การประยุกต์ทฤษฎีเกมในการวิเคราะห์ความปลอดภัยของการจัดเส้นทางแบบเฟ้นสุ่มในโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทาง

นายภัทร บุญญกาญจน์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

Game Theoretical Application in Security Analysis of Stochastic Routing in Wireless Mesh Network with Directional Antenna

Mr.Pat Boonyakarn

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 2010

หัวข้อวิทยานิพนธ์	การประยุกต์ทฤษฎีเกมในการวิเคราะห์ความปลอดภัยของการจัดเส้นทางแบบเฟ้นสุ่มในโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทาง
โดย	นายภัทร บุญญกาญจน์
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. วัสกา วิสุทธิวิเศษ)

ภัทร บุญญกาญจน์ : การประยุกต์ทฤษฎีเกมในการวิเคราะห์ความปลอดภัยของการจัดเส้นทางแบบเฟ้นสุ่มในโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทาง (Game Theoretical Application in Security Analysis of Stochastic Routing in Wireless Mesh Network with Directional Antenna) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : ผศ. ดร. เชาวน์ดิศ อัศวกุล, 53 หน้า.

ในวิทยานิพนธ์นี้ได้เสนอระเบียบวิธีการจัดหาเส้นทางแบบเฟ้นสุ่มเพื่อป้องกันการดักฟังและส่งสัญญาณรบกวนข้อมูลในโครงข่ายไร้สายแบบเมชด้วยสายอากาศระบุทิศทางที่ใช้โมเดลแบบโคน โดยทฤษฎีเกมได้สามารถหารูปแบบเส้นทางแบบเฟ้นสุ่มที่ดีที่สุดที่ทำให้ค่าความคาดหวังของจำนวนเซสชั่นที่ปลอดภัย (expected number of secure sessions: ESS) สูงที่สุดภายใต้สถานการณ์ที่โครงข่ายถูกโจมตีอย่างร้ายแรงได้ ในวิทยานิพนธ์นี้ได้จำลองเกมโครงข่ายไร้สายแบบเมชเป็นแบบเกมเล่นสองคนที่มีผลรวมเป็นศูนย์ โดยผู้เล่นสองคนแบ่งเป็น ผู้เล่นฝ่ายป้องกันโครงข่ายและผู้เล่นฝ่ายที่มาโจมตีโครงข่าย ซึ่งผู้เล่นฝ่ายป้องกันทำหน้าที่เลือกรูปแบบการส่งข้อมูลแบบทรีด้วยความน่าจะเป็นค่าต่าง ๆ เพื่อให้ค่า ESS มีค่ามากที่สุด ในทางกลับกันผู้เล่นฝ่ายโจมตีจะเลือกตำแหน่งในการโจมตีด้วยความน่าจะเป็นค่าต่าง ๆ เพื่อให้ค่า ESS ต่ำที่สุด จากการหาผลเฉลยทำให้ค่าของเกมนั้นสามารถการันตีจำนวนเซสชั่นที่ปลอดภัยเสมอได้ไม่ว่าผู้โจมตีจะโจมตีแบบใด จากผลการทดลองแสดงให้เห็นว่าการใช้สายอากาศระบุทิศทางทำให้ค่า ESS สูงกว่าในกรณีที่ใช้สายอากาศรอบทิศทางเสมอในแบบจำลองเดียวกัน ยิ่งไปกว่านั้นการลดค่าบีมวิดท์ของสายอากาศระบุทิศทางในการดักฟังข้อมูลสามารถเพิ่มค่า ESS เฉพาะกรณีของการส่งข้อมูลฝั่งขาลงเท่านั้นและโครงข่ายจะต้องมีขนาดไม่เล็กจนเกินไป ในทางกลับกันกรณีการส่งข้อมูลฝั่งขาขึ้นถ้าต้องการจะเพิ่ม ESS จะต้องเพิ่มจำนวนเกตเวย์แทน และจากผลการทดลองของโครงข่ายสุ่มแสดงให้เห็นว่ากรณีการส่งข้อมูลฝั่งขาขึ้นนั้นจะถูกโจมตีได้ร้ายแรงกว่าฝั่งขาลง ซึ่งจากการวิเคราะห์ค่าชี้วัด ESS นี้จะเป็นประโยชน์ในการออกแบบโครงข่ายไร้สายแบบเมชที่มีความทนทานต่อการถูกโจมตีได้ในอนาคต

ภาควิชา	วิศวกรรมไฟฟ้า	**ลายมือชื่อนิสิต**	.....
สาขาวิชา	วิศวกรรมไฟฟ้า	**ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนธ์หลัก**	.....
ปีการศึกษา	2553		

5270683721 : MAJOR ELECTRICAL ENGINEERING
KEYWORDS: WIRELESS MESH NETWORK (WMN)/ GAME THEORY/ STOCHASTIC ROUTING/ INTELLIGENT EAVESDROPPING AND JAMMING/ DIRECTIONAL ANTENNA/.

PAT BOONYAKARN : GAME THEORETICAL APPLICATION IN SECURITY ANALYSIS OF STOCHASTIC ROUTING IN WIRELESS MESH NETWORK WITH DIRECTIONAL ANTENNA . ADVISOR: ASST. PROF. CHAODIT ASWAKUL, Ph.D., 53 pp.

This thesis is concerned with the framework for finding the optimal stochastic routing to defend intelligent eavesdropping and jamming attacks in the Wireless Mesh Network (WMN) with a cone-based, directional antenna. A game-theoretical model is used to find the best strategy to maximize the expected number of secure sessions (*ESS*) under the most severe circumstance. In particular, the WMN has been modeled by the two-person zero-sum game with two players, namely, a network defender and a network attacker. The defender tries to maximize *ESS* by assigning the best selection probabilities to the tree patterns for forwarding data to and from gateways. The attacker tries to minimize *ESS* by assigning the best selection probabilities to the positioning of attacker. In this regard, the obtained value of game represents the minimum guarantee on the number of secure sessions at the defender optimality in WMNs under any attacks. Numerical results show that using directional antenna can lead to higher ESS values when compared to the corresponding cases with only the omni-directional antenna capability. The enhancement of antenna directionality by decreasing the beamwidth can help improve ESS in the sufficiently large network case of downlink. On the contrary, in the case of uplink, the increasing number of gateways will add to the improvement of ESS. In addition, based on reported numerical results on both deterministic and random topologies, the uplink loading case can be attacked more severely than in the downlink case. The analyzed ESS here would benefit the design of WMN in terms of robustness.

Department	:	Electrical Engineering	**Student's Signature**	.....
Field of Study	:	Electrical Engineering	**Advisor's Signature**	.....
Academic Year	:	2010		

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่ง จากอาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ. ดร.เชาวน์ดิศ อัศวกุล ซึ่งได้ให้ความรู้และคำแนะนำอันมีค่ายิ่งต่อผู้วิจัย อีกทั้งตรวจทานงานวิทยานิพนธ์ฉบับนี้ด้วยดีเสมอมา ผู้วิจัยจึงขอกราบขอบพระคุณมา ณ ที่นี้

ขอขอบคุณกลุ่มวิจัยโครงข่าย (Network Reserch Group) ซึ่งดูแลโดย ผศ. ดร. เชาวน์ดิศ อัศวกุล และ ผศ. ดร. ชัยเชษฐ์ สายวิจิตร ที่จัดกิจกรรมเพื่อส่งเสริมการเรียนรู้และการทำงานของผู้วิจัยให้มีประสิทธิภาพที่ดียิ่งขึ้น รวมถึงให้ความอนุเคราะห์อุปกรณ์เครื่องมือในการทำงานแก่ผู้วิจัย ทำให้งานวิทยานิพนธ์นี้สำเร็จได้อย่างสะดวกราบรื่น

ขอขอบคุณโครงการ GE12 และทุนศิษย์ก้นกุฏิของภาควิชาวิศวกรรมไฟฟ้า จุฬาลงกรณ์มหาวิทยาลัย รวมถึงโครงการ TRIDI CE in Lightwave and high-speed Communications at EeDept CU ที่สนับสนุนด้านทุนการศึกษาวิจัยและคุรุพัฒน์

ขอขอบคุณอาจารย์ภัทรชาติ โกมลกิติ ผู้คอยให้คำแนะนำ ข้อคิดเห็นต่างๆ อันเป็นประโยชน์ต่องานวิทยานิพนธ์นี้ด้วยดีเสมอมา

ขอบคุณเพื่อนพี่น้องนักวิจัยทุกคน รวมถึงเจ้าหน้าที่ บุคลากรที่อยู่ในภาควิชาไฟฟ้า สาขาโทรคมนาคม จุฬาลงกรณ์มหาวิทยาลัย ที่ได้ให้ความช่วยเหลือในเรื่องต่าง ๆ และเป็นกำลังใจที่ดียิ่งต่อผู้วิจัย

สุดท้ายนี้ขอขอบคุณครอบครัวของผู้วิจัย ซึ่งได้ให้การสนับสนุนและเป็นกำลังใจให้แก่ผู้วิจัยเสมอมาจนสำเร็จการศึกษา

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

หน้า

สารบัญตัวย่อ

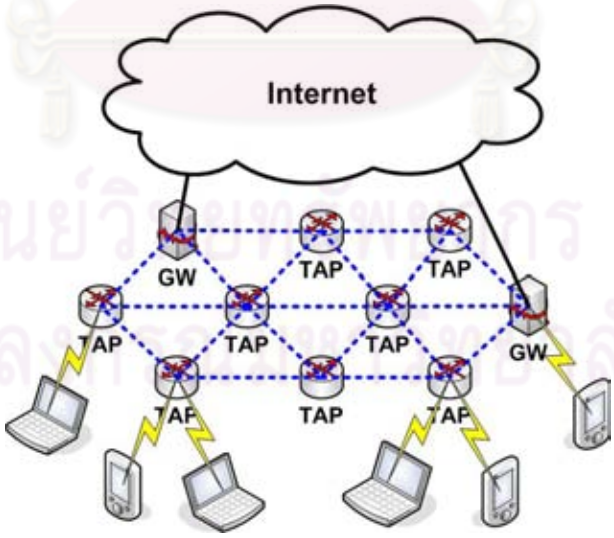
WMN	wireless mesh network
GW	gateway
TAP	transit access point
ESS	expected number of secure sessions
BW	beamwidth
MSA	method of successive average

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันโครงข่ายไร้สายแบบเมช (wireless mesh network: WMN) กำลังเป็นที่ได้รับความสนใจจากทั้งผู้ให้บริการโครงข่ายและกลุ่มนักวิจัย เนื่องจากมีข้อดีมากมายเมื่อเทียบกับโครงข่ายไร้สายชนิดอื่น ๆ โดยโครงข่ายไร้สายแบบเมชจะประกอบด้วยโนด (node) ที่ต่อถึงกันผ่านตัวกลางไร้สายในรูปแบบของเมช และใช้วิธีการส่งข้อมูลผ่านโนดข้างเคียง (neighbor node) ในลักษณะหลายช่วงเชื่อมต่อ (multi-hop) ทำให้มีความยืดหยุ่นในการส่งสูงและไม่ต้องถูกควบคุมจากส่วนกลาง โดยสามารถจัดโครงข่ายไร้สายแบบเมชเป็นกรณีเฉพาะของโครงข่ายแอดฮอก (ad hoc networks) ที่โนดทั้งหมดไม่มีการเคลื่อนที่ได้ การใช้งานของโครงข่ายไร้สายแบบเมชนั้นสามารถใช้ได้หลากหลายเนื่องจากมีรัศมีในการส่งครอบคลุมพื้นที่เป็นบริเวณกว้างและทั่วถึงจึงเหมาะสำหรับเป็นตัวรับส่งข้อมูลของผู้ใช้บริการแต่ละพื้นที่โดยผู้ใช้บริการอาจจะเคลื่อนที่ผ่านจุดต่าง ๆ แต่ก็ยังอยู่ในรัศมีการส่งของโครงข่าย ตัวอย่างเช่น การให้บริการอินเทอร์เน็ตไร้สาย โครงข่ายไร้สายแบบเมชแตกต่างจากโครงข่าย WiFi ทั่วไปตรงที่การส่งข้อมูลจากช่วงเชื่อมต่อเดียว (single hop) มาเป็นหลายช่วงเชื่อมต่อ โดยโครงข่ายไร้สายแบบเมชนั้นจะติดต่อกับโครงข่ายอินเทอร์เน็ตภายนอกผ่านเกตเวย์ (gate-way) และจุดเชื่อมต่อ (transit access point: TAP) อื่น ๆ ในโครงข่ายดังรูปที่ 1.1



รูปที่ 1.1: โครงข่ายไร้สายแบบเมชเพื่อให้บริการเชื่อมต่อระบบอินเทอร์เน็ตแบบไร้สาย

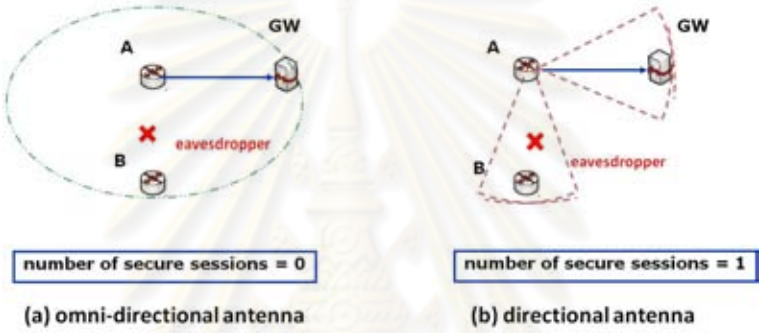
เนื่องจากเป็นการส่งแบบโครงข่ายแอดฮอกทำให้ใช้ตัวกลางไร้สายเป็นตัวส่งข้อมูล จึงติดตั้งง่าย รวดเร็ว รวมทั้งประหยัดต้นทุนเนื่องจากไม่ต้องมีการวางสายและค่าบำรุงซ่อมแซมสาย ยิ่งไปกว่านั้นยังมีความน่าเชื่อถือ (reliability) สูง เนื่องจากรูปแบบของโครงข่าย

เป็นแบบเมช มีความยืดหยุ่นหรือปรับขนาดได้ง่าย (scalability) และยังสามารถใช้ได้กับเทคโนโลยีที่มีมาก่อนเช่น IEEE 802.11 [1], IEEE 802.16 [2] เป็นต้น ทำให้ผู้ให้บริการโครงข่ายนำโครงข่ายไร้สายแบบเมชมาใช้กันมากขึ้น [3] เช่น โครงข่ายเชื่อมต่อภายในชุมชน (community networking), ภายในบ้าน (broadband home networking), ภายในองค์กร (enterprise networking) และโครงข่ายในตึกอัจฉริยะ (building automation) เป็นต้น นอกจากการเชื่อมต่ออินเทอร์เน็ตแบบไร้สายแล้ว โครงข่ายไร้สายแบบเมชสามารถนำมาใช้งานในลักษณะแบบแยกเดี่ยว (stand alone) เนื่องจากใช้ระยะเวลาในการติดตั้งไม่นานจึงเหมาะสมกับการใช้งานในสถานการณ์ฉุกเฉินต่าง ๆ เช่น การช่วยเหลือผู้ประสบภัยพิบัติ (disaster recovery) [4] การใช้งานเป็นโครงข่ายทางทหารทั้งการรบภาคสนามและการซ้อมรบ [5] เป็นต้น

ถึงแม้ว่าโครงข่ายไร้สายแบบเมชจะมีข้อดีมากมายก็ตามแต่ก็มีข้อเสียอยู่หลายประการเช่นกัน ได้แก่ ปัญหาขีดจำกัดของความจุในการส่งข้อมูล (capacity constraint) ปัญหาค่าประวิงของการส่งข้อมูล (delay constraint) อันเนื่องจากการส่งผ่านตัวกลางไร้สาย มีงานวิจัยมากมายที่พยายามจะเพิ่มประสิทธิภาพของโครงข่ายไร้สายแบบเมช [6], [7], [8], [9], [10] แต่ยังมีปัญหาสำคัญอีกปัญหาหนึ่งที่ทำให้โครงข่ายไร้สายแบบเมชไม่แพร่หลายในปัจจุบันเท่าที่ควรนั่นคือปัญหาด้านความปลอดภัย โดยปกติแล้วการติดต่อผ่านตัวกลางไร้สายจะมีความสามารถในการป้องกันต่อการถูกโจมตีต่ำกว่าโครงข่ายที่ใช้สายสื่อสาร (wired network) เนื่องจากโครงข่ายไร้สายแบบเมชมีโครงข่ายแกนกลาง (backbone network) เป็นตัวกลางไร้สายทั้งหมดจึงทำให้ข้อมูลสำคัญต่าง ๆ ของผู้ใช้งานโครงข่าย เช่น รหัสเครดิตการ์ด รหัสอีเมล์ หรือข้อมูลสำคัญที่เป็นความลับอื่น ๆ ซึ่งล้วนถูกส่งผ่านตัวกลางไร้สายนั้นจะถูกดักฟัง (eavesdropping) ได้ง่าย ยิ่งไปกว่านั้นโครงสร้างไร้สายแบบเมชยังง่ายต่อการถูกโจมตีด้วยสัญญาณรบกวน (jamming) โดยการโจมตีนี้จะทำให้การรับ/ส่งข้อมูลของจุดเชื่อมต่อที่อยู่ภายในพื้นที่ครอบคลุม (coverage area) ของผู้โจมตีไม่สามารถทำได้และนำไปสู่ภาวะที่ผู้ใช้งานไม่สามารถติดต่อสื่อสารผ่านโครงข่ายได้ตามปกติ (denial of service, DoS) และเนื่องจากสัญญาณรบกวนที่มาจากปัจจัยอื่นมีมากมายทำให้ยากต่อการตรวจจับหรือรู้ตำแหน่งทิศทางของผู้โจมตี ดังนั้นปัญหาที่เกิดจากทั้งการถูกดักฟังและการส่งสัญญาณรบกวนจากผู้โจมตีจึงเป็นปัญหาที่ไม่อาจมองข้ามและยังต้องการการป้องกันที่เหมาะสมกับโครงข่ายไร้สายแบบเมช

ด้วยเหตุนี้เองจึงได้มีงานวิจัยที่จะแก้ปัญหาเรื่องความปลอดภัยในโครงข่ายไร้สายแบบเมช [11],[12],[13],[14] โดยเฉพาะในงานวิจัย [14] ซึ่งได้นำทฤษฎีเกมมาประยุกต์เข้ากับการจัดเส้นทางแบบเฟ้นสุ่ม (stochastic routing) ในงานวิจัยนั้นได้แบ่งผู้เล่นออกเป็น 2 ฝ่าย คือ ผู้เล่นฝ่ายป้องกันโครงข่าย และผู้เล่นฝ่ายโจมตี ซึ่งแผนการเล่นของผู้เล่นฝ่ายป้องกันจะเป็นการจัดเส้นทางเฟ้นสุ่มในรูปแบบของทรี โดยมีเป้าหมายเพื่อให้ลดจำนวนโนดที่ส่งข้อมูลแล้วถูกดักฟังหรือรบกวนสัญญาณให้มีน้อยที่สุด ส่วนแผนการเล่นของผู้เล่นฝ่ายโจมตีคือการเลือกพื้นที่ต่าง ๆ ในโครงข่ายที่จะดักฟังหรือรบกวนสัญญาณโดยเป้าหมายเพื่อให้เพิ่มจำนวนโนดที่ส่งข้อมูลแล้วถูกดักฟังหรือรบกวนสัญญาณให้มีมากที่สุด เมื่อหาผลเฉลยของเกมแล้วจะได้ค่าของเกมเป็นค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตี (expected number of secure sessions: ESS) และแผนการที่ดีที่สุดของทั้งผู้เล่นฝ่าย

