ บริเวณการโจมตีที่ 2 หรือ 3 ดังนั้นผู้เล่นฝั่งป้องกันจำเป็นต้องใช้การจัดเส้นทางแบบเฟ้นสุ่มระหว่างการจัดเส้นทางรูปแบบที่ 1 และ 2 เพื่อเพิ่มค่า ESS ให้กับโครงข่าย ด้วยวิธีป้องกันดังกล่าวทำให้ผู้เล่นฝั่งโจมตีเลือกบริเวณการโจมตี 3 บริเวณ ดังแสดงในรูปที่ 4.14 โดยค่าความน่าจะเป็นในการเลือกแผนการเล่นของผู้เล่นทั้งสองฝั่งสามารถคำนวณได้จากการสร้างตารางผลได้ผลเสีย ดังแสดงในรูปที่ 4.15

		ฝั่งโจมตี	
ฝั่งป้องกัน	บริเวณที่ 1	บริเวณที่ 2	บริเวณที่ 3
รูปแบบที่ 1	5	4	3
รูปแบบที่ 2	3	4	5

รูปที่ 4.15: ตารางผลได้ผลเสียกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง ณ รัศมีการส่งสัญญาณเท่ากับ 23 หน่วย

เมื่อพิจารณาตารางผลได้ผลเสีย การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุด คือ การเลือกใช้การจัดเส้นทางในรูปแบบที่ 1 ด้วยค่าความน่าจะเป็นเท่ากับ 0.5 และการเลือกใช้การจัดเส้นทางในรูปแบบที่ 2 ด้วยความน่าจะเป็นเท่ากับ 0.5 และด้วยการจัดเส้นทางแบบเฟ้นสุ่มที่ได้นี้ทำให้ผู้เล่นฝั่งโจมตีไม่ว่าจะเลือกบริเวณใดก็จะให้ค่า ESS เท่ากับ 4 เสมอ

ในขณะที่การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น ผู้เล่นฝั่งโจมตีจะมุ่งดักฟังข้อมูลจากจุดเชื่อมต่อผ่านที่เป็นโนดข้างเคียงของเกตเวย์ รวมทั้งดักฟังข้อมูลจากจุดเชื่อมต่อผ่านอื่นที่เหลือให้ได้มากที่สุด จากผลการทดสอบพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีเลือกเป็นพื้นที่ตรงกลางของโครงข่าย หรือ บริเวณที่ 1 ดังแสดง



รูปที่ 4.16: การป้องกันด้วยการจัดเส้นทางแบบเฟ้นสุ่มและพื้นที่โจมตีที่ถูกเลือกใช้ในการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น ณ รัศมีการส่งสัญญาณเท่ากับ 23 หน่วย

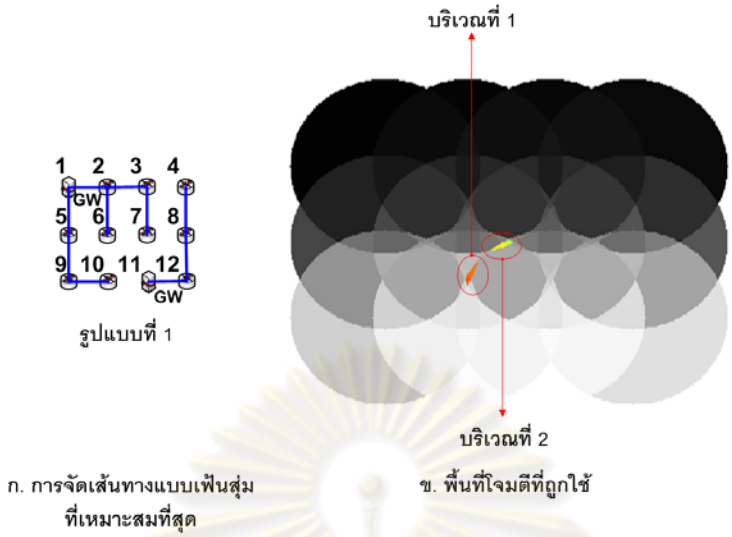
ในรูปที่ 4.16 โดยบริเวณดังกล่าวผู้เล่นฝั่งโจมตีสามารถดักฟังข้อมูลจากโนดที่ 2 และ 5 ซึ่งเป็นโนดข้างเคียงของโนดที่ 1 ขณะเดียวกันผู้เล่นฝั่งโจมตียังสามารถดักฟังโนดที่ 6, 7, 10 ซึ่งส่งผลให้โนดที่ 9 ถูกดักฟังไปด้วยเนื่องจากโนดที่ 9 ต้องใช้โนดที่ 5 หรือ 10 เพื่อใช้ส่งต่อข้อมูล อีกบริเวณการโจมตีหนึ่งที่ผู้เล่นฝั่งโจมตีเลือกใช้ คือ บริเวณที่ 2 ซึ่งผู้โจมตีสามารถดักฟังข้อมูลจากโนดที่ 7, 10, 12 ซึ่งเป็นโนดข้างเคียงของโนดที่ 11 ได้ ดังนั้นการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดจะได้ดังรูปที่ 4.16

		ฝั่งโจมตี	
ฝั่งป้องกัน		บริเวณที่ 1	บริเวณที่ 2
	รูปแบบที่ 1	3	4
	รูปแบบที่ 2	4	1

รูปที่ 4.17: ตารางผลได้ผลเสียกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง ณ รัศมีการส่งสัญญาณเท่ากับ 23 หน่วย

เมื่อการพิจารณาตารางผลได้ผลเสีย การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุด คือ การเลือกใช้การจัดเส้นทางในรูปแบบที่ 1 ด้วยค่าความน่าจะเป็นเท่ากับ 0.75 และการเลือกใช้การจัดเส้นทางในรูปแบบที่ 2 ด้วยความน่าจะเป็นเท่ากับ 0.25 ด้วยการจัดเส้นทางแบบเฟ้นสุ่มที่ได้จะทำให้ผู้เล่นฝั่งโจมตีไม่ว่าจะเลือกบริเวณใดก็จะให้ค่า ESS เท่ากับ 3.25 เสมอ

การโจมตีโดยการส่งสัญญาณรบกวนจากรูปที่ 4.18 ผู้เล่นฝั่งโจมตีเลือกพื้นที่โจมตีที่สามารถส่งสัญญาณรบกวนโนดที่ 11 พร้อมกับส่งสัญญาณรบกวนโนดที่เหลือที่เชื่อมต่อกับอีกเกตเวย์หนึ่ง คือ โนดที่ 1 ได้มากที่สุด ดังนั้นการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดเพื่อป้องกันการส่งสัญญาณรบกวนในกรณีตัวอย่างนี้จะเป็นดังรูปที่ 4.18



รูปที่ 4.18: การป้องกันด้วยการจัดเส้นทางแบบเฟ้นสุ่มและพื้นที่โจมตีที่ถูกเลือกใช้ในการส่งสัญญาณรบกวนด้วยรัศมีเท่ากับ 23 หน่วย

		ฝั่งโจมตี	
		บริเวณที่ 1	บริเวณที่ 2
ฝั่งป้องกัน	รูปแบบที่ 1	2	2

รูปที่ 4.19: ตารางผลได้ผลเสียกรณีการส่งสัญญาณรบกวนโดยผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับ 23 หน่วย

เมื่อพิจารณาตารางผลได้ผลเสียจะเห็นว่าไม่ว่าผู้ฝั่งโจมตีเลือกบริเวณใดใน 2 บริเวณดังรูป 4.18 เพื่อส่งสัญญาณรบกวนจะให้ค่า ESS เท่ากับ 2 เสมอ

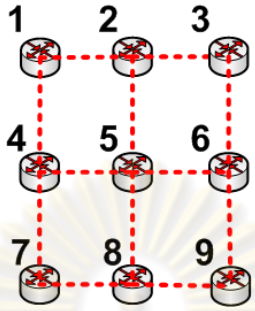
การโจมตีทั้งสามแบบในกรณีตัวอย่าง เมื่อโครงข่ายมีรัศมีการส่งสัญญาณไร้สายของโนดมีค่าเท่ากับ 23 หน่วย และกรณีการส่งสัญญาณรบกวนที่ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับ 23 หน่วยนี้ จะเห็นถึงผลกระทบที่แตกต่างกันอย่างชัดเจน ซึ่งส่งผลให้โครงข่ายจำเป็นต้องใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดแตกต่างกัน เพื่อให้เหมาะสมกับป้องกันการโจมตีแต่ละแบบในแต่ละทิศทาง รวมทั้งการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดในกรณีดังกล่าว ยังแสดงให้เห็นถึงความจำเป็นที่ผู้เล่นฝั่งป้องกันจะต้องใช้รูปแบบการจัดเส้นทางในลักษณะเฟ้นสุ่ม นอกจากนั้นการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดยังไม่ใช่รูปแบบที่จุดเชื่อมต่อผ่านจะเชื่อมกับเกตเวย์ที่อยู่ใกล้ที่สุดอีกด้วย

4.4 ผลกระทบของการเพิ่มจำนวนเกตเวย์ให้กับโครงข่าย

การทดสอบในหัวข้อนี้เป็นการศึกษาผลกระทบจากการโจมตีเมื่อมีการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายไร้สายแบบเมช โดยวิทยานิพนธ์ฉบับนี้ได้แบ่งการทดสอบออกเป็นสองส่วน ในส่วนแรกจะเป็นการศึกษาผลกระทบจากการโจมตี โดยการเปรียบเทียบรูปแบบการเพิ่มจำนวนเกตเวย์ที่แตกต่างกัน 2 รูปแบบ ในส่วนที่สองจะเป็นการวิเคราะห์และเปรียบเทียบระดับความปลอดภัยกับความคุ้มค่าในการเพิ่ม

จำนวนเกตเวย์ ซึ่งวิทยานิพนธ์นี้ได้ทำการทดสอบกับโครงข่ายที่ได้จากการสุ่ม

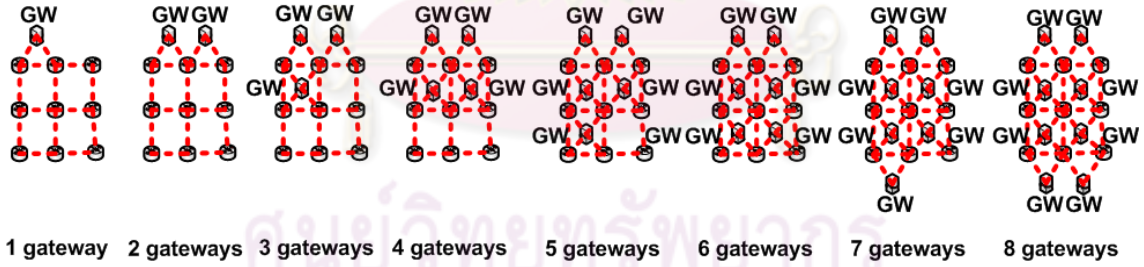
4.4.1 การทดสอบผลกระทบของการเพิ่มจำนวนเกตเวย์ในรูปแบบที่แตกต่างกัน



รูปที่ 4.20: โครงข่ายแบบตารางซึ่งประกอบไปด้วยจุดเชื่อมต่อผ่าน 9 โนด

การทดสอบในส่วนนี้เป็นการศึกษาผลกระทบของการเพิ่มจำนวนเกตเวย์ โดยเปรียบเทียบรูปแบบการเพิ่มจำนวนเกตเวย์ที่แตกต่างกัน 2 รูปแบบ โครงข่ายที่นำมาใช้ทดสอบประกอบไปด้วยจุดเชื่อมต่อผ่าน 9 โนดต่อถึงกันแบบตารางดังแสดงในรูปที่ 4.20 โดยจุดเชื่อมต่อผ่านอยู่ห่างกัน 20 หน่วย ทั้งในแนวแกนตั้งและแนวแกนนอน รัศมีในการส่งสัญญาณไร้สายของทุกโนด คือ 25 หน่วย รวมทั้งกรณีการโจมตี คือ การส่งสัญญาณรบกวน กำหนดให้ผู้เล่นฝั่งโจมตีมีรัศมีในการส่งสัญญาณรบกวนเท่ากับ 25 หน่วย