ป้องกันและผู้เล่นฝ่ายโจมตี ทำให้สามารถหาจำนวนเซสชั่นที่ปลอดภัยในกรณีที่ถูกโจมตีร้ายแรงที่สุดได้ แต่ในงานวิจัยที่กล่าวมาเป็นการจำลองโดยให้โนดทุกตัวใช้สายอากาศรอบทิศทาง (omni–directional antenna) ซึ่งมีข้อดีในด้านของรัศมีการส่งที่ครอบคลุมแต่ในด้านของความปลอดภัยแล้วกลับพบว่าการที่รัศมีการส่งที่ครอบคลุมนั้น ทำให้เพิ่มพื้นที่ที่ผู้โจมตีจะสามารถโจมตีจุดที่อยู่ในรัศมีครอบคลุมจำนวนโนดได้มากขึ้น ในวิทยานิพนธ์นี้จึงได้นำสายอากาศระบุทิศทาง (directional Antenna) มาประยุกต์ใช้เพื่อเพิ่มค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตี (ESS) สิ่งที่แตกต่างกันระหว่างสายอากาศรอบทิศทางกับสายอากาศระบุทิศทางในการส่งข้อมูลแสดงในรูปที่ 1.2



รูปที่ 1.2: การส่งข้อมูลของสายอากาศรอบทิศทางและสายอากาศระบุทิศทาง

จากรูปที่ 1.2(a) จะเห็นได้ว่าโนด A ต้องการส่งข้อมูลไปยังเกตเวย์จึงทำการส่งข้อมูลออกมาในรัศมีการส่ง ปรากฏว่าผู้โจมตีที่ดักรออยู่ที่ตำแหน่งระหว่างโนด A และ B อยู่ในรัศมีการส่งของโนด A ด้วยทั้ง ๆ ที่โนด A ไม่ได้ตั้งใจจะส่งข้อมูลไปยังโนด B จึงทำให้กรณีนี้ทั้งโนด A และโนด B ถูกโจมตีทั้งคู่จำนวนเซสชั่นที่ปลอดภัยจึงมีค่าเท่ากับศูนย์ ในทางกลับกันจากรูปที่ 1.2(b) ได้ใช้สายอากาศระบุทิศทางแทนเมื่อพิจารณาจากโครงข่าย โนด A มีจุดหมายปลายทางสองจุดคือไปยังเกตเวย์และโนด B จึงมีสองบีม (beam) ในการเลือกส่งบีมแรกคือลำบีมที่พุ่งไปยังเกตเวย์ และบีมที่สองคือพุ่งลงมายังโนด B โดยจะถือว่าสายอากาศระบุทิศทางเป็นแบบสวิทซ์บีม (beam–switching antenna) เมื่อโนด A ต้องการส่งข้อมูลไปยังเกตเวย์ จึงทำการเปิดบีมในทิศที่พุ่งไปยังเกตเวย์เท่านั้น โดยที่ปิดบีมที่พุ่งลงมายังโนด B ทำให้ผู้โจมตีที่อยู่ระหว่างโนด A และ โนด B ไม่สามารถโจมตีข้อมูลที่โนด A ส่งไปยังเกตเวย์ได้ ทำให้จำนวนเซสชั่นที่ปลอดภัยมีค่าเป็นหนึ่ง

จากที่กล่าวมาทำให้เห็นประโยชน์ของสายอากาศระบุทิศทางในการเพิ่มความปลอดภัยให้กับโครงข่าย ซึ่งจากการศึกษางานวิจัย [9], [10], [13] เป็นการนำสายอากาศระบุทิศทางมาใช้กับโครงข่ายไร้สายแบบเมช โดยในงานวิจัย [9] เป็นการออกแบบการเชื่อมโยงโดยใช้ความสามารถของสายอากาศระบุทิศทางทำให้จุดเชื่อมต่อแต่ละจุดมีรัศมีในการส่งไกลขึ้นโดยทำให้โครงข่ายมีความยืดหยุ่นและเพิ่มประสิทธิภาพให้กับโครงข่าย ในงานวิจัยที่ [13] เป็นการป้องกันผู้โจมตีโดยการเพิ่มกำลังในการส่งแข่งกับผู้โจมตีและลดความกว้างของบีมวิดท์ด้วยสายอากาศระบุทิศทางทำให้มุมในการส่งแคบลงจนผู้โจมตีมีโอกาสที่จะโจมตีได้น้อยลง

ส่วนในงานที่ [10] เป็นการเสนออัลกอริธึมเพื่อหาค่าบีมวิทด์ที่เหมาะสมให้กับโนดทุกโนด เป้าหมายเพื่อลดการกวนกันของสัญญาณ (interference) ซึ่งสุดท้ายจะได้ค่าบีมวิทด์ที่มากที่สุดโดยที่ไม่เกิดการกวนกันของสัญญาณของแต่ละโนด โดยคำนึงถึงค่าต้นทุนในการติดตั้งสายอากาศ ยิ่งบีมวิทด์มีค่าน้อยจะมีต้นทุนแพงกว่าบีมวิทด์ที่มีค่ามากเพราะจำนวนบีมที่ต้องติดตั้งจะมากกว่าเพื่อให้ทิศทางในการส่งครอบคลุมทุกทิศทาง

ในวิทยานิพนธ์นี้ได้นำสายอากาศระบุทิศทางมาประยุกต์ใช้โดยวิธีการแบ่งค่าบีมวิทด์ที่เหมาะสมรวมถึงการคำนวณค่าต้นทุนในการติดตั้งจากงานวิจัย [10] มาประยุกต์เข้ากับงานวิจัย [14] การจัดเส้นทางแบบเฟ้นสุ่มโดยใช้ทฤษฎีเกมแก้ปัญหาที่เกิดจากทั้งการดักฟังและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมช โดยผลเฉลยของเกมจะสามารถบ่งชี้ออกมาได้ว่าโครงข่ายใดมีความปลอดภัยมากที่สุด ซึ่งคิดจากกรณีที่ถูกโจมตีร้ายแรงที่สุดแล้วยังสามารถรับประกันจำนวนเซสชั่นที่ปลอดภัย รวมไปถึงวิธีการส่งข้อมูลที่ดีที่สุดได้โดยได้นำเสนอสมการในการวิเคราะห์ปัญหา โดยใช้แบบจำลองของสายอากาศระบุทิศทางและในวิทยานิพนธ์ฉบับนี้ได้จำลองลักษณะการดักฟังข้อมูลของผู้โจมตีให้ขึ้นกับตำแหน่งของผู้โจมตีว่าอยู่ในพื้นที่ครอบคลุมของจุดเชื่อมต่อใดบ้าง จากนั้นในส่วนท้ายของวิทยานิพนธ์ได้ชี้ให้เห็นถึงความสัมพันธ์และความแตกต่างของการโจมตีทั้งสองแบบ คือ การดักฟังข้อมูลและการส่งสัญญาณรบกวนรวมไปถึงค่าต้นทุนที่ใช้ในการติดตั้งโครงข่ายเพื่อให้ได้การจัดเส้นทางที่เหมาะสมกับการโจมตีในแต่ละแบบต่อไป

1.2 วัตถุประสงค์

เพื่อ เสนอ วิธีการ คำนวณ หา รูปแบบ การ จัด เส้นทาง การ ส่ง ข้อมูล ที่ เหมาะสม สำหรับโครงข่ายไร้สายแบบเมช เพื่อป้องกันการดักฟังและส่งสัญญาณรบกวน โดยใช้สายอากาศระบุทิศทางและประยุกต์ทฤษฎีเกมเข้ากับวิธีการจัดเส้นทางเฟ้นสุ่ม

1.3 ขอบเขตของวิทยานิพนธ์

1. นำเสนอ ระเบียบวิธี การ คำนวณ หา รูปแบบ การ จัด เส้นทาง การ ส่ง ข้อมูล ที่ เหมาะสม สำหรับการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่ายไร้สายแบบเมช เพื่อป้องกันการดักฟังและการส่งสัญญาณรบกวน โดยประยุกต์ทฤษฎีเกมเข้ากับวิธีการจัดเส้นทางแบบเฟ้นสุ่ม

2. ในวิทยานิพนธ์นี้ไม่ได้พิจารณากรณีที่จุดเชื่อมต่อมีการระบุการเชื่อมต่อกับเกตเวย์ใดเกตเวย์หนึ่งโดยเฉพาะ

3. ระเบียบวิธีการคำนวณหารูปแบบการป้องกันที่เหมาะสมที่ได้นำเสนอนั้น สามารถนำไปใช้ ในกรณีที่มีจำนวนผู้โจมตีมากกว่าหนึ่งคนได้ แต่ในวิทยานิพนธ์นี้จะศึกษาในกรณีที่มีผู้โจมตีเพียงหนึ่งคนเท่านั้น

4. ในวิทยานิพนธ์นี้ไม่ได้หาค่าบีมวิดท์ที่ทำให้ค่าคาดหวังของเซสชั่นที่ปลอดภัยสูงที่สุด

ซึ่งในการทดสอบเบื้องต้นในข้อเสนอวิทยานิพนธ์นี้ได้ทดสอบแบบกำหนดค่าบีมวิดท์ทุกโนดเท่ากันและภายหลังจะทดสอบกับการแบ่งค่าบีมวิดท์แต่ละโนดอย่างเหมาะสม โดยการเลือกบีมวิดท์ที่กว้างที่สุดที่ไม่ทำให้พื้นที่ครอลคลุมการส่งของบีมที่มาจากโนดต้นทางเดียวกันซ้อนทับกัน [10]

5. ในวิทยานิพนธ์นี้พิจารณาผู้โจมตีที่ใช้สายอากาศระบุทิศทางซึ่งมีโมเดลสายอากาศเป็นแบบโคนนั่นคือให้ค่าอัตราขยายของสายอากาศคงที่ในบีมของการรับส่งและค่าอัตราขยายเป็นศูนย์นอกบีมของสายอากาศและกำหนดให้ผู้โจมตีใช้สายอากาศรอบทิศทางเท่านั้น ทั้งในกรณีการดักฟังและการส่งสัญญาณรบกวน และกำหนดให้รัศมีของสัญญาณรบกวนมีค่าเท่ากับรัศมีของการส่งในแต่ละโนด

6. โครงข่ายไร้สายแบบเมชที่นำมาพิจารณานั้นถือว่าเป็นโครงข่ายในอุดมคติ คือ การส่งข้อมูลไม่มีโอกาสเกิดความผิดพลาดจากการส่ง เช่น ข้อมูลหายระหว่างการส่งและวางอยู่ในพื้นที่แนวราบที่ไม่มีสิ่งกีดขวางใดๆ

7. ในเบื้องต้นวิทยานิพนธ์นี้ได้ทดสอบกับโครงข่ายแบบตารางและจะทดสอบในโครงข่ายที่เกิดจากการสุ่มขึ้นมาในรูปแบบต่าง ๆ โดยใช้ Waxman Topology generator [15]–[17] ต่อไป ซึ่งเป็นการเชื่อมต่ออย่างง่ายที่สามารถครอบคลุมพื้นที่ให้บริการได้ทั่วถึง

1.4 ขั้นตอนการดำเนินงาน

1. ศึกษางานวิจัยที่เกี่ยวข้องและทฤษฎีเกม
2. สร้างแบบจำลองทางคณิตศาสตร์สำหรับแก้ปัญหาที่พิจารณา
3. สร้างแบบจำลองด้วยโปรแกรม MATLAB®เพื่อใช้ทดสอบวิธีที่เสนอ
4. สรุปผลการทดลองและวิเคราะห์ผล
5. เขียนบทความทางวิชาการและส่งตีพิมพ์
6. จัดทำวิทยานิพนธ์ฉบับสมบูรณ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

เพื่อที่จะได้วิธีการป้องกันการดักฟังและรบกวนสัญญาณของโครงข่ายไร้สายแบบเมช โดยใช้การจัดเส้นทางเฟ้นสุ่มเพื่อหลีกเลี่ยงการโจมตีที่ร้ายแรงที่สุดได้ ด้วยทฤษฎีเกมทำให้สามารถรับประกันค่าจำนวนเซสชั่นที่ปลอดภัย ยิ่งไปกว่านั้นยังประยุกต์การใช้สายอากาศระบุทิศทางมาเพื่อเพิ่มความปลอดภัยกับโครงข่ายมากยิ่งขึ้น

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 ทฤษฎีเกม

ทฤษฎีเกม [18] คือ ทฤษฎีซึ่งนำเสนอวิธีการคำนวณผลได้ผลเสียของการแข่งขันที่มีจำนวนผู้เล่นตั้งแต่สองคนขึ้นไป โดยคำนึงถึงการตัดสินใจของผู้เล่นทุกฝ่าย โดยทุกรอบการแข่งขันผู้เล่นในแต่ละฝ่ายจะคำนึงถึงการเล่นเพื่อให้ได้ผลประโยชน์กับตนเองมากที่สุด ซึ่งผลลัพธ์ที่ได้อาจจะเกิดจากผู้เล่นแต่ละฝ่ายพยายามโจมตีผู้เล่นฝ่ายตรงข้ามให้ได้มากที่สุด (non–cooperative game) หรือ ทุกฝ่ายต่างร่วมมือกันเพื่อให้ได้ผลประโยชน์ตอบแทนมากที่สุด (cooperative game) โดยแผนการเล่นจะมีสองแบบ ดังนี้

1. แผนการเล่นแบบบริสุทธิ์ (pure strategy) : ในแต่ละรอบของการแข่งขัน ผู้เล่นแต่ละคนจะมีแผนการเล่นเด่น (dominant strategy) ทำให้เลือกแผนการเล่นนั้น ๆ มาเล่นและใช้แผนเดิมกับทุกรอบของเกม

2. แผนการเล่นแบบผสม (mix strategies) : ในแต่ละรอบของการแข่งขัน ผู้เล่นแต่ละคนจะสุ่มแผนขึ้นมาเล่น โดยขึ้นกับการแจกแจงความน่าจะเป็น ซึ่งจะแตกต่างจากกรณีแผนการเล่นบริสุทธิ์ตรงที่ผู้เล่นแต่ละคนเลือกแผนมากกว่า 1 แผนในการเล่น

2.1.1 เกมเล่นสองคนที่มีผลรวมเป็นศูนย์ (two–person zero–sum game)

หมายถึง เกมในรูปแบบที่มีผู้เล่นสองคน โดยผลประโยชน์ที่ทั้งสองคนได้รับจะรวมกันเป็นศูนย์เสมอหรือกล่าวอีกนัยได้ว่า ถ้ามีผู้เล่นได้ผลตอบแทนมาเท่าไหร่ผู้เล่นอีกฝ่ายจะเสียไปเท่านั้น ซึ่งเกมในลักษณะนี้เป็นเกมที่ขัดแย้งกันระหว่างผู้เล่นอย่างชัดเจน ตัวอย่างเช่น หมากรุก เกมโยนเหรียญ เป็นต้น โดยปกติแล้วเกมเล่นสองคนที่มีผลรวมเป็นศูนย์นั้น จะแสดงผลได้ผลเสียด้วยตาราง ซึ่งเรียกว่า ตารางผลได้ผลเสีย (payoff table) ดังตัวอย่างในตารางที่ 2.1

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

รูปที่ 2.1: ตัวอย่างตารางผลได้ผลเสีย

ตารางที่ 2.1 แสดงถึงค่าผลได้ผลเสียระหว่างผู้เล่นทั้งสองคน โดยผู้เล่นคนที่หนึ่ง (แนวแถว) มีสองแผน ได้แก่ แผน x และ y ส่วนผู้เล่นคนที่สอง (แนวหลัก) มีสองแผนเช่นกัน

ได้แก่ a และ b โดยค่าตัวเลขในตารางหมายถึงค่าผลได้เสียของผู้เล่นคนที่หนึ่ง ยกตัวอย่าง เช่น หากผู้เล่นคนที่หนึ่งเลือกแผน y และผู้เล่นคนที่สองเลือกแผน a ค่าที่ได้จากตารางจะเป็น 2 ซึ่งหมายความว่าผู้เล่นคนที่หนึ่งจะได้ผลประโยชน์ 2 หน่วย แต่ในทางกลับกันผู้เล่นคนที่สองจะเสียผลประโยชน์ 2 หน่วย แต่ถ้าผู้เล่นคนที่หนึ่งเลือกแผน x และผู้เล่นคนที่สองเลือกแผน a จะได้ค่าเท่ากับ -2 หมายความว่าผู้เล่นคนที่หนึ่งจะเสียผลประโยชน์ 2 หน่วย แต่ในทางกลับกันผู้เล่นคนที่สองจะได้ผลประโยชน์ 2 หน่วย

2.1.2 ทฤษฎีมินิแมกซ์ (minimax theorem)

จากเกมเล่นสองคนที่มีผลรวมเป็นศูนย์ที่กล่าวไปข้นต้น หากผู้เล่นทั้งสองคนมีแผนของการเล่นเป็นเซตจำกัดแล้ว จะเรียกเกมประเภทนี้ว่า เกมเล่นสองคนที่มีผลรวมเป็นศูนย์แบบจำกัด (finite two–person zero–sum game) ซึ่งเกมประเภทนี้จะสามารถหาผลเฉลยของเกมได้โดยทฤษฎีมินิแมกซ์ [18] จากทฤษฎีกล่าวไว้ว่าถ้าเกมเล่นสองคนที่มีผลรวมเป็นศูนย์เป็นแบบจำกัดแล้ว

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

2. จะมีแผนการเล่นแบบผสมสำหรับผู้เล่นคนที่หนึ่งซึ่งทำให้ได้รับประโยชน์โดยเฉลี่ยอย่างน้อยที่สุดเท่ากับค่า V ไม่ว่าผู้เล่นคนที่สองจะเลือกแผนการเล่นแบบไหนก็ตาม ซึ่งแผนของผู้เล่นคนที่หนึ่งเป็นการหาค่ามากที่สุดจากผลได้น้อยที่สุด

3. จะมีแผนการเล่นแบบผสมสำหรับผู้เล่นคนที่สองซึ่งทำให้ผู้เล่นคนที่สองเสียผลประโยชน์โดยเฉลี่ยอย่างมากที่สุดเท่ากับ V ไม่ว่าผู้เล่นคนที่หนึ่งจะเลือกแผนการเล่นแบบไหนก็ตาม ซึ่งแผนของผู้เล่นคนที่สองเป็นการหาค่าน้อยที่สุดจากผลเสียมากที่สุด

จากที่กล่าวมาจะเห็นได้ว่าเกมเล่นสองคนที่มีผลรวมเป็นศูนย์ทุกเกมนั้นจะสามารถหาค่าของเกมได้ซึ่งจะสอดคล้องกับแผนของผู้เล่นคนที่หนึ่งและสองที่ทำให้ได้ค่าที่พอใจในผลได้ผลเสียทั้งสองฝ่าย โดยแผนที่ทั้งคู่เลือกมาเล่นนี้จะเรียกว่าแผนการเล่นแบบมินิแมกซ์หรือแผนการเล่นที่เหมาะสมที่สุด (optimal strategy)

2.1.3 แผนการเล่นเด่น (dominant strategy)

จากนิยาม [18] กล่าวว่าแผนการเล่น S จะเป็นแผนการเด่นกว่าแผนการเล่น T ก็ต่อเมื่อทุก ๆ ค่าของผลได้เสียใน S ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้ามมีค่าผลได้ผลเสียที่ดีกว่าหรือเท่ากับค่าผลได้ผลเสียใน T ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้าม ซึ่งกลยุทธ์เด่นนั้นสามารถแบ่งออกเป็น 2 รูปแบบคือ

1. แผนการเล่นเด่นอย่างชัดเจน (strictly dominant)

ถ้าแผนการเล่น S เด่นกว่าแผนการเล่น T อย่างชัดเจนแล้ว ทุก ๆ ค่าของผลได้ผลเสียใน S ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้ามจะมีค่าผลได้ผลเสียดีกว่าค่าผลได้ผลเสียใน T ที่ได้จากแผนการเล่นของผู้เล่นฝ่ายตรงข้าม

2. แผนการเล่นไม่ด้อยกว่า (weakly dominant)

หากแผนการเล่น S ไม่ด้อยกว่าแผนการเล่น T แล้ว จะมีอย่างน้อยหนึ่งค่าของผลได้ผลเสียใน S ที่ได้จากแผนการการเล่นของผู้เล่นฝ่ายตรงข้ามมีค่าผลได้ผลเสียที่ดีกว่าค่าของผลได้ผลเสียใน 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: ตัวอย่างตารางผลได้ผลเสียเพื่อแสดงแผนการเล่นเด่นของผู้เล่นทั้งสอง

เนื่องจากค่าในตารางเป็นค่าผลได้ผลเสียของผู้เล่นแนวแถว (ผู้เล่น 1) ดังนั้นค่าผลได้ผลเสียที่ดีกว่าสำหรับผู้เล่น 1 จะหมายถึง ค่าผลได้ผลเสียที่มากกว่านั้นเอง จากตัวอย่างจะเห็นว่าแผนการเล่น x นั้นเป็นแผนการเล่นที่เด่นกว่าแผนการเล่น w อย่างชัดเจน เนื่องจากค่าผลได้ผลเสียทุกค่าของแผน x มีค่ามากกว่าค่าผลได้ผลเสียของแผนการเล่น w ในทุกกรณี ในขณะที่แผนการเล่น y นั้นเป็นแผนการเล่นที่ไม่ด้อยกว่าแผนการเล่น x เนื่องจากมีอย่างน้อยหนึ่งค่าของแผนการเล่น y ที่ทำให้ผลได้ผลเสียมากกว่าแผนการเล่น x นั่นคือ ค่าผลได้ผลเสียในกรณีที่ผู้เล่น 2 เลือกแผนการการเล่น b ส่วนค่าผลได้ผลเสียในกรณีที่เหลือที่ผู้เล่น 2 เลือกนั้นแผนการเล่น x และ y มีค่าผลได้ผลเสียเท่ากัน

สำหรับผู้เล่น 2 เนื่องจากค่าในตารางเป็นค่าผลได้ผลเสียของผู้เล่น 1 ดังนั้นค่าผลได้ผลเสียที่ดีกว่าสำหรับผู้เล่น 2 จะหมายถึง ค่าผลได้ผลเสียที่น้อยกว่า และจากตัวอย่างจะเห็นว่าแผนการเล่น a เป็นแผนการเล่นที่เด่นที่สุดอย่างชัดเจน เนื่องจากค่าผลได้ผลเสียทุกค่าของแผน a มีค่าน้อยกว่าค่าผลได้ผลเสียของแผน b, c และ d ไม่ว่าผู้เล่น 1 จะเลือกแผนการเล่นใด เป็นต้น

จากหลักการของแผนการเล่นเด่น ทำให้สามารถลดความซับซ้อนในการหาผลเฉลยได้ เนื่องจากผู้เล่นที่มีเหตุมีผล (rational) นั้นจะไม่เลือกกลยุทธ์ที่ด้อยกว่าเพื่อมาใช้เล่น ทำให้สามารถตัดกลยุทธ์ที่ด้อยกว่าออกก่อนหาผลเฉลยได้โดยค่าของเกมที่ได้จะไม่เปลี่ยนแปลง

2.2 การส่งข้อมูลหลายวิถี (multi-path routing)

เมื่อต้องการส่งข้อมูลจากจุดเชื่อมต่อหนึ่งไปยังอีกจุดเชื่อมโยงต่อ โครงข่ายจะต้องมีกระบวนการจัดหาเส้นทางการส่งข้อมูล (routing) เพื่อให้ข้อมูลถูกส่งไปเส้นทางที่ทำให้เกิดประสิทธิภาพดีที่สุด เช่น ในด้านต้นทุน ด้านความน่าเชื่อถือ เป็นต้น โดยปกติแล้วการจัดหาเส้นทางการส่งข้อมูลจะส่งไปตามเส้นทางใดเส้นทางหนึ่งจากต้นทางไปยังปลายทาง (single path routing) ซึ่งถ้าหากเกิดปัญหาเส้นทางนั้นเสียหายไม่ว่าจากอุปกรณ์การส่งหรือสายเชื่อมโยง จะทำให้การส่งข้อมูลในขณะนั้นใช้งานไม่ได้และเกิดความเสียหายต่อข้อมูลขึ้น ยิ่งไปกว่านั้นถ้าหากการส่งข้อมูลถูกโจมตีด้วยการดักฟังหรือการรบกวนสัญญาณแล้ว โครงข่ายจะถูกโจมตีได้โดยง่ายเพราะสามารถคาดเดาหรือรู้เส้นทางการส่งที่แน่นอน ด้วยเหตุนี้จึงเกิดแนวคิดการส่งข้อมูลที่ใช้มากกว่าหนึ่งเส้นทางเกิดขึ้น (multi-path routing) เพื่อแก้ปัญหาดังกล่าว ซึ่งทำได้หลายลักษณะดังนี้

2.2.1 การส่งแบบระยะทางที่สั้นที่สุด (shortest path)

การส่งแบบระยะทางที่สั้นที่สุด [19] เป็นวิธีการส่งวิธีการส่งข้อมูลไปในทุกเส้นทางที่มีระยะทางสั้นที่สุดหรือต้นทุนต่ำที่สุดซึ่งจะเป็นวิธีการส่งที่ประหยัดทรัพยากรของโครงข่ายแต่ความปลอดภัยนั้นจะต่ำเพราะผู้โจมตีสามารถคาดเดาเส้นทางการส่งข้อมูลได้ง่าย โดยจะเลือกเส้นทางที่สั้นที่สุดในการโจมตี

2.2.2 การจัดเส้นทางแบบเฟ้นสุ่ม

การจัดเส้นทางแบบเฟ้นสุ่ม [14], [20] เป็นวิธีการส่งโดยเลือกเส้นทางการส่งข้อมูลมาหนึ่งเส้นทางอย่างสุ่ม การจัดเส้นทางด้วยวิธีนี้เป็นการยากต่อผู้ที่จะมาโจมตีโครงข่ายเพราะไม่สามารถคาดเดาเส้นทางการส่งข้อมูลที่แน่นอนได้และเป็นการบังคับให้ผู้โจมตีเลือกโจมตีทุกเส้นทางที่เป็นอิสระต่อกัน นอกจากนี้การจัดเส้นทางแบบเฟ้นสุ่มยังไม่เปลืองทรัพยากรมากเท่าการส่งแบบกระจายทุกทิศทางดังนั้นในวิทยานิพนธ์นี้จะพิจารณาเฉพาะการจัดเส้นทางแบบเฟ้นสุ่มโดยมุ่งศึกษาการปรับค่าความน่าจะเป็นในการเลือกเส้นทางการส่งของฝ่ายป้องกันโดยใช้ทฤษฎีเกมเพื่อใช้ในการหาเส้นทางที่ปลอดภัยที่สุดและคำนวณค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีต่อไป

ในวิทยานิพนธ์นี้ได้ใช้การจัดเส้นทางแบบเฟ้นสุ่มเพื่อแก้ไขการถูกโจมตีทั้งสองชนิดได้แก่ การดักฟังและการส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมช โดยได้นำทฤษฎีเกมมาประยุกต์ใช้ในการคำนวณเพื่อเลือกเส้นทางที่ดีที่สุดในการส่งข้อมูล ทำให้สามารถรับประกันค่าความปลอดภัยของโครงข่ายขั้นต่ำที่พึงจะได้ โดยในวิทยานิพนธ์จะสามารถแยกฝ่ายป้องกันและฝ่ายโจมตีซึ่งขัดแย้งกันอย่างชัดเจนจึงจำลองได้โดยใช้เกมผู้เล่นสองคนที่มีผลรวมเป็นศูนย์ แต่ในรูปแบบการโจมตีแบบดักฟังและส่งสัญญาณรบกวนมีลักษณะที่แตกต่างกัน จึงพิจารณาแยกเป็นสองส่วน โดยส่วนแรกจะวิเคราะห์ปัญหาที่เกิดจากการดักฟังข้อมูลในโครงข่าย ส่วนที่สองจกเป็นการวิเคราะห์การถูกโจมตีด้วยสัญญาณรบกวนซึ่งจะกล่าวโดยละเอียดในบทต่อไป

บทที่ 3

ระเบียบวิธีที่นำเสนอในการจัดเส้นทางแบบเฟ้นสุ่มด้วยทฤษฎีเกม

ในบทนี้จะกล่าวถึงระเบียบวิธีที่นำเสนอ โดยในหัวข้อที่ 3.1 กล่าวถึงแบบจำลองของโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทางที่พิจารณาในวิทยานิพนธ์นี้ รวมทั้งอธิบายถึงความแตกต่างระหว่างการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทาง และยังได้อธิบายถึงความแตกต่างของการโจมตีแบบดักฟังข้อมูลกับการรบกวนสัญญาณในโครงข่ายและหัวข้อที่ 3.2 จะกล่างถึงสัญลักษณ์ต่าง ๆ ที่ถูกนิยามขึ้น

ส่วนหัวข้อที่ 3.3 จะกล่าวถึงการจำลองสถานการณ์ที่โครงข่ายไร้สายแบบเมชถูกโจมตีโดยสามารถแบ่งผู้เล่นออกเป็น 2 ฝ่าย คือ ผู้เล่นคนที่หนึ่ง จะทำหน้าที่ป้องกันโครงข่ายโดยการส่งข้อมูลไปตามเส้นทางต่าง ๆ แบบเฟ้นสุ่มเพื่อหลีกเลี่ยงผู้เล่นคนที่สองที่จะมาคอยดักฟังหรือส่งสัญญาณรบกวนต่อโครงข่าย โดยผู้เล่นฝ่ายโจมตีจะพยายามเลือกจุดที่ดีที่สุดเพื่อโจมตีโครงข่ายให้ร้ายแรงที่สุด โดยตอนท้ายของหัวข้อนี้จะอธิบายถึงตัวชี้วัดความปลอดภัยจากงานวิจัยที่ [14] ซึ่งได้นำมาใช้วิเคราะห์ผลกระทบของการเปลี่ยนแปลงพารามิเตอร์ต่าง ๆ ที่ใช้ในโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทาง หัวข้อสุดท้ายของบทหัวข้อที่ 3.4 ได้กล่าวถึงขั้นตอนการหาผลเฉลยของเกมที่ถูกนำมาใช้ในวิทยานิพนธ์นี้

3.1 แบบจำลองโครงข่าย

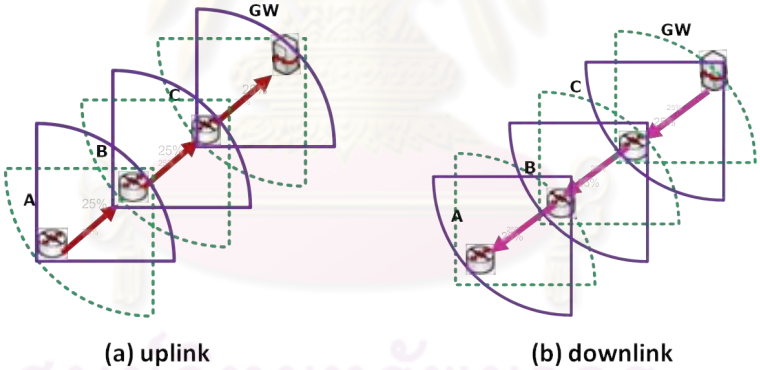
วิทยานิพนธ์นี้กำหนดให้แบบจำลองโครงข่ายไร้สายแบบเมชมีจุดเชื่อมต่อสองชนิดคือเกตเวย์ซึ่งเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตผ่านสายสื่อสารและจุดเชื่อมต่อซึ่งทำหน้าที่รับส่งข้อมูลผ่านตัวกลางไร้สายและส่งข้อมูลกับอินเทอร์เน็ตผ่านเกตเวย์ในลักษณะหลายช่วงเชื่อมต่อ เนื่องจากในวิทยานิพนธ์นี้มองในระดับผู้ให้บริการโครงข่ายอินเทอร์เน็ต จึงพิจารณาเซสชั่นระหว่างจุดเชื่อมต่อกับเกตเวย์เท่านั้น ไม่ได้พิจารณาเซสชั่นระหว่างผู้ใช้งานกับจุดเชื่อมต่อ

ในวิทยานิพนธ์นี้ได้พิจารณาสถานการณ์ที่โครงข่ายถูกโจมตีอย่างร้ายแรงด้วยทฤษฎีเกมสองแบบ คือ การดักฟังข้อมูลและการส่งสัญญาณรบกวน โดยจะพิจารณาปัญหาจากผู้โจมตีรายเดียวแยกกรณีกันและถือว่าเวลาที่ต้องใช้ในการส่งข้อมูลมมีค่าน้อยกว่าเวลาที่ต้องใช้ในการเคลื่อนที่ของผู้โจมตีมาก ทำให้ผู้โจมตีหนึ่ง ๆ ไม่สามารถเคลื่อนที่ไปดักฟังข้อมูลหรือส่งสัญญาณรบกวนใน 2 ตำแหน่งพร้อมกันได้ การโจมตีทั้งสองแบบนี้ผู้เล่นฝ่ายโจมตีจะเลือกพื้นที่ซึ่งอยู่ในเซตของตำแหน่งทั้งหมดในโครงข่ายเพื่อดักฟังข้อมูลหรือส่งสัญญาณรบกวนให้ได้มากที่สุดเท่าที่จะทำได้ ส่วนผู้เล่นฝ่ายป้องกันจะจัดเส้นทางแบบเฟ้นสุ่มระหว่างจุดเชื่อมต่อต่าง ๆ และเกตเวย์ โดยเลือกเส้นทางให้ถูกโจมตีน้อยที่สุดเท่าที่จะทำได้ ในวิทยานิพนธ์นี้จะเรียกการรับส่งข้อมูลระหว่างจุดเชื่อมต่อและเกตเวย์ว่า เซสชั่น และกำหนดให้จำนวนเซสชั่นที่ไม่ถูกโจมตี เป็น ค่าของเกม ซึ่งจะกล่าวโดยละเอียดในหัวข้อ 3.2

3.1.1 ความแตกต่างระหว่างการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่าย

การส่งข้อมูลฝั่งขาขึ้นนั้นมีความแตกต่างจากการส่งข้อมูลฝั่งขาลง เนื่องจากการส่งข้อมูลฝั่งขาขึ้นข้อมูลจะถูกส่งจากจุดเชื่อมต่อทั้งหมดไปยังเกตเวย์โดยผ่านช่องสัญญาณไร้สาย ดังรูปที่ 3.1(a) จากนั้นข้อมูลจะถูกส่งไปยังโครงข่ายอินเทอร์เน็ตที่เชื่อมต่อผ่านสายสื่อสาร ซึ่งการสื่อสารระหว่างโนดนั้นใช้สายอากาศระบุทิศทางทำให้เมื่อโนดต้นทางที่ต้องการส่งข้อมูลโดยการส่งสัญญาณไปหาโนดปลายทางผ่านช่องสัญญาณไร้สาย จะเริ่มจากโนดต้นทางจะส่งสัญญาณที่มีทิศทางพุ่งไปยังโนดปลายทางซึ่งมีข้อมูลส่งไปกับสัญญาณแสดงโดยโคนเส้นทึบ ส่วนในภาครับโนดปลายทางก็ปรับบีมการรับสัญญาณ ของสายอากาศมายังทิศทางพุ่งไปยังโนดต้นทางแสดงโดยโคนเส้นประ ทำให้การส่งข้อมูลฝั่งขาขึ้นนั้นเกตเวย์จะไม่ส่งข้อมูลออกมาเพียงแต่ปรับบีมการรับสัญญาณของสายอากาศมายังจุดเชื่อมต่อ C เท่านั้นซึ่งก็คือจะไม่มีโคนเส้นทึบพุ่งออกจากเกตเวย์ ในทำนองเดียวกันจุดเชื่อมต่อ A ก็จะไม่มีการปรับบีมมารับสัญญาณเพราะเป็นจุดเชื่อมต่อต้นทาง

ส่วนในการส่งข้อมูลฝั่งขาลงนั้นข้อมูลจะถูกส่งจากเกต์เวย์ไปหาจุดเชื่อมต่อทั้งหมดโดยผ่านช่องสัญญาณไร้สาย ดังรูปที่ 3.1(b) ทำให้จุดเชื่อม A ซึ่งเป็นจุดเชื่อมต่อสุดท้ายจะไม่ส่งข้อมูลออกมาเพียงแต่จะปรับบีมการรับสัญญาณของสายอากาศมายังทิศทางพุ่งไปจุดเชื่อมต่อ B เท่านั้น และเกตเวย์ก็จะส่งแต่สัญญาณส่งข้อมูล ไม่ได้ปรับบีมมารับสัญญาณ

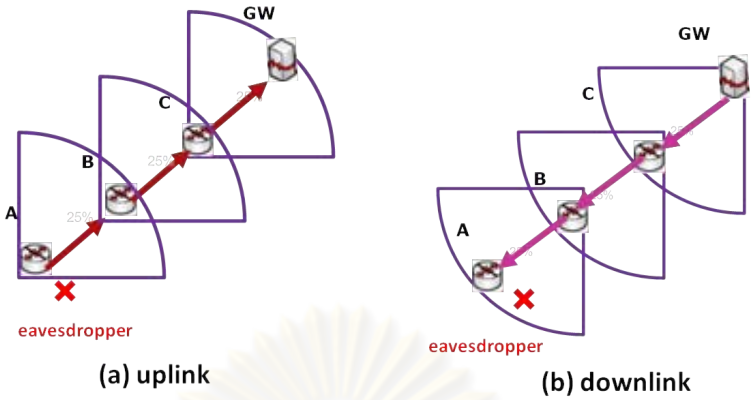


รูปที่ 3.1: ความแตกต่างระหว่างการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

3.1.2 ผลกระทบของการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

ในการจำลองสถานการณ์มีความแตกต่างระหว่างการส่งข้อมูลฝั่งขาขึ้น และการส่งข้อมูลฝั่งขาลงของโครงข่ายไร้สายแบบเมช ซึ่งมีผลต่อการเลือกตำแหน่งในการดักฟังของผู้โจมตี โดยผู้โจมตีจะเลือกตำแหน่งในการดักฟังซึ่งจะคำนึงถึงสัญญาณที่โนดแต่ละโนดใช้ส่งข้อมูลออกมาหรือก็คือพื้นที่โคนเส้นทึบในรูปที่ 3.1 เพื่อความชัดเจนจะอธิบายในรูปที่ 3.2

จากรูปที่ 3.2(a) เป็นการส่งข้อมูลฝั่งขาขึ้นของเซสชั่นระหว่างจุดเชื่อมต่อ A กับเกตเวย์โดยผ่านจุดเชื่อมต่อ B และ C ตามลำดับ ซึ่งเกตเวย์จะไม่ส่งข้อมูลผ่านตัวกลางไร้สายแต่จะส่งข้อมูลไปยังโครงข่ายอินเทอร์เน็ตผ่านสายสื่อสาร ดังนั้นผู้โจมตีดังรูปที่ 3.2(a) จะไม่สามารถ



รูปที่ 3.2: การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

ดักฟังเซสชั่นในตัวอย่างนี้ได้เนื่องจากทิศทางของสายอากาศพุ่งจากจุดเชื่อมต่อ A ตรงไปยังเกตเวย์

จากรูปที่ 3.2(b) เป็นการส่งข้อมูลฝั่งขาลงของเซสชั่นระหว่างจุดเชื่อมต่อ A กับเกตเวย์ โดยผ่านจุดเชื่อมต่อ C และ B ตามลำดับ จากผู้โจมตีตำแหน่งเดิมแต่พอมาเป็นกรณีการส่งข้อมูลฝั่งขาลงทำให้สามารถดักฟังข้อมูลที่ส่งผ่านจากจุดเชื่อมต่อ B ไปยัง A ได้ทำให้ผู้โจมตีสามารถดักฟังเซสชั่นนี้ได้