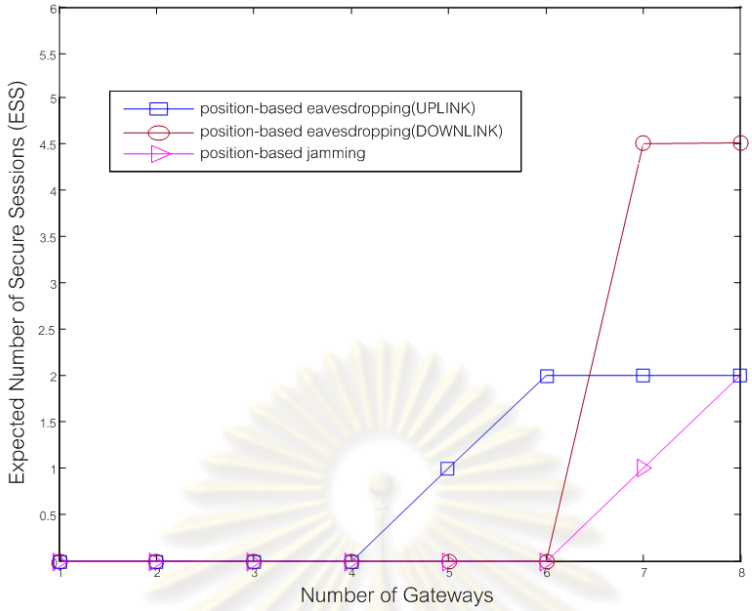
โดยรูปแบบการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายรูปแบบแรกที่ใช้ศึกษาแสดงดังรูปที่ 4.21 และมีผลการทดสอบแสดงดังรูปที่ 4.22



รูปที่ 4.21: การเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายแบบตารางขนาด 9 โนดรูปแบบที่หนึ่ง

จากผลการทดสอบที่ 4.22 จะเห็นว่าการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายส่งผลให้แนวโน้มของค่า ESS ทั้งสามกรณี คือ การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง และการส่งสัญญาณรบกวนมีค่าสูงขึ้น แต่ค่า ESS ที่สูงขึ้นนั้นมีความแตกต่างกันซึ่งสามารถอธิบายได้ตามชนิดของการโจมตีและทิศทางการส่งข้อมูลดังนี้

กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง ณ จุดที่ค่า ESS มีค่าเท่ากับศูนย์นั้น โครงข่ายมีพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีสามารถเลือกดักฟังข้อมูลจากเกตเวย์ทุกโนดได้พร้อมกัน จนกระทั่ง ณ จุดที่โครงข่ายมีเกตเวย์ 7 โนดซึ่งผู้เล่นฝั่งโจมตีไม่สามารถดักฟังข้อมูลจากเกตเวย์ทุกโนด ส่งผลให้ค่า ESS ที่ได้มีค่าสูงขึ้น หลังจากนั้นค่า ESS มีค่าคงที่ เหตุผลเนื่องมาจากการเพิ่มเกตเวย์โนดที่ 8 ในตำแหน่งดังกล่าวเป็น



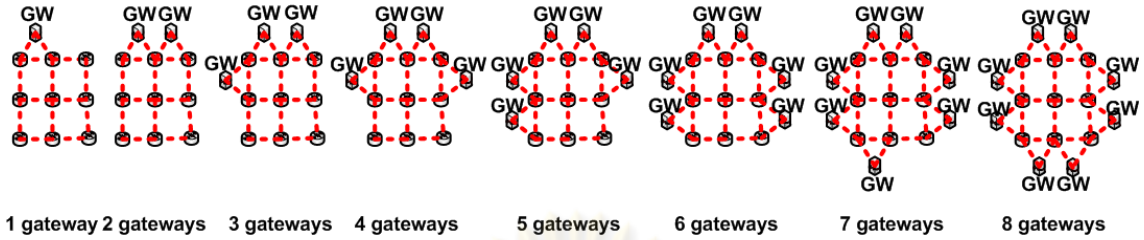
รูปที่ 4.22: ผลการทดสอบกรณีการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายแบบตารางขนาด 9 โนดรูปแบบที่หนึ่ง

การเพิ่มทางเลือกให้กับจุดเชื่อมต่อผ่านที่สามารถเชื่อมต่อกับเกตเวย์ได้อย่างปลอดภัยอยู่แล้ว ทำให้การเพิ่มจำนวนเกตเวย์ ณ จุดดังกล่าวในกรณีตัวอย่างนี้ไม่สามารถเพิ่มระดับความปลอดภัยให้แก่โครงข่ายได้

ขณะที่กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น ณ จุดที่ค่า ESS มีค่าเท่ากับศูนย์ โครงข่ายมีพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีสามารถเลือกดักฟังข้อมูลจากโนดข้างเคียงของเกตเวย์ได้ทั้งหมดพร้อมกัน จนกระทั่ง ณ จุดที่โครงข่ายมีเกตเวย์ 5 โนดซึ่งผู้เล่นฝั่งโจมตีไม่สามารถดักฟังข้อมูลจากโนดข้างเคียงของเกตเวย์ได้ทั้งหมดพร้อมกัน ส่งผลให้ค่า ESS สูงขึ้น นอกจากนั้นค่า ESS ในกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นยังมีแนวโน้มสูงขึ้นจากเดิมได้ โดย ณ จุดที่โครงข่ายมีเกตเวย์ 6 โนด การเพิ่มเกตเวย์โนดที่ 6 ที่ตำแหน่งดังกล่าวนั้นเป็นการเพิ่มทางเลือกให้กับจุดเชื่อมต่อผ่านสามารถเชื่อมต่อกับเกตเวย์ได้โดยไม่จำเป็นต้องส่งต่อข้อมูลของตนเองผ่านจุดเชื่อมต่อผ่านอื่น การเชื่อมต่อกับเกตเวย์ภายในช่วงเชื่อมต่อเดียว ทำให้จุดเชื่อมต่อผ่านทั้งหมดในโครงข่ายสามารถกระจายเส้นทางในการส่งข้อมูลไปที่เกตเวย์ได้ดียิ่งขึ้น และส่งผลต่อระดับความปลอดภัยของโครงข่ายที่สูงขึ้นได้

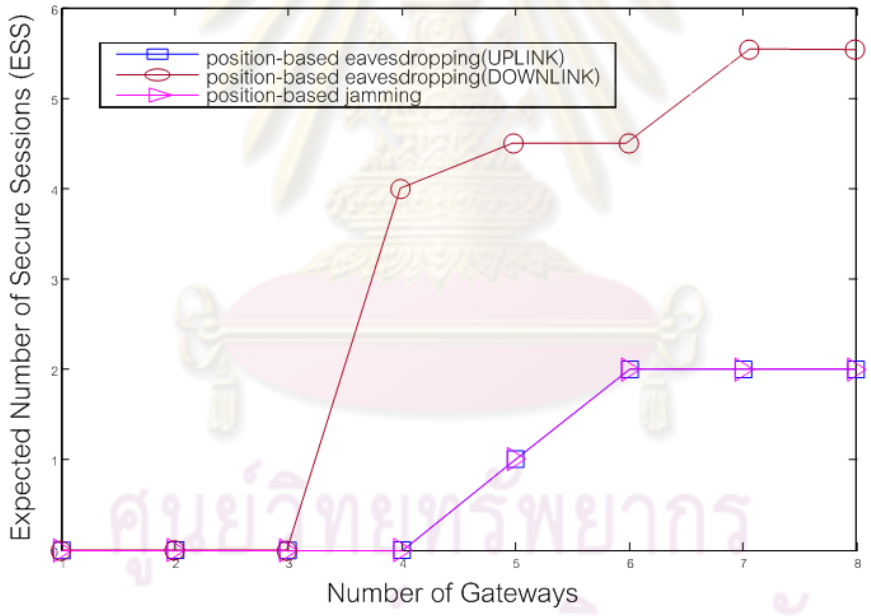
กรณีการส่งสัญญาณรบกวนจุดที่ค่า ESS มีค่าเท่ากับศูนย์นั้นโครงข่ายมีพื้นที่โจมตีที่ผู้เล่นฝั่งโจมตีสามารถส่งสัญญาณรบกวน ทำให้เกตเวย์กับจุดเชื่อมต่อผ่านทั้งหมดในโครงข่ายไม่สามารถรับส่งข้อมูลระหว่างกันได้ จนกระทั่ง ณ จุดที่โครงข่ายมีเกตเวย์ 7 โนด ซึ่งเป็นจุดที่ผู้เล่นฝั่งโจมตีไม่สามารถส่งสัญญาณรบกวนเกตเวย์ได้ทุกโนดพร้อมกันทำให้ ณ จุดดังกล่าวให้ค่า ESS สูงขึ้น โดยผู้เล่นฝั่งโจมตีหันมาส่งสัญญาณรบกวนจุดเชื่อมต่อผ่านและเกตเวย์ที่สำคัญให้ได้มากที่สุดแทน จากนั้น ณ จุดที่โครงข่ายมีเกตเวย์ 8 โนด การเพิ่มเกตเวย์โนดที่ 8 ที่ตำแหน่งดังกล่าวนั้นสามารถเพิ่มค่า ESS ให้กับโครงข่ายได้เนื่องจากตำแหน่งของเกตเวย์ที่เพิ่มเข้าไปเป็นการเพิ่มทางเลือกให้กับจุดเชื่อมต่อผ่านสามารถเชื่อมต่อกับเกตเวย์ได้ในช่วงเชื่อมต่อเดียว

เพื่อเปรียบเทียบให้เห็นถึงค่า ESS เมื่อมีการเพิ่มเกตเวย์ให้กับโครงข่ายในรูปแบบที่แตกต่างออกไป วิทยานิพนธ์นี้จึงได้ศึกษารูปแบบการเพิ่มเกตเวย์ให้กับโครงข่ายในรูปแบบที่สองดังรูปที่ 4.23



รูปที่ 4.23: การเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายแบบตารางขนาด 9 โนดรูปแบบที่สอง

หากเปรียบเทียบรูปแบบการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายรูปแบบที่สอง กับรูปแบบการเพิ่มจำนวนเกตเวย์ให้กับรูปแบบที่หนึ่ง จะเห็นว่ารูปแบบที่สองมีลักษณะการวางเกตเวย์ให้อยู่ห่างกันมากกว่า เพื่อเป็นการลดการซ้อนทับกันของพื้นที่โจมตีของเกตเวย์ ส่งผลให้โอกาสที่ผู้เล่นฝั่งโจมตีจะโจมตีเกตเวย์ทั้งหมดในโครงข่ายได้พร้อมกันลดลง ซึ่งผลการทดสอบการเพิ่มเกตเวย์ในรูปแบบที่สองแสดงดังรูปที่ 4.24



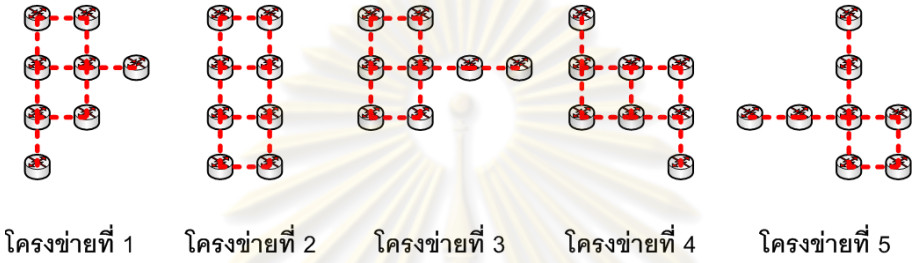
รูปที่ 4.24: ผลการทดสอบกรณีการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายแบบตารางขนาด 9 โนดรูปแบบที่สอง