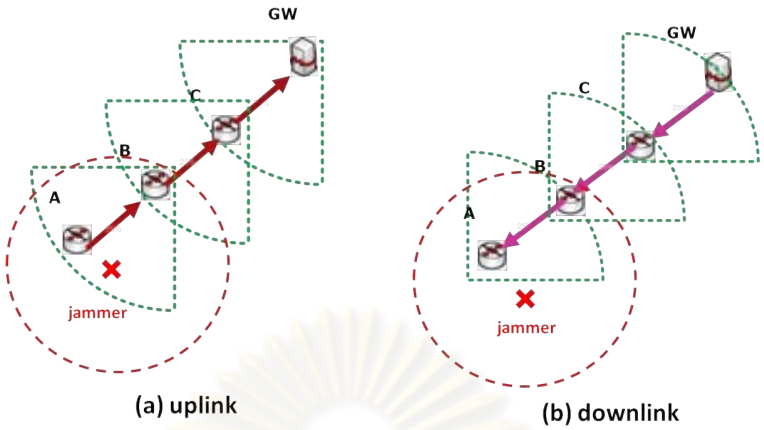
การที่จุดเชื่อมต่อสุดท้ายของเส้นทางในการส่งข้อมูลทั้งฝั่งขาขึ้น คือ เกตเวย์ และฝั่งขาลง คือ จุดเชื่อมต่อที่เป็นเจ้าของข้อมูลของเซสชั่นนั้น ๆ ไม่มีการส่งข้อมูลออกมาผ่านตัวกลางไร้สาย มีผลทำให้การดักฟังของผู้โจมตีต่อการส่งข้อมูลทั้งสองแบบมีลักษณะแตกต่างกัน ดังนั้นโครงข่ายจึงต้องมีการจัดเส้นทางที่แตกต่างกัน เพื่อป้องกันการดักฟังข้อมูลได้อย่างถูกต้องเหมาะสม

3.1.3 ผลกระทบของการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

ในกรณีของการส่งสัญญาณรบกวนจะแตกต่างจากการดักฟังข้อมูลตรงที่ผู้โจมตีจะเลือกตำแหน่งที่ไปรบกวนสัญญาณในพื้นที่บีมของตัวรับสัญญาณซึ่งแสดงเป็นพื้นที่โคนเส้นประในรูปที่ 3.1 โดยเงื่อนไขที่จะสามารถรบกวนสัญญาณได้นั้นคือ ผู้โจมตีจะต้องอยู่ตำแหน่งในพื้นที่บีมภาครับของโนดที่เปิดบีมมารับโนดที่ต้องการจะส่งสัญญาณและรัศมีของสัญญาณรบกวนจะต้องครอบคลุมโนดตัวที่รับสัญญาณ เพื่อความชัดเจนจะอธิบายในรูปที่ 3.3

จากรูปที่ 3.3(a) เป็นการส่งข้อมูลฝั่งขาขึ้นของเซสชั่นระหว่างจุดเชื่อมต่อ A กับเกตเวย์ โดยผ่านจุดเชื่อมต่อ B และ C ตามลำดับ โดยโคนเส้นประแสดงถึงบีมที่ส่งมารับข้อมูล โดยผู้โจมตีส่งสัญญาณรบกวนในพื้นที่บีมที่จุดเชื่อมต่อ B ปรับทิศทางบีมมาเพื่อรับสัญญาณข้อมูลจากจุดเชื่อมต่อ A และรัศมีสัญญาณรบกวนถึงจุดเชื่อมต่อ B ทำให้จุดเชื่อมต่อ B ถูกรบกวนสัญญาณเป็นผลทำให้จุดเชื่อมต่อ A ไม่สามารถส่งข้อมูลไปยังจุดเชื่อมต่อ B ได้

จากรูปที่ 3.3(b) เป็นการส่งข้อมูลฝั่งขาลงของเซสชั่นระหว่างจุดเชื่อมต่อ A กับเกตเวย์ โดยผ่านจุดเชื่อมต่อ C และ B ตามลำดับ ผู้โจมตีอยู่ในตำแหน่งเดียวกับรูปที่ 3.3(a) แต่ใน



รูปที่ 3.3: การส่งสัญญาณรบกวนข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

การส่งข้อมูลฝั่งขาลงนั้น จุดเชื่อมต่อ A ได้เปิดบีมเพื่อรับข้อมูลไปยังจุดเชื่อมต่อ B ทำให้ตำแหน่งที่ผู้โจมตีอยู่ไม่ได้อยู่ในพื้นที่บีมใด ๆ เลย ทำให้ไม่สามารถรบกวนสัญญาณได้

3.2 สัญลักษณ์พื้นฐาน

สำหรับการตั้งโจทย์ปัญหาด้วยวิธีการของเกมในโครงข่ายไร้สายแบบเมช วิทยานิพนธ์นี้ได้นิยามตัวแปรต่าง ๆ ดังนี้

- M แทนจำนวนรูปแบบที่เป็นไปได้ทั้งหมดของการเลือกรับส่งข้อมูลในลักษณะของทรี (tree) ซึ่งมีรากอยู่ที่เกตเวย์และเชื่อมต่อกับจุดเชื่อมต่อผ่านทุกโนดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต
- N แทนจำนวนรูปแบบพื้นที่โจมตีที่เป็นไปได้ทั้งหมด
- i แทนหมายเลขของรูปแบบการเลือกรับส่งข้อมูลในลักษณะของทรีซึ่งมีรากอยู่ที่เกตเวย์และเชื่อมต่อกับจุดเชื่อมต่อผ่านทุกโนดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต
- j แทนหมายเลขรูปแบบพื้นที่โจมตีที่เป็นไปได้
- p_i แทนความน่าจะเป็นที่ผู้เล่นฝั่งป้องกันจะเลือกทรีรูปแบบที่ i ในการรับส่งข้อมูลระหว่างเกตเวย์และจุดเชื่อมต่อผ่านทุกโนดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต
- P การแจกแจงความน่าจะเป็นในการเลือกรูปแบบการรับส่งข้อมูลของผู้เล่นฝั่งป้องกัน
- q_i แทนความน่าจะเป็นที่ผู้เล่นฝั่งโจมตีจะเลือกอยู่ในพื้นที่โจมตีรูปแบบที่ j
- Q การแจกแจงความน่าจะเป็นในการเลือกรูปแบบพื้นที่โจมตีของผู้เล่นฝั่งโจมตี

$s_{i,j}$ จำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตีเมื่อผู้เล่นฝ่ายป้องกันเลือกทรีรูปแบบที่ i ในการรับส่งข้อมูล และผู้เล่นฝ่ายโจมตีเลือกอยู่ในพื้นที่โจมตีรูปแบบที่ j

x_i ตัวแปรช่วย

y_j ตัวแปรช่วย

n แทนรอบของการเล่นเกม

3.3 แบบจำลองเกมของการส่งข้อมูลในโครงข่าย

ในแบบจำลองเกมของการส่งข้อมูลในโครงข่ายนั้น ผู้เล่นสองคน คือ ผู้เล่นฝ่ายป้องกันโครงข่ายและฝ่ายโจมตีโครงข่ายมีลักษณะขัดแย้งกันอย่างชัดเจน จึงสามารถจำลองด้วยเกมที่มีผู้เล่นสองคนที่มีผลรวมเป็นศูนย์

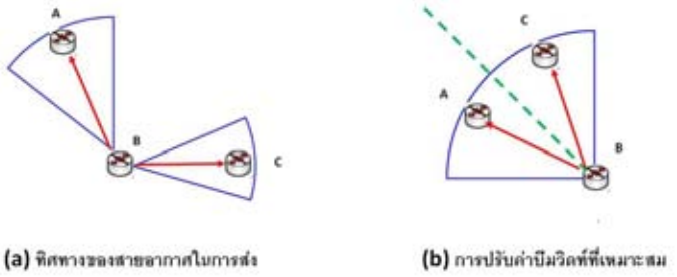
3.3.1 ผู้เล่นฝ่ายป้องกัน (defender)

มีแผนในการเล่นคือ การเลือกส่งข้อมูลในลักษณะของทรีที่มีรากของทรีเป็นเกตเวย์และเชื่อมต่อกับจุดเชื่อมต่อทุกจุดที่ต้องการรับส่งข้อมูลกับโครงข่ายอินเทอร์เน็ต กำหนดให้รูปแบบของทรีที่เป็นไปได้ทั้งหมดมี M รูปแบบได้ การแจกแจงความน่าจะเป็นในการเลือกรูปแบบการส่งสามารถนิยามได้ดังนี้

$$P^T = [p_1, ..., p_i, ..., p_M]$$

ในทางปฏิบัตินั้นเมื่อทราบรัศมีในการส่งข้อมูลผ่านตัวกลางไร้สายจากโนดต่าง ๆ และทราบตำแหน่งของโนดในโครงข่าย จะทำให้สามารถหารูปแบบการส่งของทรีทั้งหมด M รูปแบบ

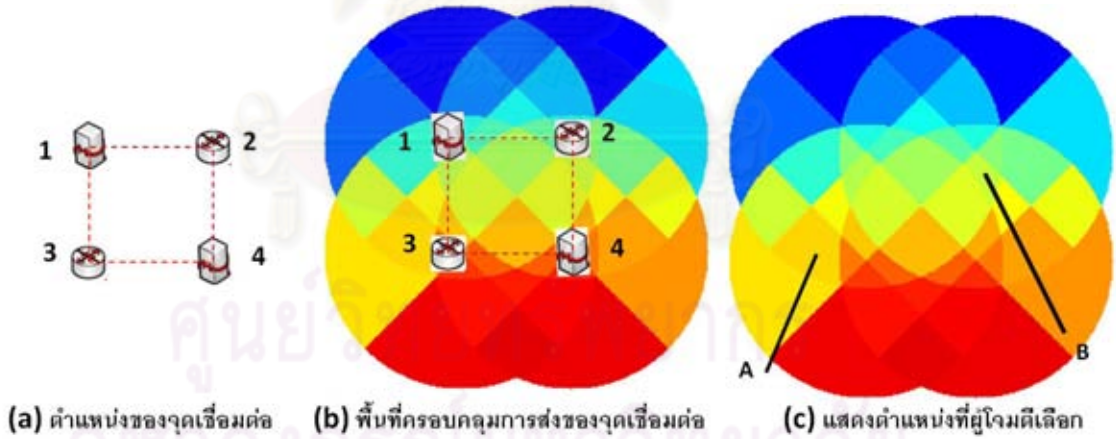
สำหรับรูปแบบของทรีหนึ่ง ๆ ในวิทยานิพนธ์นี้ จะให้ทิศทางและบีมวิดท์ในการส่งของโนดแต่ละโนดในทรีนั้นเป็นดังต่อไปนี้ กำหนดทิศทางของสายอากาศพุ่งตรงในทิศทางการกระจัดจากโนดต้นทางไปยังโนดปลายทาง ดังแสดงตัวอย่างในรูปที่ 3.4(a) และจำนวนเซกเตอร์ (sector) $= \frac{360}{BW}$ ในที่นี้กำหนดให้โครงข่ายเลือกบีมวิดท์ที่ค่ามากที่สุดที่ไม่ทำให้เซกเตอร์จากจุดเชื่อมต่อต้นทางเดียวกันซ้อนทับกัน ทั้งนี้เพื่อลดพื้นที่ซ้อนทับกันที่อาจทำให้ผู้เล่นฝ่ายโจมตีสามารถโจมตีหลาย ๆ จุดเชื่อมต่อพร้อมกันได้ง่าย รวมถึงลดการกวนกันของสัญญาณจากการส่งข้อมูลด้วยบีมที่อยู่ติดกันจากโนดต้นทางหนึ่ง ๆ เนื่องจากต้องการลดต้นทุนเพราะถือว่าสายอากาศที่ใช้บีมวิดท์น้อยจะมีต้นทุนที่แพงกว่าสายอากาศที่มีบีมวิดท์มาก อย่างไรก็ตามผลการทดลองในเบื้องต้นซึ่งได้นำเสนอในวิทยานิพนธ์นี้จะทดสอบโดยการกำหนดค่าบีมวิดท์ให้เท่ากันทุกโนดก่อน ทั้งนี้เพื่อความสะดวกในการตรวจสอบความถูกต้องผลการทดลองที่ได้ ส่วนการปรับค่าบีมวิดท์ให้เหมาะสมกับโนดแต่ละโนดดังรูปที่ 3.4(b) นั้นจะทำในลำดับต่อไป นอกจากนี้กำหนดในวิทยานิพนธ์นี้ให้ใช้แบบจำลองสายอากาศเป็นแบบโคน (cone model) [21] นั่นคือไม่คิดผลของบีมย่อยด้านอื่นที่ไม่ได้อยู่ในทิศทางหลักที่รับส่งสัญญาณ



รูปที่ 3.4: ทิศทางและการปรับค่าบีมวิดท์ที่เหมาะสม

3.3.2 ผู้เล่นฝ่ายโจมตี (attacker)

มีแผนการเล่นคือการเลือกตำแหน่งในโครงข่ายเพื่อโจมตีข้อมูลที่รับส่งสัญญาณข้อมูลระหว่างจุดเชื่อมต่อทั้งหมดกับเกตเวย์ให้ได้มากที่สุด โดยจัดกลุ่มตำแหน่งที่เป็นไปได้ทั้งหมดที่ให้ผลการโจมตีออกมาเหมือนกันไว้ในแผนเดียวกันซึ่งสามารถแสดงออกมาในรูปของพื้นที่ที่เกิดจากการตัดกันของขอบเขตของบีมของสายอากาศระบุทิศทางต่าง ๆ ดังแสดงตัวอย่างพื้นที่สีที่แตกต่างกันในรูปที่ 3.3 สำหรับตำแหน่งต่าง ๆ ทุกตำแหน่งในพื้นที่ที่มีสีเหมือนกันจะหมายความว่าหากผู้เล่นฝ่ายโจมตีเลือกแผนการเล่นโดยอยู่ที่ตำแหน่งนั้น ๆ แล้วผลของการโจมตีจะสามารถดักฟังหรือส่งสัญญาณรบกวนได้ชุดของเซสชั่นที่ถูกโจมตีที่เหมือนกัน



รูปที่ 3.5: เซตของพื้นที่ทั้งหมดที่ผู้โจมตีสามารถโจมตีโครงข่ายได้

พื้นที่สีที่แตกต่างกันในส่วนของวงกลมจะหมายถึงตำแหน่งที่ผู้เล่นฝ่ายโจมตีมาโจมตีพื้นที่ดังกล่าวแล้ว ถ้าสีเหมือนกันผลลัพธ์ที่ได้จากการโจมตีจะเหมือนกันซึ่งถือว่าเป็นแผนการเล่นเดียวกันหรือถ้าสีแตกต่างกันจะได้ผลลัพธ์ที่แตกต่างกันซึ่งจะถือว่าเป็นแผนการเล่นคนละแผน โดยถ้าเป็นกรณีของการดักฟังข้อมูลผู้เล่นฝ่ายโจมตีจะต้องไปดักฟังข้อมูลในพื้นที่ครอบคลุมของบีมที่จุดเชื่อมต่อหรือเกตเวย์ส่งออกมาจะทำให้สามารถดักฟังข้อมูลจากจุดเชื่อมต่อหรือเกตเวย์ตัวนั้น ๆ ได้ซึ่งจะแสดงความแตกต่างของตำแหน่งการโจมตีจากสีส่วนในกรณีของการส่งสัญญาณรบกวนผู้เล่นฝ่ายโจมตีจะต้องอยู่ในพื้นที่ของบีมที่มาจากจุด

เชื่อมต่อหรือเกตเวย์และรัศมีของสัญญาณรบกวนจะต้องครอบคลุมจุดเชื่อมต่อหรือเกตเวย์ตัวนั้น ๆ ด้วย

รูปที่ 3.5 เป็นการส่งข้อมูลจากจุดเชื่อมต่อ 2 และ 3 เข้าสู่เกตเวย์ 1 และ 4 ซึ่งมีพื้นที่ครอบคลุมการส่งตามภาพ หากผู้โจมตีเลือกโจมตีจากตำแหน่งของพื้นที่ A แล้วจะสามารถโจมตีข้อมูลที่ส่งผ่านเกตเวย์ 1 ไปยังจุดเชื่อมต่อ 3 และ ข้อมูลที่จุดเชื่อมต่อ 3 ในเซกเตอร์ทางซ้ายได้ หรือถ้าผู้โจมตีเลือกโจมตีจากตำแหน่งของพื้นที่ B แล้วจะสามารถโจมตีข้อมูลได้ 3 เซกเตอร์ซึ่งเซกเตอร์แรกที่ส่งข้อมูลผ่านเกตเวย์ 1 ไปยังจุดเชื่อมต่อ 2 ส่วนเซกเตอร์สองคือส่งข้อมูลจากจุดเชื่อมต่อ 2 ไปยังเกตเวย์ 4 และเซกเตอร์สุดท้ายคือส่งข้อมูลจากเกตเวย์ 4 ไปยังจุดเชื่อมต่อ 2 ดังนั้นกำหนดให้พื้นที่ครอบคลุมทั้งหมดที่เป็นไปได้มี N พื้นที่ การแจกแจงความน่าจะเป็นในการเลือกพื้นที่เพื่อโจมตีสามารถนิยามด้วยเวกเตอร์แนวคอลัมน์ $Q = [q_1, ..., q_j, ..., q_N]$

3.3.3 ค่าของเกม

ในวิทยานิพนธ์ถือว่าการส่งข้อมูลเกิดขึ้นด้วยอัตราที่สูงในช่วงเวลาสัมพัทธ์ซึ่งน้อยกว่าเวลาที่ใช้ในการเคลื่อนที่ของผู้โจมตีมาก ดังนั้นการส่งข้อมูลในทุกเส้นทางจะเกิดขึ้นพร้อม ๆ กันโดยผู้โจมตีหนึ่ง ๆ ไม่สามารถเคลื่อนที่ไปดักฟังข้อมูลหรือไปรบกวนสัญญาณที่เหลือได้ทัน ดังนั้นค่าของเกมจึงนิยามเป็นจำนวนเซสชั่นที่ไม่ถูกดักฟังหรือรบกวนสัญญาณระหว่างจุดเชื่อมต่อกับเกตเวย์ซึ่งเซสชั่นที่ถูกดักฟังหรือรบกวนสัญญาณหมายถึง เซสชั่นที่มีจุดเชื่อมต่อหรือเกตเวย์ซึ่งถูกดักฟังหรือรบกวนสัญญาณอยู่เป็นส่วนหนึ่งของเส้นทางบนทรีของการส่งข้อมูลที่เลือกใช้และเซสชั่นดังกล่าวใช้จุดเชื่อมต่อนั้นส่งข้อมูลออกมาผ่านตัวกลางไร้สาย

ค่าผลได้ผลเสียสามารถเขียนออกมาได้ดังนี้

$$S = \begin{bmatrix} s_{1,1} & \cdot & \cdot & \cdot & s_{1,N} \\ \cdot & \cdot & & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & & \cdot & \cdot \\ s_{M,1} & \cdot & \cdot & \cdot & s_{M,N} \end{bmatrix}$$

3.3.4 การวิเคราะห์และแก้ปัญหาด้วยวิธี MSA (method of successive average)

ในงานวิจัยนี้ได้หาผลเฉลยของเกมโดยใช้หลักการตอบโต้ที่ดีที่สุด (best response) ร่วมกับการปรับปรุงค่าความน่าจะเป็นด้วย MSA ซึ่งเป็นกระบวนการที่เป็นที่รู้จักและถูกใช้ในการแก้ไขปัญหาในงานวิจัยที่นำทฤษฎีเกมมาใช้ เช่น [14], [22] โดยวิธีการหาผลเฉลยดังกล่าวมีขั้นตอนดังนี้