จากผลการทดสอบจะพบว่าแนวโน้มของค่า ESS ทั้งสามกรณีมีค่าสูงขึ้นตามจำนวนเกตเวย์ที่เพิ่มขึ้นเช่นเดียวกับผลการทดสอบการเพิ่มจำนวนเกตเวย์รูปแบบที่หนึ่ง แต่ด้วยการวางเกตเวย์ที่มีลักษณะกระจายตัวเพื่อลดการซ้อนทับกันของพื้นที่โจมตีของเกตเวย์ให้น้อยในรูปแบบที่สองนั้นส่งผลให้ค่า ESS ในกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงมีค่าสูงขึ้น รวมทั้งการเพิ่มเกตเวย์ในรูปแบบที่สองยังส่งผลให้กรณีการส่งสัญญาณรบกวนได้ค่า ESS ที่สูงขึ้นเช่นเดียวกันด้วย

ในขณะที่กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นได้ค่า ESS เหมือนกับกรณีการเพิ่มเกตเวย์ให้

กับโครงข่ายรูปแบบที่หนึ่ง เหตุผลเนื่องจากการเพิ่มเกตเวย์ให้กับโครงข่ายในรูปแบบที่สองถึงแม้ว่าจะมีลักษณะกระจายตัวของเกตเวย์มากกว่าในรูปแบบที่หนึ่งซึ่งจะมีผลต่อการเลือกเส้นทางให้มีลักษณะการกระจายโหลดที่ดีมากขึ้น แต่โครงข่ายที่นำมาใช้ทดสอบเป็นโครงข่ายขนาดเล็ก ซึ่งจุดเชื่อมต่อผ่านถูกวางไว้อย่างหนาแน่น ทำให้การจัดเส้นทางเพื่อกระจายโหลดของจุดเชื่อมต่อผ่านในกรณีนี้ไม่สามารถเพิ่มระดับความปลอดภัยให้กับโครงข่ายได้

4.4.2 การทดสอบผลกระทบของการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายที่ได้จากการสุ่ม

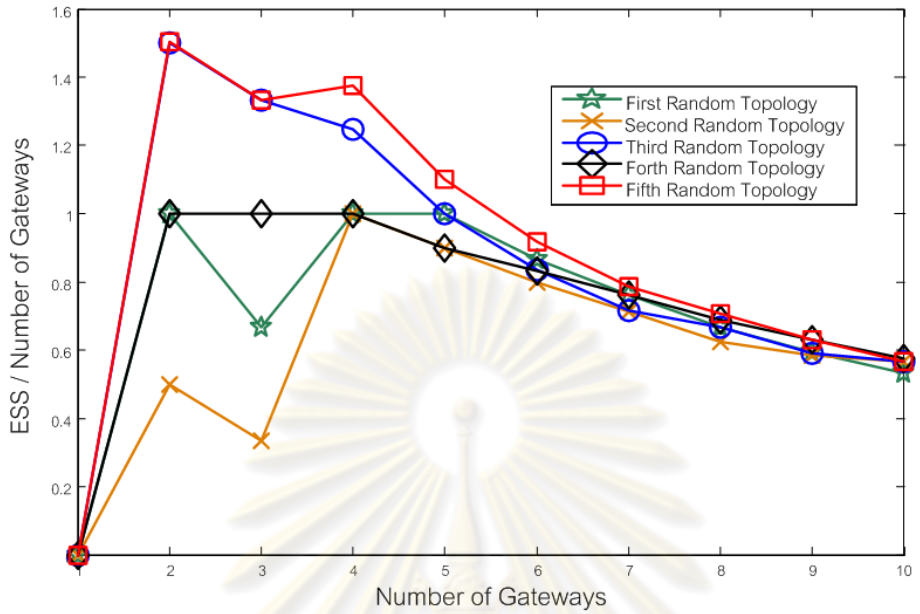


รูปที่ 4.25: การต่อถึงกันของจุดเชื่อมต่อผ่านที่ได้จากการสุ่ม

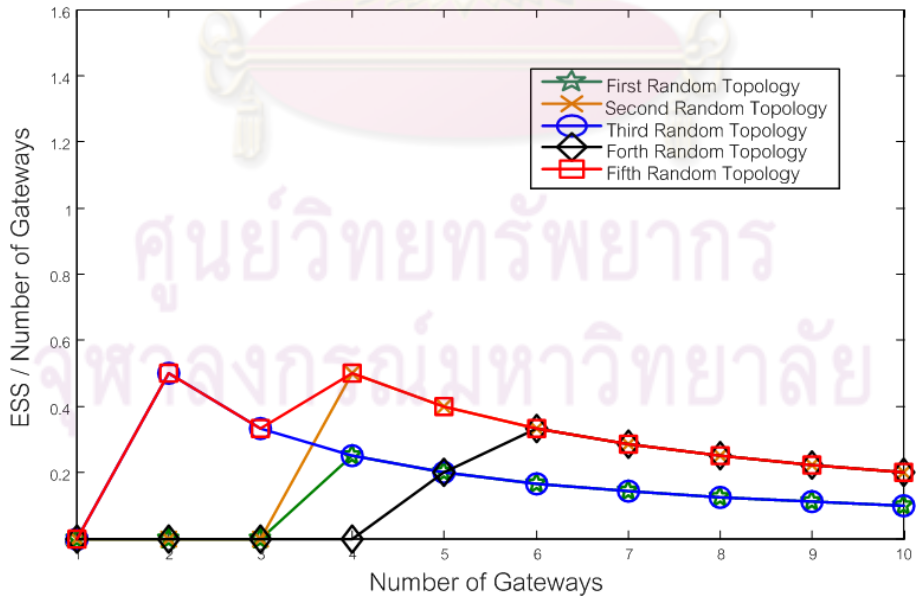
จากการทดสอบข้างต้นซึ่งศึกษาถึง ผลกระทบของการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายในรูปแบบที่แตกต่างกันจะเห็นว่า เมื่อโครงข่ายมีจำนวนเกตเวย์มากขึ้น ค่า ESS ที่ได้จะมีแนวโน้มสูงขึ้นจนกระทั่งคงที่ที่ค่าหนึ่ง ซึ่งหมายความว่า การเพิ่มเกตเวย์ให้กับโครงข่ายจะสามารถช่วยเพิ่มระดับความปลอดภัยให้กับโครงข่ายไร้สายแบบเมชได้จนถึงค่าหนึ่งเท่านั้น หลังจากนั้นการเพิ่มเกตเวย์ต่อไปอาจไม่คุ้มค่ากับต้นทุนในการติดตั้งเกตเวย์เพิ่มให้กับโครงข่าย จึงเป็นที่มาของการทดสอบส่วนที่สองซึ่งประยุกต์ใช้ระเบียบวิธีที่นำเสนอ เพื่อวิเคราะห์ประเด็นการเพิ่มระดับความปลอดภัยด้วยการเพิ่มเกตเวย์ให้กับโครงข่ายโดยเปรียบเทียบกับจำนวนเกตเวย์ที่เพิ่มขึ้น โครงข่ายไร้สายแบบเมชที่นำมาใช้ทดสอบ เป็นโครงข่ายที่ได้มาจากการสุ่มเลือกตำแหน่งของจุดเชื่อมต่อผ่านจำนวน 8 โนด โดยมีเงื่อนไขให้จุดเชื่อมต่อผ่านเหล่านี้มีข่ายเชื่อมโยงที่เชื่อมต่อถึงกันได้ทั้งหมด ดังแสดงในรูปที่ 4.25 จุดเชื่อมต่อผ่านมีระยะห่างระหว่างกันเท่ากับ 20 หน่วยทั้งในแนวแกนตั้งและแนวแกนนอน รวมทั้งกำหนดให้รัศมีการส่งสัญญาณไร้สายของทุกโนด และผู้เล่นฝั่งโจมตีกรณีการส่งสัญญาณรบกวนมีรัศมีในการส่งสัญญาณรบกวนเท่ากัน คือ 25 หน่วย ส่วนการเพิ่มเกตเวย์ให้กับโครงข่ายนั้น วิทยานิพนธ์ฉบับนี้ใช้เงื่อนไขให้การเพิ่มเกตเวย์จะพยายามให้เกตเวย์แต่ละโนดมีพื้นที่โจมตีซ้อนทับกันน้อยที่สุด ผลการทดสอบที่ได้มีดังนี้

จากผลการทดสอบกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง รูปที่ 4.26 ซึ่งแกน Y เป็นค่า ESS ต่อจำนวนเกตเวย์ในโครงข่าย จะเห็นว่า การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นมีแนวโน้มของค่า ESS ต่อจำนวนเกตเวย์สูงสุดอยู่ ณ จุดที่โครงข่ายมีจำนวนเกตเวย์ 2 และ 3 โนด และหลังจากนั้นแนวโน้มของค่า ESS ต่อจำนวนเกตเวย์มีค่าลดลง ซึ่งแสดงถึงการเพิ่มจำนวนเกตเวย์ต่อไปเพื่อเพิ่มระดับความปลอดภัยจะไม่คุ้มค่ากับต้นทุนในการติดตั้งเกตเวย์เพิ่มให้กับโครงข่าย

ขณะที่ผลการทดสอบกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น และกรณีการส่งสัญญาณรบกวนรูปที่ 4.27 พบว่า ESS ต่อจำนวนเกตเวย์มีค่าเท่ากันในทุกกรณีที่ทดสอบรวมถึงแนวโน้มที่เหมือนกัน โดย



รูปที่ 4.26: ผลกระทบของการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายที่ได้จากการสุ่มกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง



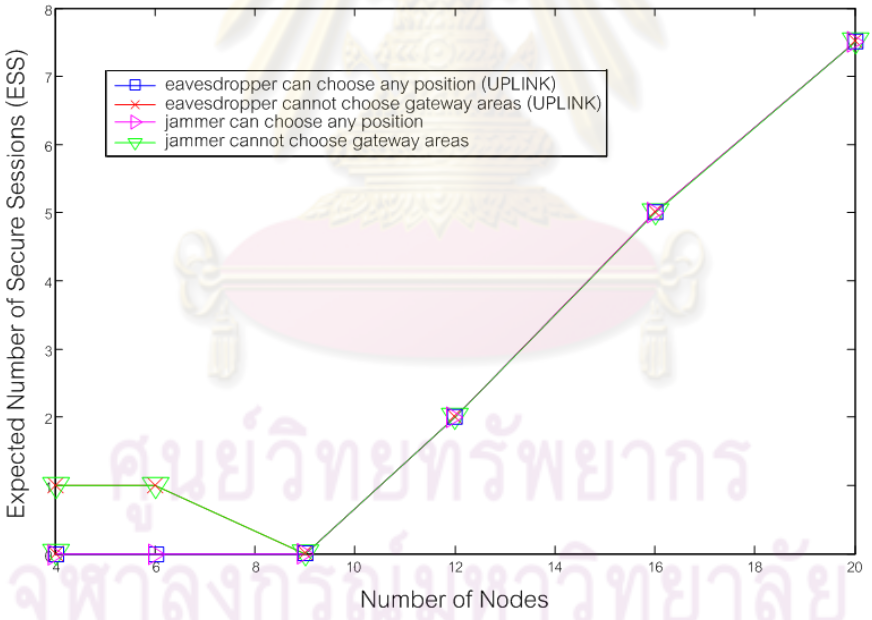
รูปที่ 4.27: ผลกระทบของการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายที่ได้จากการสุ่มกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและกรณีการส่งสัญญาณรบกวน

แนวโน้มของค่า ESS ต่อจำนวนเกตเวย์สูงสุดอยู่ ณ จุดที่โครงข่ายมีจำนวนเกตเวย์ 2 และ 3 โนดเช่นเดียวกับกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น แต่ค่า ESS ต่อจำนวนเกตเวย์มีค่าน้อยกว่า เนื่องจากการวางเกตเวย์ในการทดสอบส่วนนี้ เป็นการวางให้เกตเวย์มีพื้นที่โจมตีซ้อนทับกันน้อยที่สุด ซึ่งจะเอื้อต่อการเพิ่มระดับความปลอดภัยกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงมากกว่า

ดังนั้นจะเห็นว่าการเพิ่มระดับความปลอดภัยให้โครงข่ายด้วยการเพิ่มเกตเวย์ให้กับโครงข่ายสามารถทำได้ แต่โครงข่ายจะต้องคำนึงถึงความคุ้มค่าในการเพิ่มเกตเวย์ให้กับโครงข่าย ซึ่งประเด็นดังกล่าวสามารถวิเคราะห์ได้ด้วยระเบียบวิธีที่นำเสนอในวิทยานิพนธ์ฉบับนี้เช่นกัน

4.5 ผลกระทบจากการโจมตีกรณีที่ผู้เล่นฝั่งโจมตีไม่สามารถเลือกพื้นที่เพื่อโจมตีเกตเวย์

การทดสอบหัวข้อนี้เป็นการศึกษาผลกระทบจากการโจมตีสองแบบ ทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวนในกรณีที่ผู้เล่นฝั่งโจมตีไม่สามารถเลือกพื้นที่เพื่อโจมตีเกตเวย์ของโครงข่ายได้ โดยวิทยานิพนธ์ฉบับนี้ได้เปรียบเทียบผลกระทบจากการโจมตีดังกล่าวกับ กรณีที่ผู้เล่นฝั่งโจมตีสามารถเลือกพื้นที่โจมตีได้อย่างอิสระ ซึ่งได้ทำการทดสอบไปแล้วในหัวข้อที่ 4.2 กับโครงข่ายแบบตารางขนาดต่าง ๆ ดังแสดงในรูปที่ 4.5 ผลการทดสอบมีดังนี้

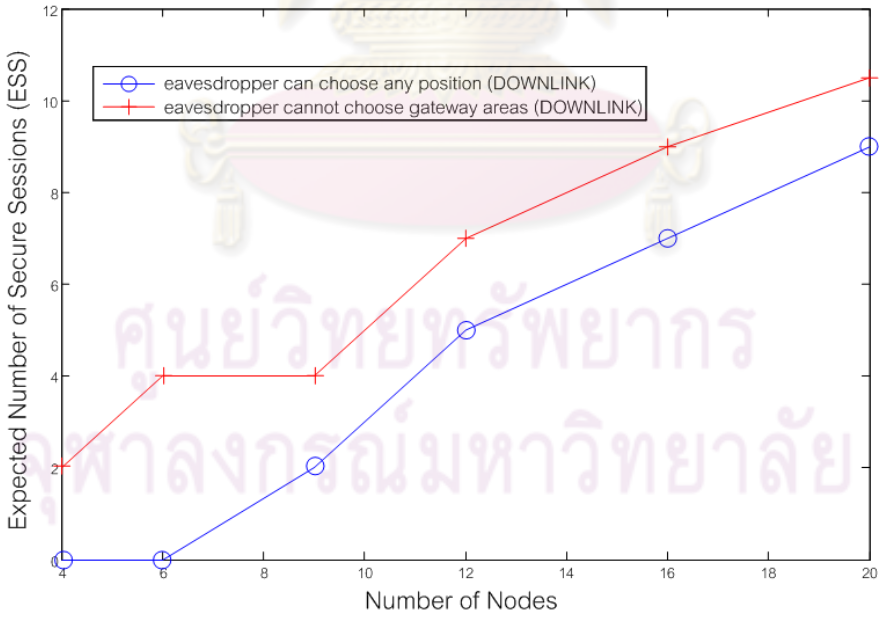


รูปที่ 4.28: ผลกระทบจากการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและการส่งสัญญาณรบกวนเมื่อผู้เล่นฝั่งโจมตีเลือกพื้นที่โจมตีได้อย่างอิสระกับกรณีที่ผู้เล่นฝั่งโจมตีไม่สามารถเลือกพื้นที่เพื่อโจมตีเกตเวย์ได้

จากผลการทดสอบดังรูปที่ 4.28 จะเห็นว่าทั้งกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและกรณีการส่งสัญญาณรบกวน มีแนวโน้มของค่า ESS ที่เหมือนกันคือ ณ ช่วงที่โครงข่ายมีขนาดเล็ก การป้องกันพื้นที่โจมตีของเกตเวย์สามารถช่วยเพิ่มค่า ESS ให้สูงขึ้นได้ แต่เมื่อโครงข่ายมีขนาดใหญ่ขึ้น การป้องกันพื้นที่ดังกล่าวไม่สามารถช่วยเพิ่มค่า ESS ได้ ซึ่งแสดงได้จากค่า ESS ซึ่งเท่ากับกรณีที่ผู้เล่นฝั่งโจมตีสามารถเลือกพื้นที่โจมตีได้อย่างอิสระ โดยเหตุผลที่เป็นเช่นนั้นสามารถอธิบายได้ดังนี้

กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น หากผู้เล่นฝั่งโจมตีสามารถเลือกพื้นที่โจมตีได้อย่างอิสระแล้ว ผู้เล่นฝั่งโจมตีจะเลือกพื้นที่โจมตีซึ่งสามารถดักฟังข้อมูลจากจุดเชื่อมต่อผ่านที่เป็นโนดข้างเคียงของเกตเวย์ได้พร้อมกัน ในกรณีที่โครงข่ายยังมีขนาดเล็ก พื้นที่โจมตีของเกตเวย์มีการซ้อนทับกับพื้นที่โจมตีซึ่งสามารถดักฟังข้อมูลจากจุดเชื่อมต่อผ่านที่เป็นโนดข้างเคียงของเกตเวย์ได้พร้อมกัน ทำให้การป้องกันพื้นที่ของเกตเวย์ เป็นการป้องกันไม่ให้ผู้เล่นฝั่งโจมตีเลือกพื้นที่โจมตีที่เหมาะสมที่สุดของผู้เล่นฝั่งโจมตีได้ ส่งผลให้ค่า ESS ในช่วงที่โครงข่ายยังมีขนาดเล็กนั้นมีค่าสูงขึ้น แต่เมื่อโครงข่ายมีขนาดใหญ่ขึ้นและตำแหน่งของเกตเวย์อยู่ห่างกันมากขึ้น ทำให้พื้นที่โจมตีของเกตเวย์ไม่ไปซ้อนทับกับพื้นที่โจมตีที่เหมาะสมที่สุดของผู้เล่นฝั่งโจมตี ทำให้การป้องกันพื้นที่โจมตีของเกตเวย์ดังกล่าวไม่สามารถเพิ่มระดับความปลอดภัยให้กับโครงข่ายได้

ในขณะที่กรณีการส่งสัญญาณรบกวน หากผู้เล่นฝั่งโจมตีสามารถเลือกพื้นที่โจมตีได้อย่างอิสระแล้ว ผู้เล่นฝั่งโจมตีจะเลือกพื้นที่โจมตี ซึ่งสามารถส่งสัญญาณรบกวนจุดเชื่อมต่อผ่านที่เป็นโนดข้างเคียงของเกตเวย์ได้พร้อมกัน หรือพื้นที่โจมตีซึ่งสามารถส่งสัญญาณรบกวนเกตเวย์ทั้งหมดได้พร้อมกัน แต่ในกรณีที่โครงข่ายยังมีขนาดเล็ก พื้นที่โจมตีของเกตเวย์มีการซ้อนทับกับพื้นที่โจมตีทั้งสองพื้นที่ข้างต้น ทำให้ในช่วงที่โครงข่ายมีขนาดเล็ก การป้องกันไม่ให้ผู้เล่นฝั่งโจมตีเลือกพื้นที่โจมตีเกตเวย์ได้สามารถเพิ่มค่า ESS ได้ แต่เมื่อโครงข่ายมีขนาดใหญ่ขึ้นและตำแหน่งของเกตเวย์อยู่ห่างกันมากขึ้น ทำให้พื้นที่โจมตีของเกตเวย์ไม่ซ้อนทับกับพื้นที่โจมตีที่เหมาะสมที่สุดของผู้เล่นฝั่งโจมตี ทำให้การป้องกันพื้นที่โจมตีของเกตเวย์ดังกล่าวไม่สามารถเพิ่มระดับความปลอดภัยให้กับโครงข่ายได้



รูปที่ 4.29: ผลกระทบจากการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงเมื่อผู้เล่นฝั่งโจมตีเลือกพื้นที่โจมตีได้อย่างอิสระกับกรณีที่ผู้เล่นฝั่งโจมตีไม่สามารถเลือกพื้นที่เพื่อโจมตีเกตเวย์ได้

แต่ในกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงมีผลกระทบที่แตกต่างกันออกไป จากผลการทดสอบรูปที่ 4.29 การป้องกันพื้นที่โจมตีของเกตเวย์สามารถเพิ่มค่า ESS ให้กับโครงข่ายที่นำมาทด

สอบได้ทุกกรณี เนื่องจากพื้นที่โจมตีที่เหมาะสมที่สุดของผู้เล่นฝั่งโจมตีในการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงกรณีนี้ คือ พื้นที่โจมตีของเกตเวย์ การป้องกันพื้นที่ดังกล่าวจึงเป็นการบังคับให้ผู้เล่นฝั่งโจมตีไม่สามารถเลือกพื้นที่โจมตีที่ดีที่สุดของตัวเองได้ ส่งผลให้โครงข่ายมีค่า ESS ที่เพิ่มขึ้นโดยจำนวนเซสชั่นที่ไม่ถูกโจมตีที่เพิ่มขึ้นนั้นเป็นเซสชั่นของโนดข้างเคียงของเกตเวย์ เนื่องจากการดักฟังเซสชั่นเหล่านี้ ผู้เล่นฝั่งโจมตีต้องเลือกพื้นที่โจมตีของเกตเวย์เท่านั้น

จากผลการทดสอบในหัวข้อนี้จะเห็นว่า กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น และกรณีการส่งสัญญาณรบกวนนั้น ผู้เล่นฝั่งโจมตีไม่จำเป็นที่ต้องโจมตีที่เกตเวย์ของโครงข่ายเสมอไป การป้องกันพื้นที่โจมตีของเกตเวย์ในโครงข่ายจึงไม่สามารถเพิ่มระดับความปลอดภัยให้กับโครงข่ายได้เสมอไป ขณะที่กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงกับโครงข่ายที่นำมาทดสอบ จะเห็นว่าการป้องกันพื้นที่โจมตีของเกตเวย์ สามารถช่วยเพิ่มระดับความปลอดภัยให้กับโครงข่ายได้ อย่างไรก็ตามการเพิ่มระดับความปลอดภัยด้วยการป้องกันพื้นที่โจมตีของเกตเวย์ไม่ให้ผู้เล่นฝั่งโจมตีเข้าไปได้ ในความเป็นจริงกระทำได้ยาก โดยปัญหาที่สำคัญ คือ การแยกความแตกต่างระหว่างผู้เล่นฝั่งโจมตีกับผู้ใช้งานโครงข่ายปกติ ซึ่งมีจำนวนมาก รวมถึงการป้องกันพื้นที่โจมตีของเกตเวย์ดังกล่าว ยังเป็นการวิธีที่เสี่ยงต่อการถูกโจมตีโดยที่ผู้เล่นฝั่งโจมตีเป็นคนในฝั่งเดียวกันเอง (insider attack) ได้ง่ายอีกด้วย

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

โครงข่ายไร้สายแบบเมชเป็นโครงข่ายที่กำลังได้รับความสนใจอย่างมาก เนื่องจากข้อดีอย่างประการทั้งการติดตั้งที่รวดเร็วและประหยัดต้นทุน แต่การใช้ตัวกลางไร้สายเป็นหลักในการสื่อสาร ทำให้ข้อมูลสำคัญต่าง ๆ ถูกดักฟังได้ง่าย นอกจากนี้การสื่อสารผ่านตัวกลางไร้สายยังเป็นการเปิดโอกาสให้ผู้โจมตีส่งสัญญาณรบกวนการสื่อสารระหว่างโนดได้ง่ายอีกด้วย