ขั้นที่ 1: เริ่มต้นโดยให้ผู้เล่นทั้งคู่กำหนดค่าความน่าจะเป็นในการเลือกแผนการเล่นแต่ละแผนให้มีค่าเท่ากันดังนี้

$$p_i = \frac{1}{M}, \forall i$$

$$q_j = \frac{1}{N}, \forall j$$

กำหนดการเล่นรอบแรกเป็นรอบที่ 1 $(n = 1)$

ขั้นที่ 2: ฝ่ายป้องกันเลือกรูปแบบการส่งที่ได้ค่าคาดหวังของจำนวนเซสชั่นที่ไม่ถูกดักฟังมากที่สุด โดยฝ่ายโจมตีเลือกโจมตีด้วยความน่าจะเป็นซึ่งกำหนดโดย Q นิยามให้

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

รูปแบบการส่งที่ได้ค่า ESS สูงสุดจะคำนวณได้จาก $\hat{i} = \arg\max_i \{ESS_i\}$ หลังจากนั้นฝ่ายป้องกันปรับปรุงความน่าจะเป็นในการเลือกรูปแบบการส่งดังนี้

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

ขั้นที่ 3: ฝ่ายผู้โจมตีเลือกพื้นที่เพื่อโจมตีเซสชั่นให้ได้มากที่สุด โดยฝั่งป้องกันเลือกรูปแบบการส่งด้วยความน่าจะเป็นซึ่งกำหนดโดย P นิยามให้

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

พื้นที่ที่โจมตีเซสชั่นได้มากที่สุด จะคำนวณได้จาก $\hat{j} = \arg\min_j \{ESS_j\}$ หลังจากนั้นผู้โจมตีปรับปรุงความน่าจะเป็นในการเลือกพื้นที่เพื่อโจมตีดังนี้

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

ขั้นที่ 4: คำนวณค่าคาดหวังของจำนวนเซสชั่นที่ปลอดภัยจากการถูกโจมตี (ESS) สำหรับรอบที่ n ดังสมการ

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

ขั้นที่ 5: ปรับรอบการเล่นดังนี้ $n \leftarrow n + 1$ แล้วดำเนินการตามขั้นที่ **2 - 4** จนกระทั่งค่า ESS ลู่เข้าค่าคงที่ค่าหนึ่งซึ่งแสดงถึงจุดสมดุลของเกม

การนำไปใช้ปฏิบัติจริงนั้นเมื่อวิเคราะห์ผลเฉลยจาก MSA แล้ว จะพบว่า ณ จุดสมดุลของเกมอาจมีคำตอบที่เหมาะสมที่สุดหลายคำตอบได้ ซึ่งจากทฤษฎีเกมที่มีผู้เล่นสองคนและมีผลรวมเป็นศูนย์กล่าวว่า ในทุกคำตอบนั้นจะทำให้ค่าของเกมหรือ ESS เท่ากันเสมอ ดังนั้นการเลือกแต่ละคำตอบที่ได้จะไม่มีผลกระทบต่อการชี้วัดระดับความปลอดภัยด้วยตัวชี้วัด ESS โดยคำตอบที่เหมาะสมที่สุดในที่นี้ คือ การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะที่สุด

นั้น โครงข่ายสามารถเลือกเอาการจัดเส้นทางแบบสุ่มที่เหมาะสมที่สุดหนึ่งคำตอบจากหลายคำตอบนี้เพื่อมาใช้ในการป้องกันการโจมตีโครงข่ายได้

จากงานวิจัย [14] การวิเคราะห์ปัญหาของ MSA นั้นมีความซับซ้อนในการหาผลเฉลย เพื่อแก้ปัญหาดังกล่าวในวิทยานิพนธ์นี้จึงได้ใช้หลักการของกลยุทธ์เด่นเพื่อตัดแผนที่ด้อยกว่าของผู้เล่นทั้งสองฝ่ายออกก่อนการหาผลเฉลยด้วย MSA นอกจากนี้สำหรับแผนการเล่นที่มีความเท่าเทียม ซึ่งหมายถึงแผนการเล่นเมื่อวิเคราะห์ด้วยตารางผลได้ผลเสียแล้วแผนการเล่นนั้นทำให้ได้ค่าผลได้ผลเสียเท่ากันทุกกรณี วิทยานิพนธ์นี้จะเลือกแผนที่มีบีมที่ใช้ซ้ำกับแผนการเล่นเหมาะสมที่สุดที่เลือกมาแล้วก่อนหน้ารวมถึงการใช้หลักการกลยุทธ์เด่นและแผนการเล่นที่มีความเท่าเทียมเพื่อเป็นการประหยัดต้นทุนในของระยะเวลาที่ใช้ในการประมวลผลโดยการลดความซับซ้อนในการหาผลเฉลย

หลังจากที่วิเคราะห์ปัญหาและจำลองโครงข่ายไร้สายแบบเมชซึ่งตกอยู่ภายใต้การโจมตีแบบดักฟังข้อมูลและส่งสัญญาณรบกวนแล้ว โนดในโครงข่ายจะใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดจากกระบวนการหาผลเฉลยโดยกรรมวิธี MSA ที่กล่าวไว้ข้างต้นเพื่อป้องกันการโจมตีทั้งสองแบบ โดยระเบียบวิธีที่นำเสนอการจัดหาเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดนั้นจะทดสอบและวิเคราะห์เกี่ยวกับระเบียบวิธีอื่น ๆ ในด้านต่าง ๆ ผ่านตัวชี้วัด ESS ในบทต่อไป

บทที่ 4

ผลการทดสอบ

เนื้อหาในบทนี้จะเป็นผลการทดสอบระเบียบวิธีนำเสนอในการหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุด รวมทั้งศึกษาผลกระทบของการถูกโจมตีด้วยการดักฟังข้อมูลและการส่งสัญญาณรบกวนข้อมูลในโครงข่ายไร้สายแบบเมช ซึ่งการทดสอบได้แบ่งออกเป็น 3 หัวข้อดังนี้

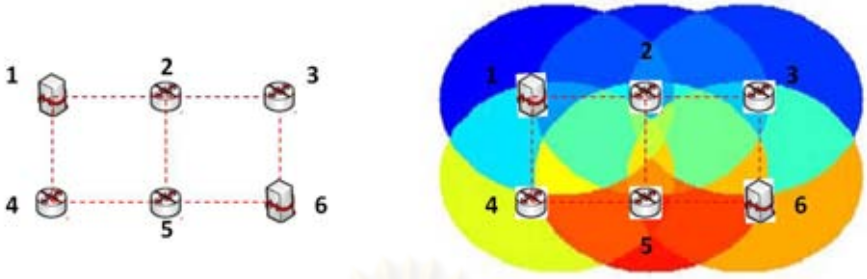
โดยหัวข้อ 4.1 จะเป็นการทดสอบกับโครงข่ายแบบตารางขนาดเล็กซึ่งจะแสดงระเบียบวิธีการคำนวนหาการจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดอย่างง่าย ต่อมาหัวข้อ 4.2 จะเป็นการทดสอบกับโครงข่ายแบบตารางที่มีขนาดใหญ่ขึ้นซึ่งจะทำการวิเคราะห์ผลกระทบต่าง ๆ ออกเป็นหลายหัวข้อย่อยได้แก่ ผลกระทบของการเปลี่ยนแปลงค่าบีมวิดท์ ความแตกต่างของค่า ESS ในโครงข่ายแบบหนาแน่นกับโครงข่ายแบบเบาบาง ผลกระทบจากการเปลี่ยนตำแหน่งเกตเวย์และจากการเพิ่มรัศมีการส่งสัญญาณไร้สายให้กับโนดในโครงข่าย การจัดหาเส้นทางเฟ้นสุ่มของผู้เล่นฝ่ายป้องกันจากทฤษฎีเกมเทียบกับการสุ่มแบบยูนิฟอร์ม การเลือกพื้นที่การโจมตีของผู้เล่นฝ่ายโจมตีจากทฤษฎีเกมเทียบกับวิธีการเลือกพื้นที่แบบยูนิฟอร์มและแบบพื้นที่ที่มีการทับซ้อนกันของบีมมากที่สุด และสุดท้ายคือการวิเคราะห์ผลกระทบต่อค่าความปลอดภัยเมื่อมีจุดเชื่อมต่อใดจุดเชื่อมต่อหนึ่งเกิดความเสียหาย หัวข้อสุดท้ายหัวข้อ 4.3 จะเป็นการวิเคราะห์โครงข่ายสุ่ม

4.1 การทดสอบกับโครงข่ายแบบตารางขนาดเล็ก

เพื่อความชัดเจนในหัวข้อที่ 4.1 นี้จะยกตัวอย่างการคำนวนการจัดหาเส้นทางเฟ้นซุ่มของโครงข่ายแบบตารางขนาด 2x3 โดยในตัวอย่างจะแสดงการจำลองทั้ง 2 แบบ คือ กรณีสายอากาศรอบทิศทาง และกรณีสายอากาศระบุทิศทาง โดยในกรณีของสายอากาศระบุทิศทางจุดเชื่อมต่อและเกตเวย์ทุกตัวมีค่าบีมวิดท์เท่ากันทั้งหมด โดยสีที่แตกต่างกันของพื้นที่ตัดกันของส่วนของวงกลมต่าง ๆ ดังรูปที่ 4.1 จะแสดงถึงเซตของตำแหน่งที่ผู้เล่นฝ่ายโจมตีดักฟังหรือส่งสัญญาณรบกวนในพื้นที่ที่มีสีเดียวกันจะให้ผลของการโจมตีเหมือนกัน โดยกำหนดให้จุดเชื่อมต่อและเกตเวย์ทุกโนดที่ติดกันห่างกัน 20 หน่วย และโนดแต่ละโนดมีมีรัศมีในการส่ง 25 หน่วย

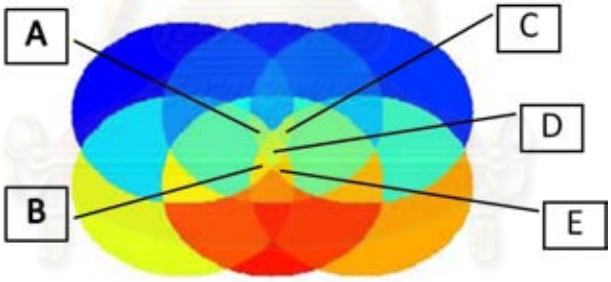
4.1.1 การทดสอบกับโครงข่ายแบบตารางขนาด 2x3 ในกรณีที่ผู้เล่นฝ่ายป้องกันใช้สายอากาศรอบทิศทาง

จากรูปที่ 4.1 เป็นการทดสอบกับโครงข่ายแบบตารางขนาด 2x3 โดยโครงข่ายประกอบไปด้วยเกตเวย์ 2 ตัวอยู่ในตำแหน่งที่ 1 และ 6 ส่วนตำแหน่งโนดที่ 2 ถึง 5 จะทำหน้าที่เป็นจุดเชื่อมต่อซึ่งโนดทั้งหมดว่างห่างกัน 20 หน่วยและกำหนดให้รัศมีในการส่งสัญญาณไร้สายในแต่ละโนดมีค่าเป็น 25 หน่วย โดยนำมาทดสอบในกรณีการส่งข้อมูลฝั่งขาขึ้นและขา



รูปที่ 4.1: โครงข่ายแบบตารางขนาด 2x3 และเซตของตำแหน่งในการดักฟังที่ส่งผลแตกต่างกันในกรณีสายอากาศรอบทิศทาง

ลง ซึ่งนำมาทดสอบทั้งในกรณีการดักฟังข้อมูลและการส่งสัญญาณรบกวน ในกรณีแรกคือการดักฟังข้อมูลปรากฏว่าได้ค่า ESS = 0 ทั้งในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง นั่นคือไม่ว่าผู้เล่นฝ่ายป้องกันจะเลือกรูปแบบทรีในการส่งแบบใดก็ตาม ผู้เล่นฝ่ายโจมตีจะสามารถดักฟังเซสชันของทุกจุดเชื่อมต่อได้หมด โดยแผนการเล่นของผู้เล่นฝ่ายโจมตีจะเลือกพื้นที่ในการดักฟังดังรูปที่ 4.2



รูปที่ 4.2: ตำแหน่งที่ผู้เล่นฝ่ายโจมตีเลือกเพื่อดักฟังข้อมูลในโครงข่ายได้ร้ายแรงที่สุด

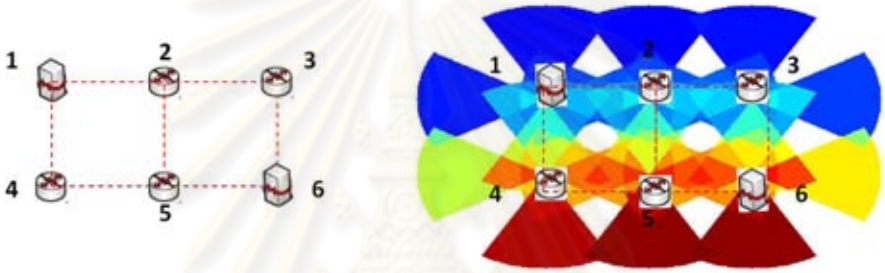
โดยพื้นที่ทั้ง B, C, D จะเป็นตำแหน่งที่ผู้เล่นฝ่ายโจมตีเลือก เพื่อให้สามารถดักฟังจำนวนเซสชั่นให้ได้มากที่สุดในกรณีการส่งข้อมูลฝั่งขาลง โดย พื้นที่ C จะสามารถดักฟังจุดเชื่อมต่อ {1, 2, 3, 5, 6} ได้ และในพื้นที่ D จะสามารถดักฟังจุดเชื่อมต่อ {1, 2, 3, 4, 5, 6} ได้ สุดท้ายพื้นที่ B จะสามารถดักฟังจุดเชื่อมต่อ {1, 2, 4, 5, 6} ได้ โดยโอกาสที่พื้นที่ B, C, D ถูกเลือกจะมีค่าความน่าจะเป็นเท่ากับ 0.32, 0.357 และ 0.323 ตามลำดับ ส่วนในกรณีของการส่งข้อมูลฝั่งขาขึ้นพื้นที่ A, D, E จะเป็นตำแหน่งในการโจมตีที่ดีที่สุดเช่นกัน จะสังเกตได้ว่าผู้เล่นฝ่ายโจมตีสามารถดักฟังข้อมูลที่ผ่านเกตเวย์ 1 และ 6 ได้ทั้ง 2 เกตเวย์พร้อมกันทำให้ไม่ว่า ผู้เล่นฝ่ายป้องกันเลือกการส่งข้อมูลแบบไหนก็จะไม่มีเซสชั่นไหนปลอดภัยทั้งสิ้น

เพื่อให้เห็นข้อแตกต่างระหว่างการใช้สายอากาศรอบทิศทางกับสายอากาศระบุทิศทางในตัวอย่างต่อไปจะพิจารณาโครงข่ายเดียวกัน โดยให้ค่าบิมวิดท์ของสายอากาศทุกตัวมีค่าเป็น

60 องศา และมีทิศทางของบีมพุ่งตามทิศทางการกระจัดไปยังจุดเชื่อมต่อหรือเกตเวย์ปลายทาง

จากงานวิจัย [14] ได้แสดงให้เห็นว่าการโจมตีด้วยการดักฟังข้อมูลและการส่งสัญญาณรบกวนในกรณีที่ฝ่ายป้องกันใช้สายอากาศรอบทิศทางนั้นจะมีผลทำให้ ESS เท่ากัน ทั้งการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง แต่แผนการเล่นทั้งผู้เล่นฝ่ายป้องกันและผู้เล่นฝ่ายโจมตีจะแตกต่างกัน

4.1.2 การทดสอบกับโครงข่ายแบบตารางขนาด 2x3 ในกรณีที่ฝ่ายป้องกันใช้สายอากาศระบุทิศทาง



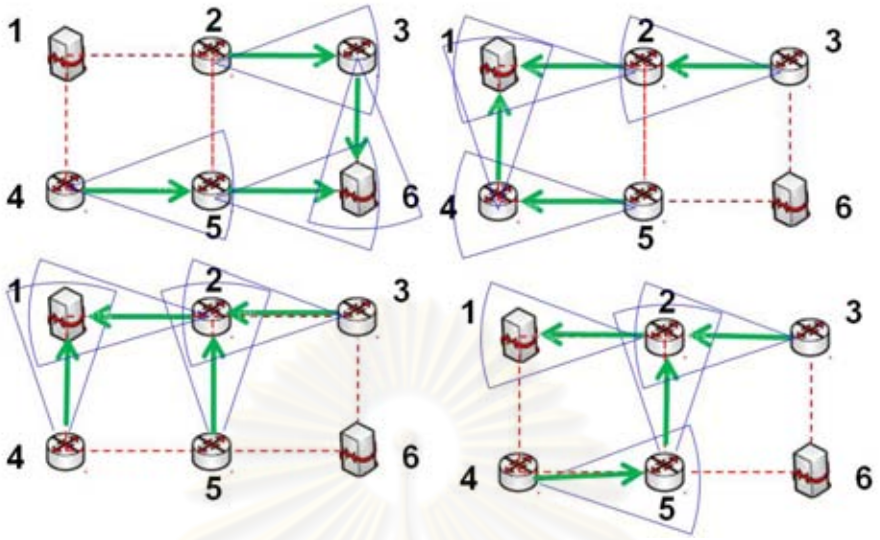
รูปที่ 4.3: โครงข่ายแบบตารางขนาด 2x3 และเซตของตำแหน่งในการดักฟังที่ส่งผลแตกต่างกันในกรณีสายอากาศระบุทิศทาง

จากรูปที่ 4.3 เป็นการทดสอบกับโครงข่ายแบบตารางขนาด 2x3 โดยโครงข่ายประกอบไปด้วยเกตเวย์ 2 ตัวอยู่ในตำแหน่งที่ 1 และ 6 ส่วนตำแหน่งโนดที่ 2 ถึง 5 จะทำหน้าที่เป็นจุดเชื่อมต่อซึ่งโนดทั้งหมดว่างห่างกัน 20 หน่วยและกำหนดให้รัศมีในการส่งสัญญาณไร้สายในแต่ละโนดมีค่าเป็น 25 หน่วย และกำหนดให้บีมวิดท์ของโนดทุกโนดมีค่าเป็น 60 องศาโดยการทดสอบได้ทดสอบทั้ง 2 กรณีคือ การส่งข้อมูลฝั่งขาขึ้นและขาลง ซึ่งได้ผลการทดสอบดังนี้

4.1.2.1 กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น

เมื่อทำการทดสอบปรากฏว่าได้ค่า ESS = 2 ซึ่งหมายความว่า ถ้าผู้เล่นฝ่ายป้องกันเลือกรูปแบบการส่งด้วยทรีที่ดีที่สุดและผู้เล่นฝ่ายโจมตีเลือกโจมตีพื้นที่ที่ดีที่สุดเช่นกัน จะมีจำนวนเซสชั่นที่ปลอดภัย 2 เซสชั่น หรือกล่าวอีกนัยหนึ่งได้ว่า ถ้าผู้เล่นฝ่ายป้องกันเลือกรูปแบบการส่งด้วยทรีที่ดีที่สุดแล้ว สามารถรับประกันได้ว่าค่าจำนวนเซสชั่นระหว่างจุดเชื่อมต่อกับเกตเวย์ที่ปลอดภัยจะไม่ต่ำกว่า 2 เซสชั่น จากการทดสอบจะได้รูปแบบการส่งข้อมูลแบบทรีที่ดีที่สุดของฝ่ายป้องกันดังรูปที่ 4.4

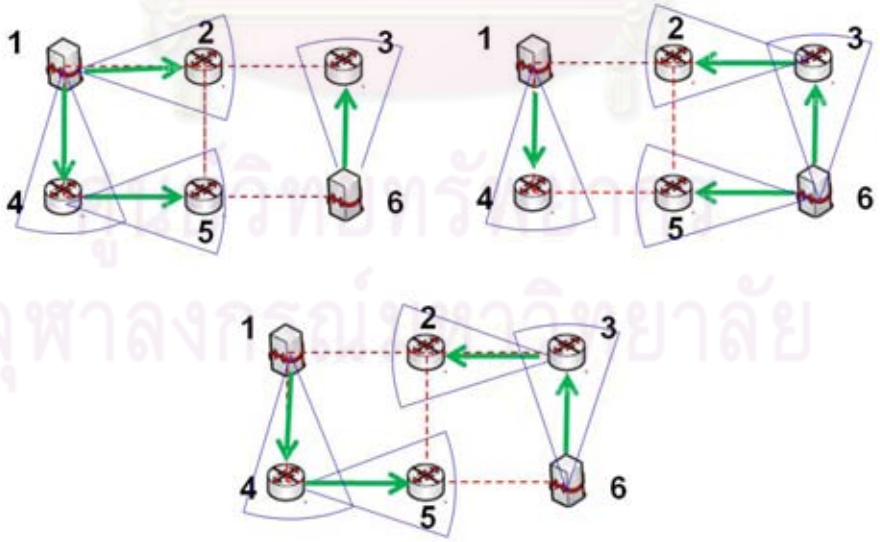
ซึ่งจากการทดสอบจะได้พื้นที่ในการโจมตีที่ดีที่สุดของผู้เล่นฝ่ายโจมตีเช่นกัน แต่ในกรณีนี้แผนการเล่นของผู้เล่นฝ่ายโจมตีหรือตำแหน่งในการโจมตีนั้นมีความน่าจะเป็นในการเลือกใกล้เคียงกัน ซึ่งจะอธิบายในตัวอย่างของการส่งข้อมูลฝั่งขาลง



รูปที่ 4.4: รูปแบบการส่งด้วยทรีที่ดีที่สุดของผู้เล่นฝ่ายป้องกันกรณีการส่งข้อมูลฝั่งขาขึ้น

4.1.2.2 กรณีการดักฟังข้อมูลการส่งข้อมูลฝั่งขาลง

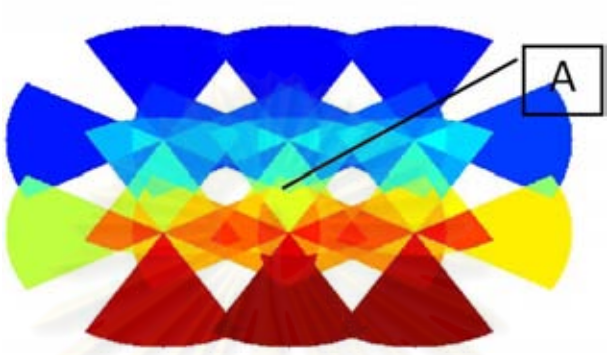
เมื่อทำการทดสอบปรากฏว่าได้ค่า $ESS = 2$ เหมือนกับกรณีของการส่งข้อมูลฝั่งขาขึ้น แต่เมื่อพิจารณาแผนของผู้เล่นทั้ง 2 ฝ่าย คือ ทั้งการเลือกรูปแบบการส่งด้วยทรีของฝ่ายป้องกันและการเลือกพื้นที่ในการดักฟังของฝ่ายโจมตี ปรากฏว่ามีรูปแบบไม่เหมือนกัน โดยรูปแบบการส่งข้อมูลแบบทรีที่ดีที่สุดของผู้เล่นฝั่งป้องกันแสดงดังรูปที่ 4.5



รูปที่ 4.5: รูปแบบการส่งแบบทรีที่ดีที่สุดของผู้เล่นฝ่ายป้องกันกรณีการส่งข้อมูลฝั่งขาลง

จากรูปที่ 4.4 และ 4.5 รูปแบบการส่งด้วยทรีจะมีรูปแบบที่สมมาตรกันเนื่องจากรูปแบบโครงข่ายมีความสมมาตร ทำให้ผู้เล่นฝ่ายป้องกันสามารถเลือกรูปแบบหนึ่ง ๆ ขึ้นมาจาก

รูปแบบที่สมมาตรกันทั้งหมดโดยที่รูปแบบที่สมมาตรนั้นจะต้องไม่เปลี่ยนตำแหน่งการโจมตีของผู้เล่นฝ่ายโจมตีทำให้ค่าของเกมยังคงไม่เปลี่ยนแปลงและลดต้นทุนที่ใช้ได้เนื่องจากไม่จำเป็นจะต้องใช้บีมทุกบีมในการส่งข้อมูล นอกจากนี้จากการทดสอบได้พื้นที่ที่ดีที่สุดของผู้เล่นฝั่งโจมตีเพื่อการดักฟัง ดังรูปที่ 4.6



รูปที่ 4.6: เซตของตำแหน่งในการดักฟังที่ส่งผลแตกต่างกันทั้งการส่งข้อมูลฝั่งขาขึ้นและขาลง

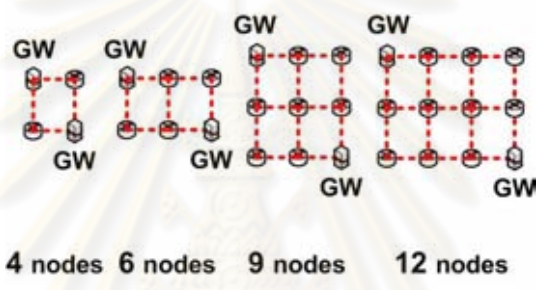
โดยพื้นที่ A จะเป็นตำแหน่งที่ผู้เล่นฝ่ายโจมตีเลือก เพื่อให้สามารถดักฟังจำนวนเซสชั่นให้ได้มากที่สุด ซึ่งการคำนวณจะแตกต่างจากกรณีของสายอากาศรอบทิศทางเนื่องจากในจุดเชื่อมต่อหนึ่งหนึ่งนั้นจะมีบีมออกไป 4 ทิศทาง วิธีการแสดงค่าพื้นที่ของผู้เล่นฝ่ายโจมตีจะแสดงโดยกำหนดให้ตัวเลขจำนวนเต็มหน้าทศนิยมแสดงถึงจุดเชื่อมต่อ และตัวเลขหลังทศนิยมหมายถึงทิศทางของบีมที่ใช้ส่งโดยอ้างอิงกับเข็มนาฬิกา เช่น 1.12 หมายถึง บีมที่อยู่ในจุดเชื่อมต่อที่ 1 และทิศทางบีมพุ่งไปด้านบนหรือ 12 นาฬิกา อีกตัวอย่างคือ 3.9 หมายถึงบีมที่อยู่ในจุดเชื่อมต่อที่ 3 และทิศทางบีมพุ่งไปด้านซ้ายหรือ 9 นาฬิกา พื้นที่ A จะสามารถดักฟังจุดเชื่อมต่อ {1.3, 2.6, 3.9, 4.3, 5.12, 6.9} ได้ โดยพื้นที่ที่ดีที่สุดของฝ่ายโจมตีนั้นจะมีแค่พื้นที่เดียวในกรณีนี้ จากการทดสอบทำให้เห็นข้อแตกต่างระหว่างการใช้สายอากาศรอบทิศทางมาเป็นสายอากาศระบุทิศทางตรงที่ ผู้เล่นฝ่ายโจมตีไม่สามารถดักฟังพื้นที่บีมที่เกตเวย์สองเกตเวย์ใช้ในการส่งข้อมูลพร้อมกันได้ และต้องเลือกดักฟังแค่บางบีมเท่านั้นจึงทำให้ถ้าผู้เล่นฝ่ายป้องกันเลือกรูปแบบการส่งข้อมูลด้วยทรีที่ดีที่สุดแล้วและผู้เล่นฝ่ายโจมตีเลือกพื้นที่ในการดักฟังที่ดีที่สุดเช่นกันจะมี 2 เซสชั่นที่ปลอดภัย ณ จุดสมดุลของเกม เนื่องจากกรณีการส่งข้อมูลขาขึ้นและขาลงมีรูปแบบแผนของผู้เล่นฝ่ายป้องกันและฝ่ายโจมตีที่ไม่เหมือนกันทำให้ต้องพิจารณาแยกกรณีในการป้องกันที่แตกต่างกัน

4.1.2.3 กรณีการส่งสัญญาณรบกวนในโครงข่าย

จากหัวข้อ 3.1 ที่ได้กล่าวมา ทำให้ทราบว่าจากรูปที่ 3.2 ในกรณีของการดักฟังข้อมูลนั้น ผู้เล่นฝ่ายโจมตีจะเลือกโจมตีตำแหน่งที่อยู่ในพื้นที่บีมที่มีทิศทางพุ่งจากโนดต้นทางไปยังโนดปลายทาง เพื่อที่จะทำให้เซสชั่นของโนดต้นทางนั้นไม่ปลอดภัย แต่ในทางกลับกันจากรูปที่ 3.3 ในกรณีของการส่งสัญญาณรบกวนผู้เล่นฝ่ายโจมตีจะเลือกพื้นที่บีมของโนดตัวรับที่หันบีมมารับข้อมูลจากโนดต้นทางแทนเพื่อที่จะทำให้เซสชั่นของโนดไม่ปลอดภัยหรือ

ไม่ได้ยินสัญญาณ เนื่องจากในวิทยานิพนธ์นี้ได้กำหนดให้ผู้เล่นฝ่ายโจมตีในกรณีของการส่งสัญญาณรบกวนนั้นมีรัศมีของสัญญาณรบกวนเท่ากับรัศมีของการส่งแต่ละโนดจึงทำให้สรุปได้ว่า ESS และแผนการเล่นของทั้งฝ่ายป้องกันและฝ่ายโจมตีของกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นจะมีค่าเหมือนกันกับกรณีการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาลง ในทำนองเดียวกัน ESS และแผนการเล่นของทั้งสองฝ่ายของกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงจะมีค่าเหมือนกันกับกรณีการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นเช่นกัน

4.2 การทดสอบกับโครงข่ายแบบตารางที่มีขนาดใหญ่ขึ้น

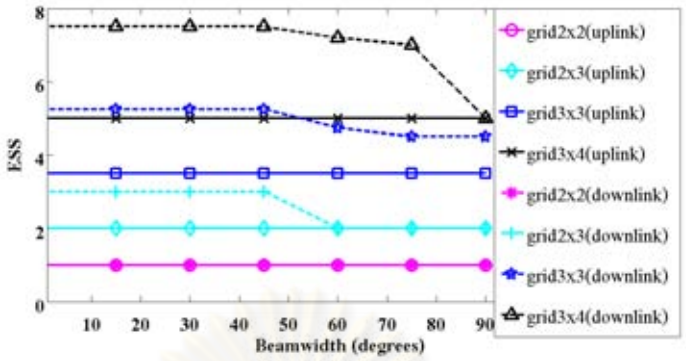


รูปที่ 4.7: โครงข่ายแบบตารางที่ใช้ในการทดสอบ

จาก [14] ได้มีการทดสอบกับโครงข่ายแบบตารางเนื่องจากเป็นโครงข่ายที่เชื่อมต่อแบบง่ายที่สามารถครอบคลุมพื้นที่ให้บริการได้โดยโครงข่ายที่นำมาทดสอบนั้นประกอบด้วยจุดเชื่อมต่อที่เป็นเกตเวย์ 2 จุดติดตั้งอยู่ที่มุมซ้ายบนและมุมขวาล่างของโครงข่าย ซึ่งในวิทยานิพนธ์นี้ได้ประยุกต์นำเอาสายอากาศระบุทิศทางเข้ามาเพื่อพัฒนาความปลอดภัยให้กับโครงข่ายมากยิ่งขึ้น รวมถึงได้ศึกษาและวิเคราะห์ผลกระทบต่าง ๆ ได้แก่ ผลกระทบของการเปลี่ยนแปลงค่าบีมวิดท์, ผลกระทบต่อโครงข่ายแบบหนาแน่น (dense network) และโครงข่ายแบบเบาบาง (sparse network), ผลกระทบต่อการเปลี่ยนตำแหน่งเกตเวย์ รวมถึงการวิเคราะห์ตำแหน่งของโนดแต่ละโนดที่มีผลต่อความปลอดภัยที่ต่างกันและสุดท้ายเป็นการเปรียบเทียบค่า ESS ว่ามีผลอย่างไรเมื่อผู้เล่นฝ่ายป้องกันและผู้เล่นฝ่ายโจมตีใช้วิธีอื่นนอกเหนือจากทฤษฎีเกม

4.2.1 ผลกระทบของการเปลี่ยนแปลงค่าบีมวิดท์

จากรูปที่ 4.8 เป็นกราฟแสดงความสัมพันธ์ระหว่าง ESS กับบีมวิดท์โดยทดสอบกับโครงข่ายแบบตารางดังรูปที่ 4.7 ซึ่งกำหนดให้ระยะทางในการส่งของโนดแต่ละโนดเท่ากันหมดและมีทิศทางในการส่งพุ่งตรงไปยังโนดปลายทางเสมอ จากผลการทดลองจะเห็นว่าในกรณีของการส่งข้อมูลฝั่งขาขึ้น ค่า ESS ที่ได้จะคงที่และไม่ขึ้นกับค่าบีมวิดท์ โดยมีจำนวนเซสชั่นที่ปลอดภัยเป็นครึ่งหนึ่งของจำนวนเซสชั่นทั้งหมด เพราะในกรณีการส่งข้อมูลฝั่งขาขึ้น



รูปที่ 4.8: ความแตกต่างของค่า ESS เมื่อมีการเปลี่ยนแปลงบีมวิดท์

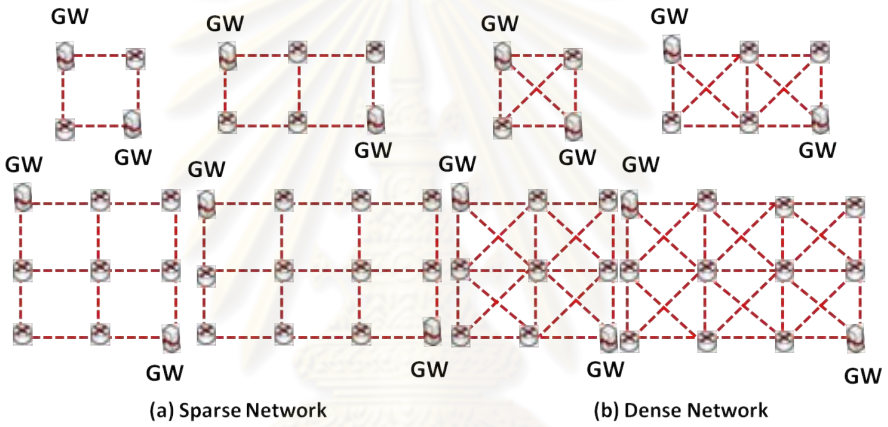
ผู้เล่นฝ่ายโจมตีจะสามารถดักฟังข้อมูลที่ส่งเข้ามายัง GW ตัวหนึ่งได้เสมอ และในโครงข่ายที่นำมาทดสอบนี้มี GW 2 ตัว ทำให้แผนการเล่นที่ดีที่สุดของผู้เล่นฝ่ายป้องกันคือการส่งข้อมูลไปยัง GW ทั้ง 2 ตัวแบบสุ่ม เพื่อหลบหลีกผู้เล่นฝ่ายโจมตีทำให้จำนวนเซสชั่นที่ปลอดภัยมีจำนวนครึ่งหนึ่งของจำนวนเซสชั่นทั้งหมด

ในกรณีการส่งข้อมูลฝั่งขาลงจะมีค่า ESS มากกว่ากรณีการส่งข้อมูลฝั่งขาขึ้น ภายใต้เงื่อนไขที่ว่าพื้นที่บีมที่ส่งออกจาก GW ตัวเดียวกันเพื่อส่งข้อมูลไปยังจุดเชื่อมต่อแต่ละตัวจะไม่ซ้อนทับกัน ซึ่งจากโครงข่ายแบบตารางที่นำมาทดสอบ ค่าบีมวิดท์จะต้องมีค่าไม่เกิน 90 องศา เพื่อให้เงื่อนไขตามที่กล่าวมาเป็นจริง ทำให้ในกรณีการส่งข้อมูลฝั่งขาลง แผนการเล่นที่ดีที่สุดของผู้เล่นฝ่ายโจมตีคือการไปดักฟังพื้นที่ที่มีการซ้อนทับกันของบีมที่มาจากจุดเชื่อมต่อต่าง ๆ มากที่สุด โดยการดักฟังพื้นที่ในกรณีนี้นั้นจะทำให้ดักฟังข้อมูลของเซสชั่นได้จำนวนน้อยกว่าในกรณีของการดักฟังบริเวณรอบ GW ของการส่งข้อมูลฝั่งขาขึ้น ยิ่งไปกว่านั้นในกรณีที่โครงข่ายมีขนาดใหญ่ขึ้น เนื่องจากมีจำนวน TAP ที่มากขึ้นเส้นทางในการส่งข้อมูลของผู้เล่นฝ่ายป้องกันเพื่อใช้ในการหลบหลีกจึงมีมากขึ้นด้วย ถึงแม้ว่าค่าบีมวิดท์จะมาก แต่ผู้เล่นฝ่ายโจมตีก็จะสามารถดักฟังข้อมูลจากโครงข่ายขนาดใหญ่ได้ยากกว่าโครงข่ายขนาดเล็ก และ ESS ในกรณีการส่งข้อมูลขาลงจะมีค่าลดลงเมื่อเพิ่มบีมวิดท์ โดยเมื่อเพิ่มบีมวิดท์ไปเรื่อย ๆ ค่า ESS จะลดลงก็ต่อเมื่อค่าบีมวิดท์ที่ค่านั้น ทำให้แผนของผู้เล่นฝ่ายโจมตีเปลี่ยนหรือทำให้เกิดพื้นที่ที่ผู้เล่นฝ่ายโจมตีมาดักฟังแล้วได้จำนวนเซสชั่นมากกว่าเดิม โดยเฉพาะอย่างยิ่งในบีมวิดท์ที่มีค่า 45 องศา จะเป็นค่าที่ทำให้เกิดพื้นที่ซ้อนทับของบีมเพิ่มขึ้น

จากผลการทดลองทำให้ขัดกับความรู้สึกที่ว่า เมื่อเราลดค่าบีมวิดท์ไปเรื่อย ๆ ค่า ESS จะไม่เพิ่มขึ้นตามเสมอไป ซึ่งในงานวิจัยนี้ได้นิยามต้นทุนแปรผกผันกับบีมวิดท์ ทำให้สามารถกล่าวอีกนัยได้ว่า การเพิ่มต้นทุนให้กับโครงข่ายนั้นอาจจะไม่ได้ทำให้ค่า ESS เพิ่มขึ้นเสมอไปยกตัวอย่างเช่นกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น ส่วนในกรณีการส่งข้อมูลฝั่งขาลงการเพิ่มต้นทุนจะต้องเพิ่มจนถึงค่าที่ทำให้บีมวิดท์แคบจนลดพื้นที่ที่เป็นแผนที่ดีที่สุดของผู้เล่นฝ่ายโจมตีใช้ในการโจมตีได้ จากผลการทดลองทำให้ทราบว่าจะในโครงข่ายรูปแบบต่าง ๆ ควรจะเพิ่มต้นทุนหรือลดบีมวิดท์เท่าไหร่เพื่อให้ค่า ESS นั้นเพิ่มขึ้น

4.2.2 การเปรียบเทียบค่า ESS ของโครงข่ายแบบหนาแน่นและโครงข่ายแบบเบาบางในโครงข่ายแบบตาราง

เพื่อต้องการศึกษาถึงการวางโครงข่ายแบบหนาแน่นและโครงข่ายแบบเบาบางโดยสมมติให้โครงข่ายที่ใช้ทดสอบจากรูปที่ 4.9(a) เป็นโครงข่ายแบบเบาบาง โดยกำหนดให้ระยะห่างระหว่างโนดห่างกัน 20 หน่วย และมีเกตเวย์ 2 ตัวอยู่ในตำแหน่งมุมซ้ายบนและมุมขวาล่าง กำหนดให้รัศมีการส่งสัญญาณไร้สายมีค่า 29 หน่วย หลังจากนั้นได้เพิ่มการเชื่อมต่อละหว่างโนดในแนวเส้นทะแยงมุมของทุกสี่เหลียมในโครงข่ายแบบตารางดังรูปที่ 4.9(b) ทำให้กลายเป็นโครงข่ายแบบหนาแน่น ซึ่งการทดสอบทั้ง 2 กรณีนี้จะทดสอบที่ค่าบีมวิดท์ 45 องศา เพราะเป็นค่าบีมวิดท์ที่ค่ามากที่สุดที่ไม่ทำให้เซกเตอร์จากจุดเชื่อมต่อต้นทางเดียวกันซ้อนทับกัน