ในวิทยานิพนธ์ฉบับนี้ได้นำเสนอระเบียบวิธีในการหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมเพื่อป้องกันการดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมชในกรณีร้ายแรงที่สุด ในระเบียบวิธีที่นำเสนอได้จำลองลักษณะการโจมตีทั้งการดักฟังข้อมูลและการส่งสัญญาณรบกวนให้สอดคล้องกับโครงข่ายไร้สายมากขึ้น โดยคำนึงถึงตำแหน่งของผู้โจมตีซึ่งเหมาะสมที่สุดที่ผู้โจมตีใช้ในการโจมตีแต่ละรูปแบบ ซึ่งผลการทดสอบแสดงให้เห็นว่า ลักษณะการโจมตีดังกล่าวมีความรุนแรงมากกว่าสมมุติฐานเดิมที่ผู้โจมตีใช้การดักฟังข้อมูล หรือการส่งสัญญาณรบกวนที่ข่ายเชื่อมโยง นอกจากนั้นด้วยแบบจำลองลักษณะการโจมตีที่มีความเหมาะสมมากขึ้น ทำให้ระเบียบวิธีที่นำเสนอสามารถแยกความแตกต่างของการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่ายไร้สายแบบเมชออกจากกัน ผลการทดสอบพบว่า ทิศทางการส่งข้อมูลในโครงข่ายมีผลกับการดักฟังข้อมูลของผู้โจมตี การทดสอบกับโครงข่ายที่ศึกษานั้นจะเห็นว่า เมื่อขนาดโครงข่ายมีขนาดใหญ่ขึ้น ผลของความเสียหายจากการดักฟังข้อมูลในแต่ละทิศทางมีผลกระทบที่ต่างกัน นอกจากนั้นระเบียบวิธีที่นำเสนอยังสามารถแยกความแตกต่างระหว่างการโจมตีโดยการดักฟังข้อมูลและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมชได้ ซึ่งจากการทดสอบแสดงให้เห็นถึง ผลกระทบจากการส่งสัญญาณรบกวนหากเปรียบเทียบกับการดักฟังข้อมูลพบว่า การส่งสัญญาณรบกวนมีความรุนแรงมากที่สุดในทุกกรณี ซึ่งระเบียบวิธีที่นำเสนอสามารถพิจารณาความแตกต่างทั้งหมดข้างต้นนี้ได้ นอกจากนั้นด้วยลักษณะการโจมตีที่เหมาะสมกับโครงข่ายไร้สายมากขึ้น ยังทำให้ระเบียบวิธีนำเสนอสามารถหาการจัดเส้นทางเพื่อป้องกันการส่งสัญญาณรบกวนด้วยรัศมีในการส่งสัญญาณรบกวนค่าหนึ่ง ๆ ได้ ดังนั้นการจัดเส้นทางแบบเฟ้นสุ่มที่ได้จากระเบียบวิธีที่นำเสนอ จึงมีความเหมาะสมและสามารถป้องกันการโจมตีแต่ละแบบในการส่งข้อมูลแต่ละทิศทางในกรณีร้ายแรงที่สุดได้ โดยการจัดเส้นทางแบบเฟ้นสุ่มที่ได้ สามารถรับประกันระดับความปลอดภัยในรูปของ ค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีขั้นต่ำให้แก่โครงข่ายไร้สายแบบเมชผ่านตัวชี้วัด ESS ที่นำเสนอได้อีกด้วย รวมถึงระเบียบวิธีที่นำเสนอยังสามารถใช้วิเคราะห์ระดับความปลอดภัย เมื่อมีการเพิ่มจำนวนเกตเวย์ให้กับโครงข่ายในรูปแบบต่าง ๆ ซึ่งเป็นประโยชน์ในการวิเคราะห์ และช่วยในการออกแบบโครงข่ายไร้สายแบบเมชที่มีความทนทานต่อการโจมตีที่สูงได้ในอนาคต

5.2 ข้อเสนอแนะ

เพื่อให้งานวิจัยมีคุณค่ามากขึ้นระเบียบวิธีที่นำเสนอโดยวิทยานิพนธ์นี้สามารถนำมาวิจัยเพิ่มเติมได้หลายด้านดังนี้

ด้านการจำลองโครงข่ายให้มีความเหมาะสมกับสภาพของโครงข่ายไร้สายมากยิ่งขึ้น เช่น สภาพของตัวกลางไร้สายที่มีการขาดหายของสัญญาณเมื่อถูกส่งผ่านตัวกลางไร้สาย ระเบียบวิธีที่นำเสนอสามารถเพิ่มเติมลักษณะดังกล่าวได้ โดยอาจจำลองการขาดหายของสัญญาณดังกล่าวในรูปของความน่าจะเป็นที่การรับส่งข้อมูลระหว่างคู่โนดจะสำเร็จ ซึ่งการจำลองลักษณะดังกล่าวนี้ จะทำให้การจัดเส้นทางแบบเฟ้นสุ่มที่ได้มีความเหมาะสมกับการใช้งานจริงมากขึ้น เป็นต้น นอกจากนั้นวิทยานิพนธ์ฉบับนี้ได้ใช้การหาผลเฉลยด้วยกรรมวิธี MSA ซึ่งสามารถแก้ปัญหาทั้งเชิงสถิตและเชิงพลวัตได้ ทำให้ระเบียบวิธีที่นำเสนอมีความยืดหยุ่น และสามารถจำลองปัจจัยอื่นเพื่อศึกษาได้โดยง่ายอีกด้วย

การเพิ่มประสิทธิภาพของการป้องกันด้วยการจัดเส้นทางแบบเฟ้นสุ่ม จากผลการทดสอบจะพบว่าตำแหน่งของโนดทั้งเกตเวย์และจุดเชื่อมต่อผ่าน รวมทั้งค่ารัศมีการส่งสัญญาณไร้สายมีผลต่อระดับความปลอดภัยของโครงข่ายไร้สายแบบเมช ดังนั้นผลการทดสอบที่ได้ในวิทยานิพนธ์ฉบับนี้ จึงเป็นแนวทางในการพัฒนาการจัดเส้นทางแบบเฟ้นสุ่มให้มีประสิทธิภาพมากขึ้น หรือเป็นแนวทางในการออกแบบโครงข่ายที่เอื้อกับการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุด เพื่อให้โครงข่ายที่นำมาใช้ทดสอบสามารถรับประกันระดับความความปลอดภัยได้สูงยิ่งขึ้น

นอกจากนั้นในด้านการป้องกันการโจมตีในแต่ละประเภทให้มีประสิทธิภาพมากขึ้น โครงข่ายไร้สายแบบเมชอาจใช้วิธีป้องกันอื่นร่วมกับการจัดเส้นทางแบบเฟ้นสุ่มเพื่อเพิ่มระดับความปลอดภัยได้ เช่น กรณีการดักฟังข้อมูล ซึ่งอาจพิจารณาการป้องกันด้วยการเข้ารหัสร่วมกับการจัดเส้นทางแบบเฟ้นสุ่ม หรือกรณีการส่งสัญญาณรบกวน ซึ่งโครงข่ายอาจใช้โนดซึ่งสามารถรองรับการทำงานหลายความถี่หรือหลายช่องสัญญาณ เพื่อให้การจัดเส้นทางแบบเฟ้นสุ่มมีความหลากหลายมากขึ้นได้ เป็นต้น

รายการอ้างอิง

[1] Akyildiz, I. F.and Wang, X. A Survey on Wireless Mesh Networks. IEEE Magazine on Communications 43, 9, (2005): S23–S30.

[2] Salem, N. B.; and Hubaux, J. P. Securing Wireless Mesh Networks. IEEE Magazine on Wireless Communications 13, 2, (2006): 50–55.

[3] Zhang, Y.; Zheng, J. and Hu, H. Security in Wireless Mesh Networks. Illustrated Edition, Crc Press (2008).

[4] Canavan, J. E. Fundamentals of Network Security. Rtech House Inc (2001).

[5] Piyanan, S.; Kalika, S. and Chaodit, A. Reliability Evaluation by Expected Achievable Capacity in Stochastic Network Using Game Theory. Proc. of ICT International Conference 11, (2008).

[6] Piyanan, S.; Kalika, S. and Chaodit, A. Vulnerability Analysis in Multicommodity Stochastic Networks by Game Theory. Proc. of 5th ECTI-CON International Conference 1, 5, (2008): 357-360.

[7] Bell, M. G. H. The Use of Game Theory to Measure the Vulnerability of Stochastic Networks. IEEE Trans. on Reliability 52, 1, (2003): 63-68.

[8] Bohacek, S. and Hespansha, J. P. Saddle Policies for Secure Routing in Communication Networks. Proc. of the 41st IEEE Conference on Decision and Control 2 , (2002): 1416-1421.

[9] Bohacek, S; Hespansha, J. P.; Lee, J.; Lim, C. and Obraczka, K. Game Theoretic Stochastic Routing for Fault Tolerance and Security in Computer Networks. Parallel and Distributed Systems. IEEE Trans. on Parallel and Distributed Systems 18, 9, (2007): 1227-1240.

[10] Li, X. Y.; Wu, Y. and Wang, W. Stochastic Security in Wireless Mesh Networks via Saddle Routing Policy. Proc. of WASA 2007 on Wireless Algorithms, Systems and Applications (2008): 121-128.

[11] Karaa, H. and Lau J. Y. Game Theory Applications in Network Reliability. Proc. of 23rd Biennial Symposium on Communications (2006): 236-239.

[12] Xu, W.; Ma, K.; Trappe,W. and Zhang, Y. Jamming Sensor Networks: Attack and Defense Strategies. IEEE Magazine on Network 20, 3, (2006): 41-47.

[13] Xu, W.; Trappe, W.; Zhang, Y. and Wood, T. The Feasible of Launching and Detecting Jamming Attacks in Wireless Networks.

Proc. of 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (2005): 46-57.

[14] Noubir, G. and Lin,G. Low-Power DoS Attacks in Data Wireless LANs and Countermeasures. ACM SIGMOBILE on Mobile Computing and Communications 3, (2003).

[15] Xu, W.; Wood, T.; Trappe, W. and Zhang, Y. Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service. Proc. of 3rd ACM workshop on Wireless Security (2004): 80-89.

[16] Liu, X.; Noubir, G.; Sundarum, R. and Tan, S. Spread: Foiling Smart Jammer using Multi-layer Agility. Proc. of 26th INFOCOM IEEE on Computer Communications (2007): 2536-2540.

[17] Luce, R. D. and Raiffa, H. Game and Decisions. John Wiley & Sons (1985)

[18] Sheffi, Y. Urban Transportation Networks: Equilibrium Analysis with Mathematical Programming Methods Prentice-Hall Inc (1985)

ภาคผนวก

ภาคผนวก 1

บทความทางวิชาการที่ได้รับการเผยแพร่

บวรรัตน์ จินดาเลิศอุดมดี; กลิกา สุขสมบูรณ์ และ เชาวน์ดิศ อัศวกุล. การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเพื่อป้องกันการดักฟังข้อมูลในโครงข่ายไร้สายแบบเมช การประชุมวิชาการทางวิศวกรรมไฟฟ้าครั้งที่ 32 (2009)

การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเพื่อป้องกันการดักฟังข้อมูลในโครงข่ายไร้สายแบบเมช
Stochastic Routing with Game Theory for Eavesdropping Defense in Wireless Mesh Network

บวรรัตน์ จินดาเลิศอุดมดี กลิกา สุขสมบูรณ์ และ เชาวน์ดิศ อัศวกุล
ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
E-mail: bowornrat.c@gmail.com, kmitmink@yahoo.com, chaodit.a@chula.ac.th

บทคัดย่อ

ปัจจุบันโครงข่ายไร้สายแบบเมชได้รับความสนใจอย่างมาก เนื่องจากการติดตั้งรวดเร็วและประหยัดต้นทุน แต่การสื่อสารผ่านตัวกลางไร้สายกลับทำให้ข้อมูลถูกดักฟังได้ง่าย ในงานวิจัยนี้จึงได้นำเสนอระเบียบวิธีใหม่ในการวิเคราะห์ และหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมโดยใช้ทฤษฎีเกมเพื่อป้องกันการดักฟังข้อมูล และได้ปรับปรุงวิธีการจำลองการดักฟังให้สอดคล้องกับโครงข่ายไร้สายมากขึ้น โดยคำนึงถึงตำแหน่งซึ่งเหมาะสมที่สุดที่ผู้โจมตีใช้ในการดักฟัง ดังนั้นระเบียบวิธีที่นำเสนอ สามารถวิเคราะห์หาค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัย (expected number of secure sessions, ESS) ขั้นต่ำที่พึงได้ในโครงข่ายไร้สายแบบเมช ผลการทดสอบแสดงให้เห็นถึงผลที่แตกต่างกันของการส่งข้อมูลในแต่ละทิศทางผ่านตัวชี้วัด ESS ที่นำเสนอ นอกจากนั้นรูปแบบการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสม จากระเบียบวิธีที่นำเสนอสามารถป้องกันการดักฟังข้อมูลในกรณีร้ายแรงที่สุด และรับประกันจำนวนเซสชั่นที่ปลอดภัยขั้นต่ำให้กับโครงข่ายไร้สายแบบเมชได้อีกด้วย

Abstract

Nowadays, Wireless Mesh Networks (WMNs) are good solutions for investment due to their fast and low-cost deployment. Using wireless medium, however, increases risk from attackers that may eavesdrop important data easily. In this paper, we propose a new framework for finding optimal stochastic routing with game theory to defend against an eavesdropper who, in turn, chooses its most appropiate positions. The proposed framework can, therefore, help analyze a lower bound in the expected number of secured sessions (ESS) that may be achieved in WMNs. The numerical results show the different effect of traffic direction in terms of ESS value. Moreover, optimal stochastic routing from proposed framework can defend intelligent eavesdropping and also guarantee number of secure sessions for WMNs.

Keywords: Wireless Mesh Network (WMN), Stochastic Routing, Game Theory, Intelligent Eavesdropping

1 บทนำ

โครงข่ายไร้สายแบบเมช (Wireless Mesh Network, WMN) มีข้อดีหลายประการเช่น การติดตั้งง่าย รวดเร็ว และประหยัดต้นทุนเนื่องจากใช้การสื่อสารผ่านตัวกลางไร้สายเป็นหลัก แต่การใช้งานโครงข่ายไร้สายแบบเมชนี้กลับยังไม่แพร่หลายเนื่องจากปัญหาด้านความปลอดภัย [1] เมื่อโครงข่ายแกนกลาง (backbone network) ประกอบด้วยตัวกลางไร้สายทั้งหมดส่งผลให้ผู้โจมตีสามารถดักฟังข้อมูลสำคัญได้ง่าย นอกจากนั้นเนื้อหาที่ถูกดักฟังอาจเป็นต้นเหตุนำไปสู่การโจมตีชนิดอื่นตามมาได้

ด้วยเหตุผลดังกล่าว ทำให้การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมซึ่งเป็นวิธีป้องกันการดักฟังข้อมูลวิธีหนึ่งที่ใช้ในโครงข่าย ที่ใช้สายสื่อสาร (wired network) ถูกนำเสนอเพื่อใช้กับโครงข่ายไร้สายแบบเมช โดยวิธีดังกล่าวนี้ จุดเชื่อมต่อจะเลือกเส้นทางเชื่อมต่อกับปลายทางอย่างสุ่ม เพื่อลดโอกาสที่ผู้โจมตีจะเลือกดักฟังข้อมูลจากเส้นทางที่ใช้ส่งได้ถูกต้องน้อยลง และทฤษฎีเกมถูกนำมาใช้วิเคราะห์เพื่อให้การจัดเส้นทางแบบเฟ้นสุ่มสามารถป้องกันการดักฟังข้อมูลในกรณีร้ายแรงที่สุดได้ ด้วยหลักการดังกล่าว ทำให้วิธีนี้ไม่เพียงใช้แก้ปัญหาการดักฟังข้อมูลเท่านั้น [2]-[4] แต่สามารถใช้ป้องกันการส่งสัญญาณรบกวนในโครงข่ายไร้สาย [4], [5] รวมถึงใช้ลดความเสี่ยงที่ข้อมูลจะสูญหายเนื่องจากอุปกรณ์โครงข่ายได้รับความเสียหาย [2] , [3], [6]-[8] ได้

อย่างไรก็ตาม ลักษณะการดักฟังข้อมูลในโครงข่ายที่ใช้สายสื่อสารซึ่งผู้โจมตีเลือกดักฟังข้อมูลจากข่ายเชื่อมโยงหนึ่ง (link-based eavesdropping) แตกต่างกับผู้โจมตีในโครงข่ายไร้สายซึ่งเลือกดักฟังข้อมูลผ่านตัวกลางไร้สาย ทำให้ผู้โจมตีมีโอกาสดักฟังข้อมูลได้ทีละหลายคู่สื่อสารขึ้นอยู่กับตำแหน่งว่าผู้โจมตีอยู่ในพื้นที่ครอบคลุมของจุดเชื่อมต่อใด ความแตกต่างดังกล่าวนี้ ทำให้การจัดเส้นทางแบบเฟ้นสุ่มซึ่งได้จากระเบียบวิธีที่ศึกษาในโครงข่ายที่ใช้สายสื่อสาร [2], [3] หรือจากระเบียบวิธีที่มีลักษณะการดักฟังข้อมูลเหมือนการดักฟังในโครงข่ายที่ใช้สายสื่อสาร [4] ไม่สามารถนำมาใช้ป้องกันการดักฟังข้อมูลในโครงข่ายไร้สายได้ อีกทั้งการเลือกช่องสัญญาณอย่างสุ่มใน [4] ก็ไม่สามารถเพิ่มระดับความปลอดภัยให้แก่โครงข่ายได้เช่นกัน เนื่องจากผู้โจมตีสามารถเลือกดักฟังข้อมูลจากช่องสัญญาณหนึ่ง จากนั้นเปลี่ยนไปดักฟังอีกช่องสัญญาณหนึ่งที่ผ่านตำแหน่งที่ดักฟังอยู่ได้ ยิ่งไปกว่านั้นภายในโครงข่ายไร้สายแบบเมชยังมีลักษณะการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง ซึ่งมีกลุ่มของจุดเชื่อมต่อที่ส่งข้อมูลออกมาผ่านตัวกลางไร้สายแตกต่างกัน โครงข่ายไร้สายแบบเมชจึงต้องการการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสม กับการส่งข้อมูลในแต่ละทิศทางอีกด้วย

ดังนั้น ในงานวิจัยนี้ได้นำเสนอระเบียบวิธีการหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมโดยใช้ทฤษฎีเกม เพื่อแก้ปัญหาการดักฟังข้อมูลในโครงข่ายไร้สายแบบเมช ในส่วนของการจำลองลักษณะการดักฟังข้อมูลให้มีความสมจริงกับการดักฟังในโครงข่ายไร้สายมากขึ้น งานวิจัยนี้ได้นำเสนอแบบจำลองใหม่สำหรับการดักฟัง โดยขึ้นกับตำแหน่งของผู้โจมตีว่าอยู่ในพื้นที่ครอบคลุมของจุดเชื่อมต่อใด (position-based eavesdropping) ซึ่งแบบจำลองดังกล่าวสามารถแยกความแตกต่างของการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่ายไร้สายแบบเมชออกจากกันได้ การจัดเส้นทางแบบเฟ้นสุ่มที่ได้จากระเบียบวิธีที่นำเสนอนั้น สามารถป้องกัน

การดักฟังข้อมูลที่เกิดขึ้นจริงในโครงข่ายไร้สายแบบเมช ในกรณีร้ายแรงที่สุดได้ และสามารถรับประกันระดับความปลอดภัยขั้นต่ำให้กับโครงข่ายไร้สายแบบเมชได้

2 แบบจำลองโครงข่าย

โครงข่ายไร้สายแบบเมชประกอบไปด้วยจุดเชื่อมต่อสองชนิด คือ เกตเวย์ (Gateways , GW) ซึ่งเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตผ่านสายสื่อสาร และจุดเชื่อมต่อผ่าน (Transit Access Points, TAP) ซึ่งรับ/ส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต โดยสร้างเซสชั่นผ่านเกตเวย์ในลักษณะหลายช่วงเชื่อมต่อ (multi-hop) นอกจากนั้นกำหนดให้การส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงมีความแตกต่างกันโดย การส่งข้อมูลฝั่งขาขึ้นเป็นการส่งข้อมูลจาก TAP ไปยัง GW ผ่านช่องสัญญาณไร้สาย จากนั้นจะส่งข้อมูลไปยังโครงข่ายอินเทอร์เน็ตที่เชื่อมต่อผ่านสายสื่อสาร ดังนั้นข้อมูลจะถูกส่งต่อผ่านช่องสัญญาณไร้สายในช่วงเชื่อมต่อทุกช่วงยกเว้น ณ จุดสุดท้าย คือ GW ในลักษณะเดียวกันนี้การส่งข้อมูลฝั่งขาลง TAP ที่เป็นจุดเชื่อมต่อปลายทาง (destination node) จะไม่ส่งข้อมูลออกมาผ่านตัวกลางไร้สายเช่นกัน

3 แบบจำลองเกมของการส่งข้อมูลในโครงข่าย

จากปัญหาการดักฟังที่เกิดขึ้นระหว่างโครงข่ายกับผู้โจมตี มีลักษณะความขัดแย้งกัน สถานการณ์ดังกล่าวสามารถจำลองด้วยเกมที่มีผู้เล่นสองคนที่มีผลรวมเป็นศูนย์ (two-person zero-sum game) โดยผู้เล่นคนหนึ่งเป็นฝั่งป้องกัน และผู้เล่นอีกคนหนึ่งเป็นฝั่งโจมตี รายละเอียดทั้งหมดอธิบายได้ด้วยเกมในรูปแบบปกติ (normal form) ประกอบไปด้วยแผนการของผู้เล่นทั้งสองฝั่งและค่าของเกมดังนี้

3.1 ผู้เล่น 1 : ฝั่งป้องกัน

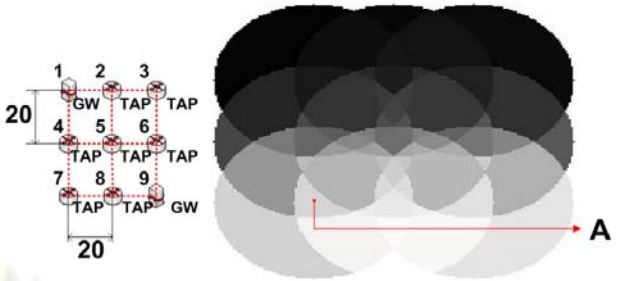
เพื่อให้ผู้โจมตีคาดเดาเส้นทางที่ใช้ส่งมูลได้ยาก TAP ซึ่งต้องการรับ/ส่งข้อมูลจะเลือกเส้นทางเชื่อมต่อกับ GW อย่างสุ่ม ด้วยการส่งข้อมูลแบบแอดฮ็อกในโครงข่ายไร้สายแบบเมช จะใช้จุดเชื่อมต่อข้างเคียงในการส่งต่อข้อมูลไปที่ปลายทาง และเส้นทางที่เป็นลูป (loop) นั้นเสี่ยงต่อการถูกดักฟัง ดังนั้นฝั่งป้องกันจึงควรใช้แผนการเล่นเป็น การเลือกส่งข้อมูลในลักษณะของทรี (tree) ที่มีราก ณ ปลายทางเป็น GW และเชื่อมต่อกับ TAP ทุกจุดที่ต้องการรับ/ส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต กำหนดให้รูปแบบของทรีที่เป็นไปได้ทั้งหมดมี M รูปแบบ การแจกแจงความน่าจะเป็นในการเลือกรูปแบบการส่งสามารถนิยามได้ดังนี้

$$P^T = [p_1, \ldots, p_i, \ldots, p_M]$$

โดย p_i คือ ความน่าจะเป็นที่รูปแบบการส่งทรีแบบที่ i ถูกเลือกใช้โดย TAP ต่าง ๆ ซึ่งเป็นผู้เล่นฝั่งป้องกัน