รูปที่ 4.9: โครงข่ายแบบเบาบางและโครงข่ายแบบหนาแน่น

ตารางที่ 4.1: ค่า ESS ที่โครงข่ายขนาดต่าง ๆ ทั้งแบบเบาบางและแบบหนานแน่นในกรณีการดักฟังข้อมูล

Network	grid 2x2 (uplink,downlink)	grid 2x3 (uplink,downlink)	grid 3x3 (uplink,downlink)	grid 3x4 (uplink,downlink)
sparse	(1,1)	(2,3)	(3.5,5)	(5,7.5)
dense	(1,1)	(2,3)	(3.5,5.5)	(5,8.5)

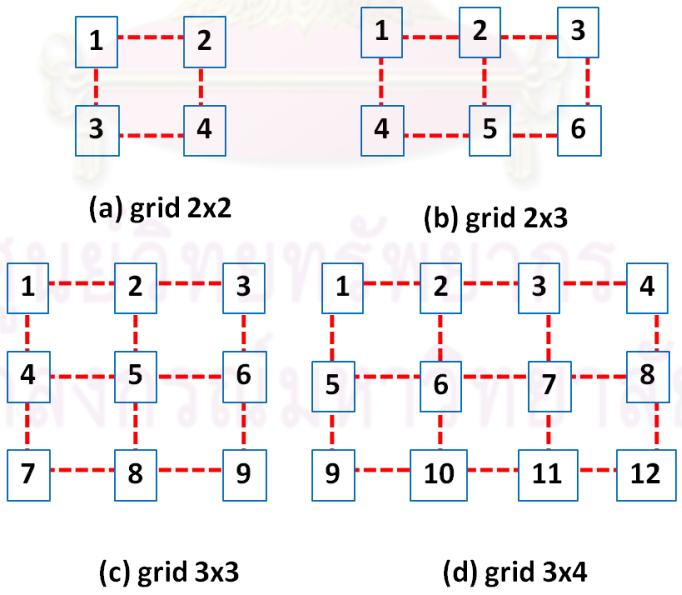
จากการทดสอบโครงข่ายในรูป 4.9(a) และ 4.9(b) พบว่าค่า ESS ของโครงข่ายแบบตารางขนาด 2x2 และ 2x3 ที่ได้มีค่าเท่ากันทั้งในกรณีการดักฟังและส่งสัญญาณรบกวนข้อมูลดังตารางที่ 4.1 และ 4.2 โดยแผนในการเล่นของผู้เล่นฝ่ายป้องกันก็ยังคงเหมือนเดิม นั้นหมายความว่าการที่เราเพิ่มการเชื่อมต่อในแต่ละโนดให้มีเส้นทางการส่งที่มากขึ้นดังรูปที่ 4.9(b) ไม่ได้ช่วยเพิ่มค่า ESS หรือเพิ่มความปลอดภัยให้กับโครงข่าย เพราะ ตำแหน่งที่ดีที่สุดจากทฤษฎีเกมของผู้เล่นฝ่ายโจมตีใช้เพื่อโจมตีโครงข่ายนั้น สามารถโจมตีได้ครอบคลุม

ตารางที่ 4.2: ค่า ESS ที่โครงข่ายขนาดต่าง ๆ ทั้งแบบเบาบางและแบบหนานแน่นในกรณีการส่งสัญญาณรบกวน

Network	grid 2x2 (uplink,downlink)	grid 2x3 (uplink,downlink)	grid 3x3 (uplink,downlink)	grid 3x4 (uplink,downlink)
sparse	(1,1)	(3,2)	(5,3.5)	(7.5,5)
dense	(1,1)	(3,2)	(5.5,3.5)	(8.5,5)

ข่ายเชื่อมโยงตามเส้นทะแยงมุมที่ได้เพิ่มเข้ามาเนื่องจากโครงข่ายมีขนาดเล็ก ทำให้แผนที่ดีที่สุดของผู้เล่นฝ่ายป้องกันในการส่งข้อมูลก็ยังคงเป็นการส่งตามเส้นรอบรูปของสี่เหลียมในรูป 4.9(a) เหมือนเดิม ส่วนในกรณีโครงข่ายแบบตารางขนาด 3x3 และ 3x4 จะพบว่าการดักฟังข้อมูลในกรณีการส่งข้อมูลฝั่งขาลง โครงข่ายแบบหนาแน่นจะให้ค่า ESS มากกว่าโครงข่ายแบบเบาบาง เนื่องจากการเชื่อมต่อตามแนวเส้นทะแยงมุมที่เพิ่มเข้ามาเป็นการเพิ่มเส้นทางการส่งข้อมูลหลบหลีกผู้เล่นฝ่ายโจมตีให้กับเกตเวย์ทำให้ค่า ESS ในกรณีนี้เพิ่มขึ้น ส่วนในการดักฟังกรณีการส่งข้อมูลฝั่งขาขึ้นนั้นถึงแม้ว่าจะมีการเพิ่มการเชื่อมโยงตามเส้นทะแยงมุมเข้ามาผู้เล่นฝ่ายโจมตีก็ยังคงสามารถโจมตีบริเวณพื้นที่รอบเกตเวย์เป็นผลทำให้สามารถดักฟังข้อมูลจากบีมที่พุ่งเข้าหาเกตเวย์ทั้งหมดได้

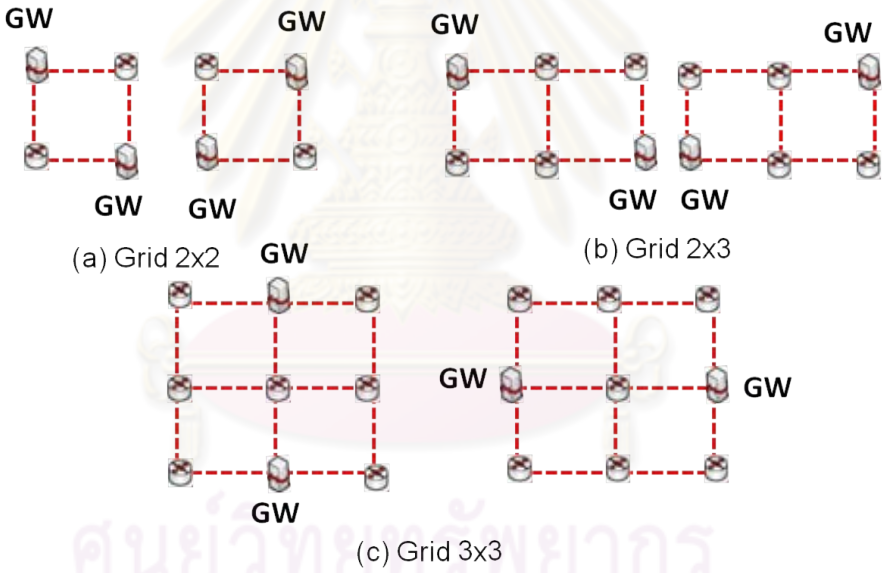
4.2.3 ผลกระทบต่อการเปลี่ยนตำแหน่งเกตเวย์



รูปที่ 4.10: ตัวเลขแทนตำแหน่งต่าง ๆ ในโครงข่ายแบบตาราง

ในหัวข้อการทดสอบนี้จะเป็นการศึกษาผลกระทบต่อค่า ESS เมื่อมีการเปลี่ยนตำแหน่งของเกตเวย์ โดยโครงข่ายที่นำมาทดสอบจะเป็นโครงข่ายดังรูปที่ 4.7 แต่ได้เปลี่ยนตำแหน่ง

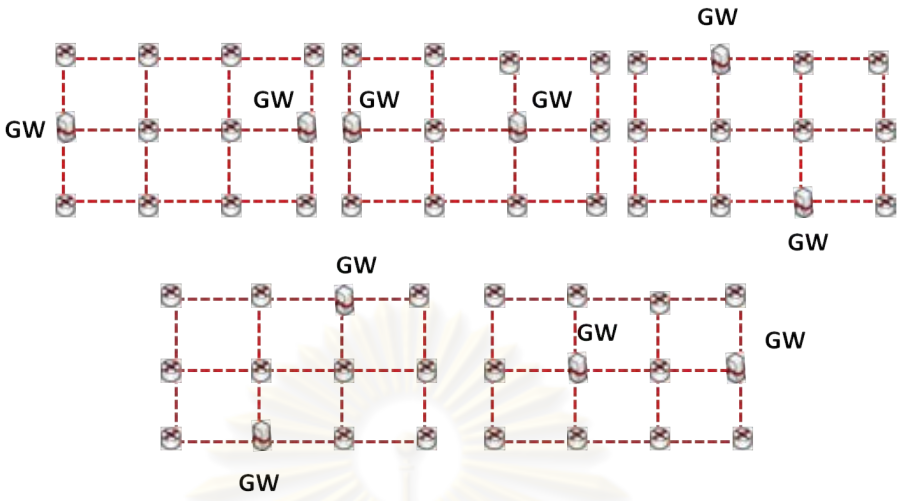
เกตเวย์ไปยังตำแหน่งต่าง ๆ แทนที่จุดเชื่อมต่อ โดยยังคงให้จำนวนของเกตเวย์มี 2 เกตเวย์เท่าเดิมและกำหนดให้ระยะห่างระหว่างโนดแต่ละตัวเป็น 20 หน่วย โดยให้บีมวิดทย์มีค่า 45 องศา ส่วนรัศมีในการส่งแต่ละโนดและรัศมีของการส่งสัญญาณรบกวนมีค่า 25 หน่วย ซึ่งตำแหน่งต่าง ๆ นั้นจะแทนด้วยตัวเลขดังรูปที่ 4.10 โดยผลการทดสอบโครงข่ายแบบตารางขนาด 2x2 ดังรูปที่ 4.10(a) พบว่า ตำแหน่งของเกตเวย์ที่ทำให้ค่า ESS สูงที่สุด คือ เกตเวย์อยู่ในตำแหน่งที่ 1, 4 ซึ่งหมายความว่าตำแหน่งที่ 2, 3 เป็นจุดเชื่อมต่อ เนื่องจากโครงข่ายเป็นโครงข่ายสมมาตรจึงสามารถให้เกตเวย์อยู่ในตำแหน่ง 2, 3 ได้ และให้ตำแหน่งที่ 1, 4 เป็นจุดเชื่อมต่อ ซึ่งการวางเกตเวย์แบบนี้จะทำให้ค่า ESS กรณีการดักฟังข้อมูลและการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงมีค่าเท่ากับ 1 แต่ถ้าวางเกตเวย์แบบอื่น เช่น ให้เกตเวย์อยู่ในตำแหน่ง 1, 3 แล้ว จะทำให้ผู้เล่นฝ่ายโจมตีสามารถดักฟังข้อมูลที่ทั้งออกและเข้าจากเกตเวย์ทั้ง 2 ตัวได้พร้อมกันทำให้ค่า ESS ในทุกกรณีมีค่าเท่ากับ 0 เพราะฉะนั้นตำแหน่งการวางเกตเวย์ที่ดีที่สุดของโครงข่ายแบบตารางขนาด 2x2 จะเป็นดังรูปที่ 4.11(a)



รูปที่ 4.11: ตำแหน่งเกตเวย์ที่ทำให้ค่า ESS สูงที่สุดในโครงข่ายแบบตารางขนาด 2x2, 2x3, 3x3

หลังจากนั้นได้ทดสอบกับโครงข่ายแบบตารางแต่ละขนาดดังรูปที่ 4.10(b), 4.10(c), 4.10(d) ทำให้พบว่าค่า ESS ในเกตเวย์ตำแหน่งต่าง ๆ และจากการโจมตีทั้งแบบดักฟังข้อมูลและส่งสัญญาณรบกวนมีค่าเป็นเท่าใด โดยแสดงค่าต่าง ๆ ออกมาในตารางที่ 4.3, 4.4, 4.5 เนื่องจากโครงข่ายขนาด 3x3 และ 3x4 มีตำแหน่งที่เป็นไปได้ของเกตเวย์เป็นจำนวนมากเพื่อให้กระชับจะขอแสดงค่าแค่ตำแหน่งที่ไม่ซ้ำเท่านั้น เนื่องจากโครงข่ายมีความสมมาตร โดยตำแหน่งของเกตเวย์ที่ทำให้ค่า ESS สูงที่สุดจะแสดงในรูปที่ 4.11(a), 4.11(b), 4.11(c) และ 4.12

จากผลการทดสอบจะสังเกตได้ว่าตำแหน่งเกตเวย์ที่ทำให้ค่า ESS สูงที่สุด จะเป็นตำแหน่งที่มีค่าองศาอิสระ (degree of freedom) มากกว่าตำแหน่งที่องศาอิสระน้อย



รูปที่ 4.12: ตำแหน่งเกตเวย์ที่ทำให้ค่า ESS สูงที่สุดในโครงข่ายแบบตารางขนาด 3x4

ตารางที่ 4.3: ค่า ESS ในตำแหน่งเกตเวย์ต่าง ๆ ของโครงข่ายแบบตารางขนาด 2x3

Position of GW (GW1,GW2)	Eavesdropping-case ESS (uplink,downlink)	Jamming-case ESS (uplink,downlink)
(1,2)	(2,2)	(2,2)
(1,3)	(2,2.5)	(2.5,2)
(1,4)	(0,0)	(0,0)
(1,5)	(2,2)	(2,2)
(1,6)	(2,3)	(3,2)
(2,3)	(2,2)	(2,2)
(2,4)	(2,2)	(2,2)
(2,5)	(2,2)	(2,2)
(2,6)	(2,2)	(2,2)
(3,4)	(2,3)	(3,2)
(3,5)	(2,2)	(2,2)
(3,6)	(0,0)	(0,0)
(4,5)	(2,2)	(2,2)
(4,6)	(2,2.5)	(2.5,2)
(5,6)	(2,2)	(2,2)

เนื่องจากยิ่งมีค่าองศาอิสระมากก็ยิ่งเหมือนกับมีเส้นทางในการที่จะหลบหลีกผู้โจมตีได้มาก ข้อสังเกตข้อที่สองคือตำแหน่งเกตเวย์ทั้งสองตัวนั้นจะต้องไม่อยู่ติดกัน ยกตัวอย่างเช่นในกรณีโครงข่ายขนาด 3x4 ถ้าเราให้เกตเวย์มีตำแหน่งที่ 6, 7 แล้ว จะเห็นได้ว่าที่ตำแหน่งเกตเวย์ทั้งสองอยู่มีค่าองศาอิสระ 4 ทั้งคู่ซึ่งเป็นค่าที่มากที่สุดถ้าเทียบกับที่ตำแหน่ง

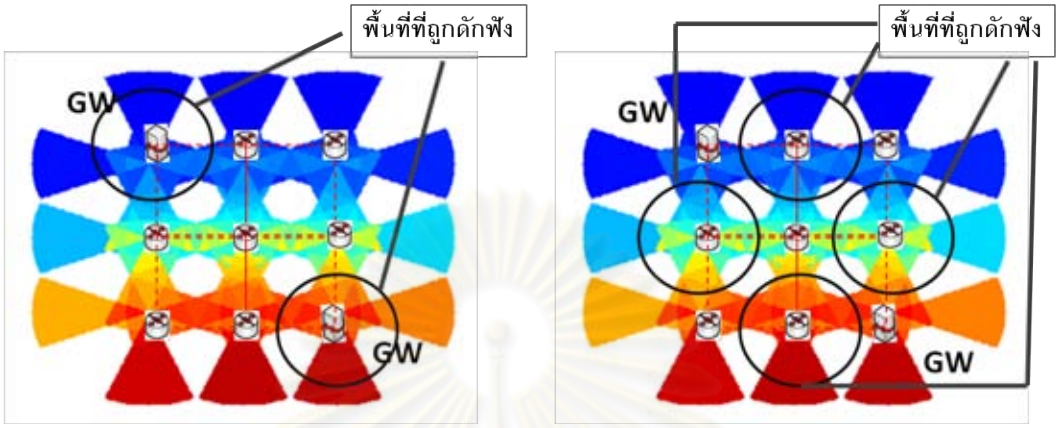
ตารางที่ 4.4: ค่า ESS ในตำแหน่งเกตเวย์ต่าง ๆ ของโครงข่ายแบบตารางขนาด 3x3

Position of GW (GW1,GW2)	Eavesdropping-case ESS (uplink,downlink)	Jamming-case ESS (uplink,downlink)
(1,2)	(3.5,5)	(5,3.5)
(1,3)	(3.5,4)	(4,3.5)
(1,5)	(3.5,4.5)	(4.5,3.5)
(1,6)	(3.5,5)	(5,3.5)
(1,9)	(3.5,5)	(5,3.5)
(2,4)	(3.5,4.5)	(4.5,3.5)
(2,5)	(3.5,4.5)	(4.5,3.5)
(2,8)	(3.5,5.5)	(5.5,3.5)

ตารางที่ 4.5: ค่า ESS ในตำแหน่งเกตเวย์ต่าง ๆ ของโครงข่ายแบบตารางขนาด 3x4

Position of GW (GW1,GW2)	Eavesdropping-case ESS (uplink,downlink)	Jamming-case ESS (uplink,downlink)
(1,2)	(5,5)	(5,5)
(1,3)	(5,6)	(6,5)
(1,4)	(5,6)	(6,5)
(1,5)	(5,5)	(5,5)
(1,9)	(5,5.5)	(5.5,5)
(1,10)	(5,6.5)	(6.5,5)
(1,11)	(5,7.5)	(7.5,5)
(1,12)	(5,7.6)	(7.6,5)
(2,5)	(5,6)	(6,5)
(2,6)	(5,6)	(6,5)
(2,6)	(5,7.3)	(7.3,5)
(2,10)	(5,7)	(7,5)
(2,11)	(5,8)	(8,5)
(5,7)	(5,8)	(8,5)
(5,8)	(5,8)	(8,5)
(6,7)	(5,7.3)	(7.3,5)

อื่น ๆ แต่กลับมีค่า ESS กรณีดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงน้อยกว่าในกรณีที่เกตเวย์วางอยู่ในรูปที่ 4.12 ทั้งนี้เพราะเมื่อเกตเวย์ทั้งสองตัวติดกันแล้วทำให้ผู้เล่นฝ่ายโจมตีสามารถดักฟังหรือส่งสัญญาณรบกวนข้อมูลที่ออกมาจากเกตเวย์ทั้งสองตัวพร้อมกันได้จึงเป็นเหตุทำให้ค่า ESS ลดต่ำลง



(a) กรณีการส่งข้อมูลฝั่งขาขึ้น (b) กรณีการส่งข้อมูลฝั่งขาลง

รูปที่ 4.13: พื้นที่ที่ผู้เล่นฝ่ายโจมตีเลือกในการโจมตีกรณีของการดักฟังข้อมูลของโครงข่ายแบบตาราง ขนาด 3x3 โดยมีเกตเวย์ในตำแหน่งที่ 1, 9

(a) กรณีการส่งข้อมูลฝั่งขาขึ้น (b) กรณีการส่งข้อมูลฝั่งขาลง

รูปที่ 4.14: พื้นที่ที่ผู้เล่นฝ่ายโจมตีเลือกในการโจมตีกรณีของการดักฟังข้อมูลของโครงข่ายแบบตาราง ขนาด 3x3 โดยมีเกตเวย์ในตำแหน่งที่ 2, 8