3.2 ผู้เล่น 2 : ฝั่งโจมตี

ผู้โจมตีมีเป้าหมายคือ การเลือกตำแหน่งในโครงข่ายเพื่อดักฟังข้อมูลที่รับ/ส่งระหว่าง TAP ทั้งหมดกับ GW ให้ได้มากที่สุด ดังนั้นแผนการเล่น จึงเป็นเซตของตำแหน่งที่เป็นไปได้ทั้งหมดในพื้นที่ที่โครงข่ายไร้สายแบบเมชติดตั้งอยู่ ซึ่งเซตที่ได้เป็นเซตอนันต์ เพื่อหลีกเลี่ยงกรณีดังกล่าว งานวิจัยนี้จึงพิจารณาแผนการเล่นของผู้โจมตี โดยจัดกลุ่มภายในเซตของตำแหน่งที่เป็นไปได้ทั้งหมดใหม่ และนิยามเป็นเซตของพื้นที่ครอบคลุมซึ่งหากผู้โจมตีเลือกพื้นที่ดังกล่าวเพื่อดักฟังแล้ว จะสามารถดักฟังเซตของจุดเชื่อมต่อได้เป็นเซตเดียวกัน การพิจารณาแผนการเล่นของผู้โจมตีใหม่นี้ ทำให้แผนการเล่นของฝั่งผู้โจมตีเป็นเซตจำกัดและสามารถหาผลเฉลยได้เสมอตามทฤษฎีมินิแมกซ์ เพื่อความชัดเจนจึงขออธิบายด้วยการยกตัวอย่างต่อไปนี้ จากรูปที่ 1 แสดงเซตของพื้นที่ครอบคลุม



รูปที่ 1: การเปลี่ยนเซตของตำแหน่งมาเป็นเซตของพื้นที่ครอบคลุมทั้งหมดที่เป็นไปได้

ทั้งหมดที่เป็นไปได้ของทุกโหนดในโครงข่ายแบบตารางขนาด 9 โหนด ซึ่งวางห่างกัน 20 หน่วยของระยะทางและมีรัศมีการส่งสัญญาณไร้สายเท่ากัน คือ 25 หน่วย หากผู้โจมตีเลือกดักฟังที่ตำแหน่งในพื้นที่ A จะสามารถดักฟังข้อมูลที่ส่งผ่านตัวกลางไร้สาย ณ จุดเชื่อมต่อที่ 4,7 และ 8 ดังนั้นกำหนดให้พื้นที่ครอบคลุมทั้งหมดที่เป็นไปได้มี N พื้นที่ การแจกแจงความน่าจะเป็นในการเลือกพื้นที่เพื่อดักฟังข้อมูลสามารถนิยามได้ดังนี้

$$Q^T = [q_1, \ldots, q_j, \ldots, q_N]$$

โดย q_j คือ ความน่าจะเป็นที่พื้นที่ที่ j ถูกเลือกโดยผู้ดักฟังซึ่งเป็นผู้เล่นที่จ้องโจมตีความปลอดภัยในการรับ/ส่งข้อมูลของโครงข่าย

3.3 ค่าของเกม

เมื่อเปรียบเทียบความเร็วในการส่งข้อมูลของโครงข่าย กับการเคลื่อนที่ของผู้โจมตีจะพบว่าการส่งข้อมูลมีความเร็วมากกว่าผู้โจมตีมาก ผู้โจมตีจึงเห็นการส่งข้อมูลระหว่าง TAP กับ GW ในทุกเส้นทางเกิดขึ้นพร้อมกันโดยไม่สามารถเคลื่อนที่ไปดักฟังข้อมูลที่เหลือได้ทัน ดังนั้นค่าของเกมจึงนิยามเป็น จำนวนเซสชั่นที่ปลอดภัยระหว่าง TAP กับ GW ซึ่งเซสชั่นที่ไม่ปลอดภัยหมายถึง เซสชั่นที่มีจุดเชื่อมต่อซึ่งถูกดักฟังอยู่เป็นส่วนหนึ่งของเส้นทางบนทรีของการส่งข้อมูลที่เลือกใช้ และเซสชั่นดังกล่าวใช้จุดเชื่อมต่อนั้นส่งข้อมูลออกมาผ่านตัวกลางไร้สาย

ตารางผลได้ผลเสีย (payoff table) สามารถเขียนออกมาได้ดังนี้

$$S = \begin{pmatrix} s_{1,1} & \cdots & s_{1,N} \\ \vdots & \ddots & \vdots \\ s_{M,1} & \cdots & s_{M,N} \end{pmatrix}$$

โดย $s_{i,j}$ คือ จำนวนเซสชั่นที่ปลอดภัยเมื่อฝั่งป้องกันเลือกรูปแบบการส่งที่ i และผู้โจมตีเลือกพื้นที่ที่ j ในการดักฟังข้อมูล

4 การวิเคราะห์และแก้ปัญหาด้วยวิธี MSA (Method of Successive Average)

ในการหาผลเฉลยนั้นงานวิจัยนี้ใช้หลักการโต้ตอบที่ดีที่สุด (best response) ร่วมกับกระบวนการปรับปรุงความน่าจะเป็นด้วย MSA ซึ่งเป็นกระบวนการที่เป็นที่รู้จัก และถูกใช้ในการแก้ปัญหาในงานวิจัยซึ่งศึกษาการจัดเส้นทางแบบเฟ้นสุ่ม เช่น [6]-[8] โดยวิธีการหาผลเฉลยดังกล่าวมีขั้นตอนดังนี้

1. เริ่มต้นโดยให้ผู้เล่นทั้งคู่กำหนดค่าความน่าจะเป็นในการเลือกแผนการเล่นแต่ละแผนมีค่าเท่ากันตามสมการต่อไปนี้

ฝั่งป้องกัน

$$p_i = \frac{1}{M}, \quad \text{สำหรับทุกค่า} \quad i$$

ฝั่งผู้โจมตี

$$q_j = \frac{1}{N}, \quad \text{สำหรับทุกค่า} \quad j$$

และกำหนดรอบของการเล่นเกมเริ่มแรกเป็นรอบที่ 1 ($n = 1$)

2. ฝั่งป้องกันเลือกรูปแบบการส่งที่ได้ค่าคาดหวัง (expectation) ของจำนวนเซสชั่นที่ปลอดภัยมากที่สุดโดยถือว่าฝั่งโจมตีได้เลือกพื้นที่ เพื่อดักฟังเซสชั่นตามการแจกแจงความน่าจะเป็นล่าสุด ซึ่งค่าคาดหวังของจำนวนเซสชั่นดังกล่าวนิยามได้ดังนี้

$$ESS_i = \sum_{j=1}^{N} [q_j s_{i,j}]$$

โดยรูปแบบการส่งที่ได้ค่าของ ESS_i สูงสุด $(\hat{i})$ นิยามได้ดังนี้ $\hat{i} = \arg\max_i \{ESS_i\}$ หลังจากนั้นฝั่งป้องกันปรับปรุงการแจกแจงความน่าจะเป็นในการเลือกรูปแบบการส่งดังสมการนี้

$$p_i \leftarrow \left(\frac{1}{n}\right) x_i + \left(\frac{n-1}{n}\right) p_i; \; x_i = \begin{cases} 1, & \text{ถ้า } i = \hat{i} \\ 0, & \text{อื่น ๆ} \end{cases}$$

3. ฝั่งผู้โจมตีเลือกพื้นที่เพื่อดักฟังเซสชั่นให้ได้มากที่สุดโดยถือว่าฝั่งป้องกันได้เลือกรูปแบบการส่งตามการแจกแจงความน่าจะเป็น ในการเลือกรูปแบบการส่งล่าสุด ซึ่งค่าคาดหวังของจำนวนเซสชั่นดังกล่าวนิยามได้ดังนี้

$$ESS_j = \sum_{i=1}^{M} [p_i s_{i,j}]$$

โดยพื้นที่ที่ดักฟังเซสชั่นได้มากที่สุด $(\hat{j})$ นิยามได้ดังนี้ $\hat{j} = \arg\min_j \{ESS_j\}$ หลังจากนั้นฝั่งผู้โจมตีปรับปรุงการแจกแจงความน่าจะเป็นในการเลือกพื้นที่เพื่อดักฟังเซสชั่นดังสมการนี้

$$q_j \leftarrow \left(\frac{1}{n}\right) y_j + \left(\frac{n-1}{n}\right) q_j; \; y_j = \begin{cases} 1, & \text{ถ้า } j = \hat{j} \\ 0, & \text{อื่น ๆ} \end{cases}$$

4. คำนวนค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัย (ESS) สำหรับรอบที่ n ดังสมการ

$$ESS = \sum_{i=1}^{M} \sum_{j=1}^{N} p_i q_j s_{i,j} = P^T S Q$$

5. ดำเนินการตามขั้นตอนที่ 2-4 พร้อมทั้งปรับรอบของการเล่นดังนี้ $n \leftarrow n + 1$ จนกระทั่งค่า ESS เข้าสู่จุดสมดุล คือ ลู่เข้าสู่ค่าคงที่ค่าหนึ่ง

ค่า ESS ที่ได้รวมถึงการแจกแจงความน่าจะเป็นในการเลือกแผนการเล่น ณ จุดสมดุลจะเป็นคำตอบที่เหมาะสมที่สุดของผู้เล่นทั้งสองฝั่ง โดยความหมายของค่า ESS ณ จุดสมดุลนี้คือ จำนวนเซสชั่นที่ปลอดภัยขั้นต่ำที่สุดที่พึงได้ เมื่อโครงข่ายใช้รูปแบบการส่งข้อมูลอย่างเหมาะสมที่สุดและงานวิจัยนี้ใช้ค่า ESS เพื่อบ่งชี้ระดับความปลอดภัยขั้นต่ำที่สุดที่พึงได้ของโครงข่าย

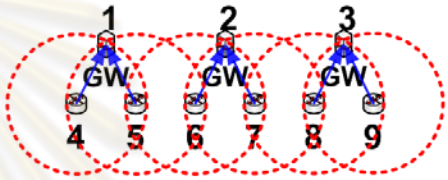
สำหรับการวิเคราะห์ในทางปฏิบัตินั้น พบว่าปัญหาที่พิจารณาอาจมีหลายคำตอบของแผนการเล่น ณ จุดสมดุลของเกม จากทฤษฎีเกมที่มีผู้เล่นสองคนที่มีผลรวมเป็นศูนย์ ในทุกคำตอบจะให้ค่าของเกม ESS เท่ากัน ดังนั้นแต่ละคำตอบที่ได้จึงไม่มีผลกระทบต่อการชี้วัดระดับความปลอดภัย โดยตัวชี้วัดที่นำเสนอ รวมทั้งโครงข่ายสามารถเลือกใช้รูปแบบการส่งที่เหมาะสมที่สุดจากคำตอบหนึ่งเพื่อใช้ป้องกันการดักฟังได้

5 ผลการทดสอบ

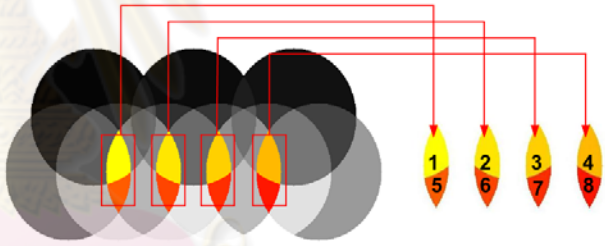
งานวิจัยนี้แบ่งการทดสอบเป็น 2 ส่วน ซึ่งการทดสอบทั้งหมดใช้โปรแกรม MATLAB จำลองสถานการณ์ โดยส่วนแรกจะแสดงถึงรูปแบบการส่งข้อมูลที่เหมาะสม การดักฟังของผู้โจมตี และค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยของการส่งข้อมูลในแต่ละทิศทาง ส่วนที่สองจะศึกษาผลของกระทบ และเปรียบเทียบลักษณะการดักฟังจากตัวกลางไร้สายกับการดักฟังจากข่ายเชื่อมโยงเมื่อโครงข่ายมีขนาดใหญ่ขึ้น

5.1 ผลของทิศทางการส่งข้อมูล

โครงข่ายที่นำมาทดสอบ คือ โครงข่ายอย่างง่ายประกอบไปด้วย GW 3 โหนดซึ่งวางห่างกัน 30 หน่วยของระยะทางในแนวนอน และมี TAP 6 โหนดซึ่งวางห่างกัน 20 หน่วยในแนวแกนนอน และห่างกับ GW ในแนวแกนตั้ง 20 หน่วย แต่ละจุดเชื่อมต่อมีรัศมีการส่งสัญญาณไร้สายเท่ากันคือ 25 หน่วย ผลที่ได้มีดังนี้



ก. รูปแบบการส่งที่ดีที่สุดสำหรับการส่งข้อมูลฝั่งขาขึ้น

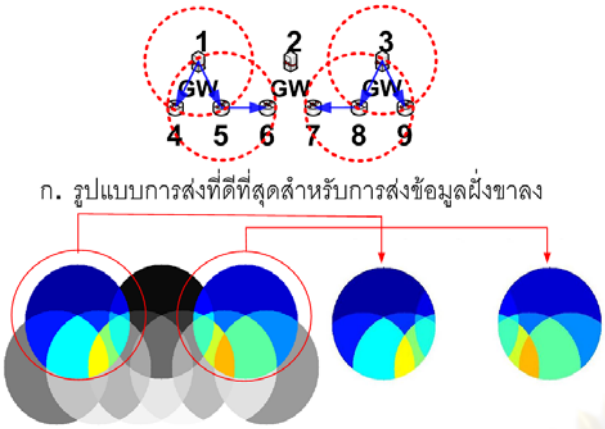


ข. พื้นที่ที่ผู้โจมตีเลือกใช้ดักฟังเซสชั่นฝั่งขาขึ้น

รูปที่ 2: ผลการทดสอบกับโครงข่ายอย่างง่ายในการส่งข้อมูลฝั่งขาขึ้นไปยัง GW

ในการส่งข้อมูลฝั่งขาขึ้น GW ไม่ได้ส่งข้อมูลออกมาผ่านตัวกลางไร้สาย หากผู้โจมตีเลือกพื้นที่ของ GW อย่างเดียวเพื่อดักฟังจะทำให้ผู้โจมตีไม่สามารถดักฟังเซสชั่นใดๆ ได้ ดังนั้นผู้โจมตีจึงเลือกดักฟังเซสชั่นในพื้นที่ของจุดเชื่อมต่อข้างเคียงของ GW ซ้อนทับกันพื้นที่ใดก็ได้จาก 8 พื้นที่ดังรูปที่ 2ข. ส่วนรูปแบบการส่งที่เหมาะสำหรับการส่งข้อมูลฝั่งขาขึ้นเป็นแบบกระจายเส้นทางอย่างสมดุล (load balancing) ดังรูปที่ 2ก. ทำให้ค่า ESS สำหรับการส่งข้อมูลฝั่งขาขึ้นมีค่าเท่ากับ 3 เซสชั่น

ในขณะที่การส่งข้อมูลฝั่งขาลงได้ค่า ESS เท่ากับ 3 เซสชั่นเช่นกัน แต่ลักษณะพื้นที่ในการดักฟังเซสชั่นของผู้โจมตีแตกต่างกันอย่างสิ้นเชิง โดยในฝั่งขาลงผู้โจมตีเลือกดักฟังในพื้นที่ของ GW ดังรูปที่ 3ข. เนื่องจาก GW จะส่งข้อมูลของทุกเซสชั่นออกมาผ่านตัวกลางไร้สาย ส่งผลให้รูปแบบการส่งที่เหมาะสำหรับการส่งข้อมูลฝั่งขาลงแตกต่างออกไป คือ การส่งโดยไม่ใช้ GW ที่มีพื้นที่ครอบคลุมซ้อนทับกันอยู่ส่งพร้อมกันดังรูปที่ 3ก. โดยรูปแบบการส่งที่เหมาะสม และการ



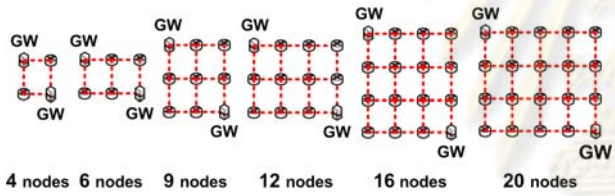
ก. รูปแบบการส่งที่ดีที่สุดสำหรับการส่งข้อมูลฝั่งขาลง

ข. พื้นที่ที่ผู้โจมตีเลือกใช้ดักฟังเซสชั่นฝั่งขาลง

รูปที่ 3: ผลการทดสอบกับโครงข่ายอย่างง่ายในการส่งข้อมูลฝั่งขาลงไป GW ไปยัง TAP ต่างๆ

เลือกพื้นที่ของผู้โจมตีมีเพียงรูปแบบเดียว

5.2 ผลกระทบของการเพิ่มขนาดโครงข่าย



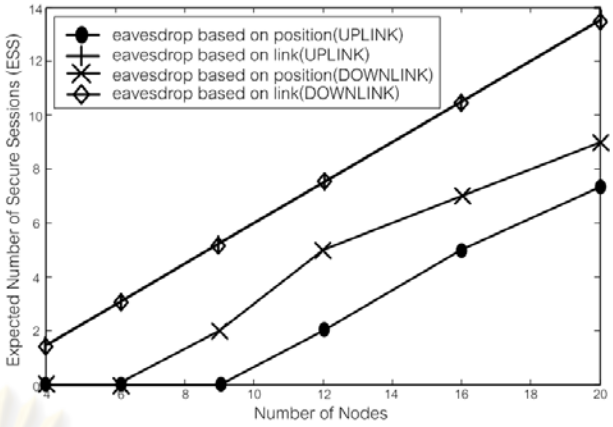
รูปที่ 4: โครงข่ายที่ใช้ศึกษากรณีที่โครงข่ายมีขนาดใหญ่ขึ้น

โครงข่ายที่นำมาทดสอบเป็นแบบตารางดังรูปที่ 4 โดยเป็นการต่อถึงกันอย่างง่าย ที่สามารถครอบคลุมพื้นที่ให้บริการได้ทั่วถึงการทดสอบนี้ ได้เปรียบเทียบผลจากการจำลองการดักฟังข้อมูลจากตัวกลางไร้สายที่นำเสนอ กับการดักฟังข้อมูลจากข่ายเชื่อมโยงที่พิจารณาใน [4] ผลการทดสอบแสดงดังรูปที่ 5

พบว่าการดักฟังข้อมูลจากตัวกลางไร้สายนั้นมีค่า ESS ต่ำกว่าการดักฟังข้อมูลจากข่ายเชื่อมโยงในทุกกรณี ซึ่งแสดงให้เห็นว่าการดักฟังข้อมูลที่เกิดขึ้นจริงจากตัวกลางไร้สาย (position-based eavesdropping) มีความรุนแรงมากกว่าการดักฟังข้อมูลในงานวิจัย [4] (link-based eavesdropping) เมื่อโครงข่ายมีขนาดใหญ่ขึ้น ลักษณะการดักฟังข้อมูลจากข่ายเชื่อมโยง ไม่สามารถแยกความแตกต่างของระดับความปลอดภัยที่เกิดขึ้นจากการส่งข้อมูลในแต่ละทิศทางได้ ทำให้ค่า ESS ของการส่งข้อมูลทั้งสองทิศทางเท่ากันทุกกรณี ในขณะที่ค่า ESS จากระเบียบวิธีที่นำเสนอสามารถชี้ให้เห็นถึงความแตกต่างได้

6 สรุป

ในงานวิจัยนี้ ได้เสนอระเบียบวิธีในการหาการจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมเพื่อป้องกันการดักฟังข้อมูลอย่างร้ายแรงที่สุด ในโครงข่ายไร้สายแบบเมช และได้จำลองวิธีการดักฟังข้อมูลที่สอดคล้องกับโครงข่ายไร้สายซึ่งจากผลการทดสอบพบว่ามีความรุนแรงมากกว่าสมมุติฐานเดิมที่ใช้รูปแบบการดักฟังข้อมูลจากข่ายเชื่อมโยง รวมถึงแบบ



รูปที่ 5: เปรียบเทียบลักษณะการดักฟังจากตัวกลางไร้สายและจากข่ายเชื่อมโยงเมื่อโครงข่ายมีขนาดใหญ่มากขึ้น

จำลองที่สมจริงมากขึ้นทำให้สามารถแยกความแตกต่างของการส่งข้อมูลในฝั่งขาขึ้นและฝั่งขาลงออกจากกัน และพบว่าการดักฟังข้อมูลที่เกิดขึ้นในแต่ละทิศทางการส่งข้อมูลนั้นต่างกัน ยิ่งไปกว่านั้นการต่อถึงกันในกรณีหนึ่งๆ เมื่อโครงข่ายมีขนาดใหญ่ขึ้นให้ผลของความเสียหายจากการดักฟังข้อมูลจากการส่งข้อมูลในแต่ละทิศทางที่ต่างกันออกไป ซึ่งระเบียบวิธีที่ได้นำเสนอ สามารถพิจารณาปัจจัยดังกล่าวนี้ทำให้การจัดเส้นทางแบบเฟ้นสุ่มที่ได้ มีความเหมาะสมกับแต่ทิศทางการส่งข้อมูลและยังสามารถป้องกันการดักฟังที่สมจริงในกรณีร้ายแรงที่สุด โดยรับประกันจำนวนเซสชั่นที่ปลอดภัยขั้นต่ำที่พึงได้แก่โครงข่ายไร้สายแบบเมช โดยบ่งชี้จากตัวชี้วัด ESS ที่นำเสนอได้อีกด้วย

เอกสารอ้างอิง

[1] N. Ben Salem and J.P. Hubaux, “Securing in Wireless Mesh Networks,” *IEEE on Wireless Communications*, 2006.

[2] S. Bohacek, J. P. Hespanha, and K. Obraczka, “Saddle Policies for Secure Routing in Communication Networks,” *Proc. of 41st IEEE Conf. on Decision and Control*, 2002.

[3] S. Bohacek, et. al., “Game Theoretic Stochastic Routing for Fault Tolerance and Security in Computer Networks,” *IEEE Trans. on Parallel and Distributed Systems*, 2007.

[4] X. Y. Li, Y. Wu, and W. Z. Wang, “Stochastic Security in Wireless Mesh Networks via Saddle Routing Policy,” *Proc. of Wireless Algorithms, Systems and Applications*, 2007.

[5] H. Karaa and J. Y. Lau, “Game Theory Applications in Network Reliability,” *Proc. of 23rd Biennial Symposium on Communications*, 2006.

[6] P Satayapiwat, K Suksomboon, and C Aswakul, “Reliability Evaluation by Expected Achievable Capacity in Stochastic Network Using Game Theory,” *Proc. of ICT 2008*, 2008.

[7] P Satayapiwat, K Suksomboon, and C Aswakul, “Vulnerability Analysis in Multicommodity Stochastic Networks by Game Theory,” *Proc. of 5th ECTI-CON 2008*, 2008.

[8] M. G. H. Bell, “The use of game theory to measure the vulnerability of stochastic networks,” *IEEE Trans. on Reliability*, 2003.

ประวัติผู้เขียนวิทยานิพนธ์

นายบวรรัตน์ จินดาเลิศอุดมดี เกิดเมื่อวันที่ 30 เมษายน พ.ศ. 2528 จังหวัดกรุงเทพมหานคร เป็นบุตรของนายวิชิต และนางสุภาพร จินดาเลิศอุดมดี สำเร็จการศึกษาระดับปริญญาหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า จากจุฬาลงกรณ์มหาวิทยาลัย เมื่อปีการศึกษา 2549 และเข้าศึกษาต่อในหลักสูตรวิศวกรรมศาตรมหาบัณฑิตในปีการศึกษาถัดมา ณ ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย สังกัดห้องปฏิบัติการวิจัยโทรคมนาคม