ข้อสังเกตอีกอย่างหนึ่งคือในโครงข่ายที่มีขนาดใหญ่ในที่นี้คือขนาด 3x3 และ 3x4 จะพบว่าการเปลี่ยนตำแหน่งของเกตเวย์นั้น ไม่มีผลต่อค่า ESS กรณีของการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นหรือการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาลง แต่จะมีผลเฉพาะกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงและการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นเท่านั้น เพื่อความชัดเจนและไม่สับสนจะขออธิบายจากการโจมตีแบบดักฟัง เหตุที่การเปลี่ยนตำแหน่งของเกตเวย์ส่งผลต่อ ESS กรณีการส่งข้อมูลฝั่งขาลงเท่านั้น เพราะว่าในการส่งข้อมูลฝั่งขาขึ้นผู้เล่นฝ่ายโจมตีจะเลือกดักฟังข้อมูลในพื้นที่รอบ ๆ เกตเวย์เท่านั้น ซึ่งแสดงในรูปที่ 4.13(a) และ 4.14(a) ทำให้ไม่ว่าจะย้ายตำแหน่งเกตเวย์ไปจุดใดผู้เล่นฝ่ายโจมตีก็จะยังคงโจมตีบริเวณรอบเกตเวย์ทั้งสองตัวเช่นเดิมเปรียบได้กับมีประตูทางหนีอยู่ 2 ประตูเท่านั้นทำให้ค่าความน่าจะเป็นในการหนีไปทางเกตเวย์ตัวที่ 1 และ 2 มีค่าอย่างละครึ่งเท่ากันจึงเป็นผลทำให้ค่า ESS กรณีการส่งข้อมูงฝั่งขาขึ้นมีค่าเป็นครึ่งหนึ่งของจำนวนเซสชั่นทั้งหมดเสมอ ถ้าหากว่าต้องการจะเพิ่มค่า ESS ของการส่งข้อมูงฝั่งขาขึ้นจะต้องเพิ่มที่จำนวนเกตเวย์แทน ต่อมาในส่วนการส่งข้อมูลฝั่งขาลงนั้นแผนที่ดีที่สุดของผู้เล่นฝ่ายโจมตีคือลือกดักฟังข้อมูลบริเวณรอบ ๆ จุดเชื่อมต่อที่ติดกับเกตเวย์ดังรูปที่ 4.13(b) และ 4.14(b) จึงทำให้การที่เกตเวย์มีค่าองศาอิสระมากเช่นตัวอย่างที่เกตเวย์อยู่ตำแหน่งที่ 2, 8 ดังรูปที่ 4.14 เกตเวย์ทั้งสองตัวมีค่าองศาอิสระตัวละ 3 ซึ่งเมื่อเทียบกับโครงข่ายที่เกตเวย์ตั้งอยู่ตำแหน่งที่ 1, 9 ดังรูปที่ 4.13 ซึ่งเกตเวย์แต่ละตัวมีค่าองศาอิสระอย่างละ 2 แล้ว ทำให้ผู้โจมตีจากที่โจมตีแค่ 4 บริเวณดังรูปที่ 4.13(b) กลับต้องเพิ่มมาโจมตี 5 บริเวณดังรูปที่ 4.14(b) จึงเป็นเหตุทำให้เส้นทางส่งข้อมูลหลบหลีกผู้เล่นฝ่ายโจมตีมีหลากหลายเส้นทางมากขึ้นเป็นผลทำให้ค่า ESS ในกรณีการส่งข้อมูลฝั่งขาลงมีค่าเพิ่มขึ้น

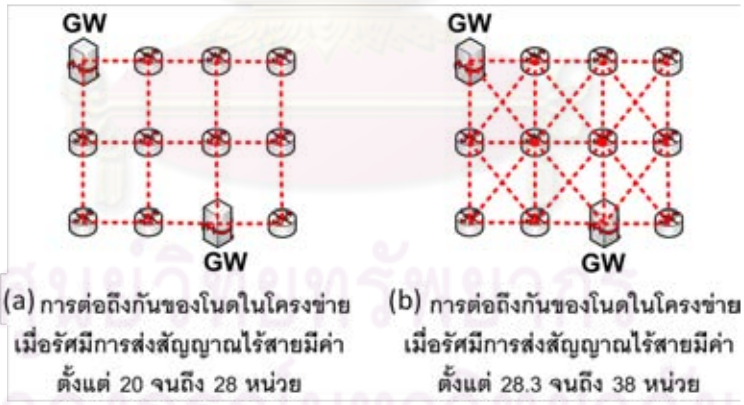
4.2.4 ผลกระทบของการเพิ่มรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่าย

รูปที่ 4.15: โครงข่ายแบบตารางขนาด 3x4 ที่ใช้ศึกษาผลกระทบต่อการเพิ่มรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่าย

การทดสอบในหัวข้อนี้เป็นการศึกษาต่อจากงานวิจัย [14] เพื่อศึกษาผลกระทบเมื่อเพิ่มรัศมีการส่งสัญญาณให้กับโนดในโครงข่ายไร้สายแบบเมช โดยทดสอบทั้งกรณีการดักฟังข้อมูลและการส่งสัญญาณรบกวน ซึ่งในกรณีของการส่งสัญญาณรบกวนนั้นจะให้รัศมีของสัญญาณรบกวนมีค่าเพิ่มขึ้นเท่ากับรัศมีการส่งของโนดในโครงข่ายเพื่อให้ผู้เล่นฝ่าย

โจมตีมีความเท่าเทียมไม่เสียเปรียบผู้เล่นฝ่ายป้องกัน เนื่องจากต้องการที่จะศึกษาผลกระทบของผู้เล่นฝ่ายป้องกันที่ใช้สายอากาศรอบทิศทางเปรียบเทียบกับสายอากาศระบุทิศทางจึงได้ทดสอบกับโครงข่ายที่ใช้ศึกษาผลกระทบของการเพิ่มรัศมีการส่งสัญญาณไร้สายจากงานวิจัย [14] โดยโครงข่ายที่นำมาทดสอบนั้นเป็นโครงข่ายที่มีโนดที่ 1 และ 11 เป็นเกตเวย์ดังรูปที่ 4.15 ส่วนโนดที่เหลืออีก 10 โนดจะเป็นจุดเชื่อมต่อผ่านทั้งหมด กำหนดให้ระยะทางระหว่างโนดเป็น 20 หน่วย ทั้งในแนวแกนตั้งและแนวแกนนอน โดยโนดทุกโนดจะมีรัศมีในการส่งสัญญาณไร้สายเริ่มต้นจาก 20 จนถึง 39 หน่วย สาเหตุที่เพิ่มรัศมีถึงแค่ 39 หน่วยเป็นเพราะถ้าหากเพิ่มรัศมีเกิน 39 หน่วยไปแล้วนั้นจะทำให้โนดในแกนเดียวกันสามารถส่งสัญญาณข้ามไปถึงกันได้ ยกตัวอย่างเช่นจากรูป 4.15 โนด 1 จะสามารถส่งสัญญาณไร้สายไปถึงโนดที่ 3 ได้ ทำให้ขัดกับเงื่อนไขที่กำหนดไว้ในหัวข้อที่ 3.3.1 นั่นคือจะไม่สามารถปรับค่าบีมวิดท์ที่ทำให้ส่งข้อมูลไปยังโนดที่ 2 และโนดที่ 3 โดยใช้คนละเซกเตอร์ได้ ส่วนในกรณีของการส่งสัญญาณรบกวนก็ได้เพิ่มรัศมีของสัญญาณรบกวนจาก 20 จนถึง 39 หน่วยเช่นกัน

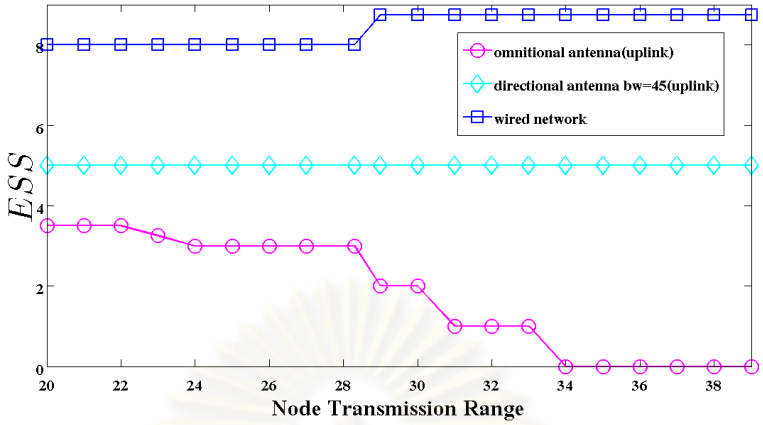
โดยในงานวิจัยนี้จะเปรียบเทียบกรณีที่ผู้เล่นฝ่ายป้องกันใช้สายอากาศระบุทิศทางกับสายอากาศรอบทิศทางและแบบโครงข่ายแบบสาย (wired network) ซึ่งในกรณีของสายอากาศระบุทิศทางนั้นจะเลือกใช้บีมวิดท์ที่มีค่า 45 องศา เพราะว่าเมื่อเพิ่มรัศมีแต่ละโนดเกิน 28.3 หน่วยจะทำให้การเชื่อมต่อถึงกันของโครงข่ายจากโครงข่ายแบบเบาบางจะกลายเป็นโครงข่ายแบบหนาแน่นดังรูปที่ 4.16 เมื่อโครงข่ายมีการเชื่อมต่อกันแบบรูปที่ 4.16(b) แล้ว ค่าบีมวิดท์ที่ค่ามากที่สุดที่ไม่ทำให้เซกเตอร์จากจุดเชื่อมต่อต้นทางเดียวกันซ้อนทับกันจะมีค่าเท่ากับ 45 องศาทำให้กำหนดค่าบีมวิดท์ที่ 45 องศาเป็นตัวแปรคงที่



รูปที่ 4.16: การต่อถึงกันที่เปลี่ยนไปเมื่อโนดในโครงข่ายไร้สายแบบเมชมีรัศมีการส่งสัญญาณเพิ่มขึ้น

จากผลการทดสอบพบว่าเมื่อเพิ่มรัศมีการส่งของโนดแต่ละโนดแล้วจะสามารถแยกวิเคราะห์แนวโน้มที่เกิดขึ้นได้ 3 กรณี คือ การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น การดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงและการส่งสัญญาณรบกวน โดยในแต่ละกรณีจะวิเคราะห์เปรียบเทียบผลที่ผู้เล่นฝ่ายป้องกันใช้สายอากาศระบุทิศทางกับสายอากาศรอบทิศทางและยังมีการเทียบกับโครงข่ายแบบมีสายด้วย ซึ่งได้ผลดังรูปที่ 4.17, 4.18 และ 4.19

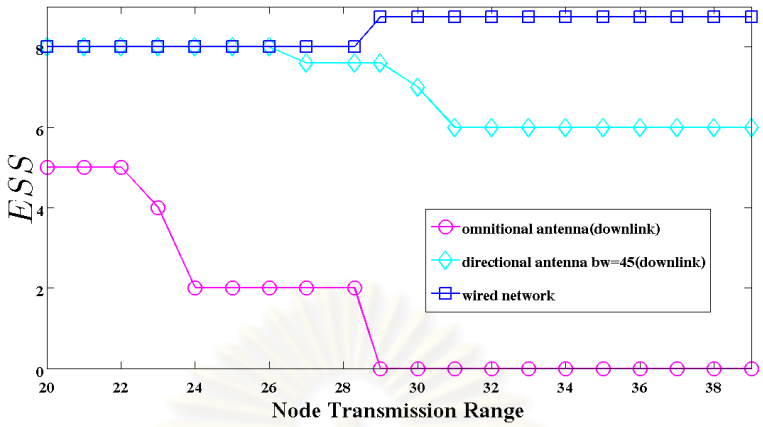
จากรูปที่ 4.17 จะแสดงให้เห็นว่าการเพิ่มรัศมีการส่งสัญญาณของโนดไร้สายในกรณีที่ใช้สายอากาศรอบทิศทางนั้น การเพิ่มรัศมีการส่งสัญญาณของโนดแต่ละโนดจะทำให้เกิด



รูปที่ 4.17: ผลกระทบของการเพิ่มรัศมีของโนดในโครงข่ายจากการถูกโจมตีแบบดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น

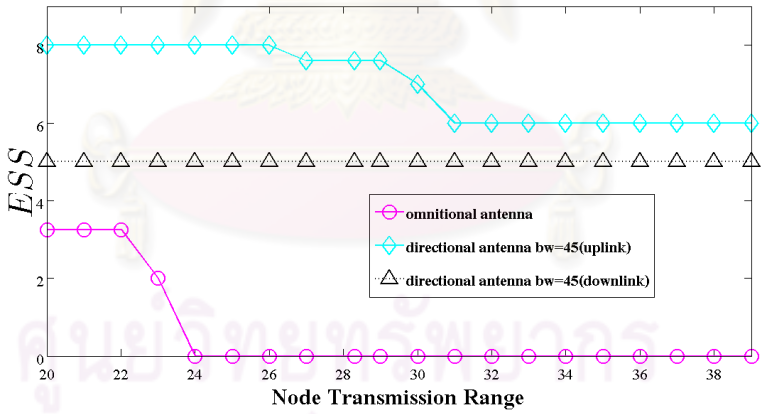
พื้นที่ที่ทำให้ผู้เล่นฝ่ายโจมตีสามารถดักฟังได้หลายคู่สายสื่อสารมากขึ้นทำให้ยิ่งเพิ่มรัศมีการส่งสัญญาณมากขึ้นเท่าไหร่ค่า ESS ก็จะยิ่งลดลงไปเรื่อย ๆ จนค่าเป็นศูนย์ในที่สุด ซึ่งค่าที่ลดลงเป็นขั้น ๆ แสดงถึงการที่เกิดพื้นที่ใหม่ที่ทำให้ผู้เล่นฝ่ายโจมตีสามารถดักฟังข้อมูลได้มากขึ้น ส่วนในกรณีที่ผู้เล่นฝ่ายป้องกันใช้สายอากาศระบุทิศทางนั้นไม่มีผลต่อ ESS เพราะเนื่องจากการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นนั้น ผู้เล่นฝ่ายโจมตีจะเลือกโจมตีพื้นที่รอบบริเวณเกตเวย์ทั้งสองตัวเสมอนั่นคือเลือกพื้นที่ระหว่างเกตเวย์ตัวที่แรกหรือตัวที่สอง ทำให้จำนวนเซสชั่นที่ปลอดภัยมีค่าเป็นครึ่งหนึ่งของจำนวนเซสชั่นทั้งหมดเสมอนั้นก็คือมีค่าเท่ากับ 5 โดยตราบเท่าที่การเพิ่มรัศมีของโนดทำให้บีมที่หันทิศทางเข้าเกตเวย์ตัวแรกไม่ไปซ้อนทับกับพื้นที่บีมจากโนดอื่น ๆ ที่ส่งเข้าหาเกตเวย์ตัวที่สองแล้ว ค่า ESS ของผู้เล่นฝ่ายป้องกันใช้สายอากาศระบุทิศทางจากการถูกโจมตีแบบดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นจะมีค่าคงที่ ส่วนเมื่อเปรียบเทียบกับโครงข่ายแบบมีสายปรากฏว่าค่า ESS ของโครงข่ายมีสายจะคงที่ตลอดจนถึงค่ารัศมีเกิน 28.3 เพราะการเพิ่มรัศมีของโนดนั้นจะมีผลต่อ ESS ของโครงข่ายแบบมีสายก็ต่อเมื่อมีการเปลี่ยนแปลงรูปแบบโครงข่ายเกิดขึ้นเท่านั้น ทำให้เมื่อรัศมีของทุกโนดเกิน 28.3 หน่วยแล้ว รูปแบบโครงข่ายจะเปลี่ยนไปดังรูปที่ 4.16 ทำให้ผู้เล่นฝ่ายป้องกันมีเส้นทางในการที่จะหลบหลีกผู้เล่นฝ่ายโจมตีมากยิ่งขึ้นจึงเป็นผลทำให้ค่า ESS มีค่าสูงขึ้นเมื่อรัศมีการส่งสัญญาณมีค่ามากกว่า 28.3 หน่วย

จากรูปที่ 4.18 แสดงให้เห็นว่าการเพิ่มรัศมีของการส่งสัญญาณทุกโนดในโครงข่ายไร้สายทำให้ค่า ESS ของผู้เล่นฝ่ายป้องกันที่ใช้สายอากาศระบุทิศทางจากการถูกโจมตีแบบดักฟังในการส่งข้อมูลฝั่งขาลงมีค่าลดลงเป็นขั้น ๆ เนื่องจากการเพิ่มรัศมีของโนดนั้นทำให้เกิดพื้นที่ที่ซ้อนทับกันของบีมเพิ่มมากขึ้นจึงทำให้ผู้โจมตีดักฟังข้อมูลได้มากขึ้นซึ่งเหมือนกับในกรณีที่พึ่งกล่าวมา แต่ในกรณีของการส่งข้อมูลฝั่งขาลงนี้ ESS ของผู้เล่นฝ่ายป้องกันใช้สายอากาศระบุทิศทางนั้นจะมีค่าลดลงจาก ESS ของโครงข่ายแบบมีสายลดลงไปเรื่อย ๆ จนหยุดที่ค่าค่าหนึ่งซึ่งหมายความว่าการเพิ่มรัศมีของโนดไร้สายนั้นไม่สามารถเพิ่มพื้นที่ซ้อนทับกันของบีมที่จะทำให้ผู้เล่นฝ่ายโจมตีสามารถโจมตีได้ร้ายแรงมากขึ้นไปกว่านี้ ซึ่งจะแตกต่าง



รูปที่ 4.18: ผลกระทบของการเพิ่มรัศมีของโนดในโครงข่ายจากการถูกโจมตีแบบดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง

กับกรณีที่ผู้เล่นฝ่ายป้องกันใช้สายอากาศรอบทิศทางซึ่งเมื่อเพิ่มรัศมีของโนดไปถึงค่าที่ทำให้ผู้เล่นฝ่ายโจมตีสามารถโจมตีจุดเชื่อมต่อทุกจุดได้พร้อมกันจึงทำให้ค่า ESS ในกรณีนี้เป็นศูนย์

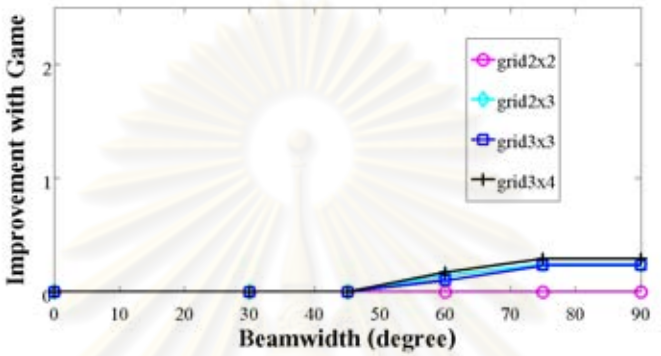


รูปที่ 4.19: ผลกระทบของการเพิ่มรัศมีของโนดในโครงข่ายจากการถูกโจมตีแบบส่งสัญญาณรบกวน

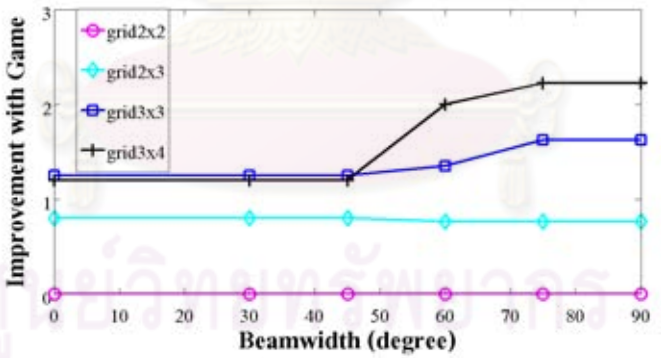
จากรูปที่ 4.19 แสดงให้เห็นว่าค่า ESS ที่เกิดจากการถูกส่งสัญญาณรบกวนในการส่งข้อมูลทั้งฝั่งขาขึ้นและฝั่งขาลงมีค่าไม่เท่ากัน ซึ่งแตกต่างจากค่า ESS กรณีที่ผู้เล่นฝ่ายป้องกันใช้สายอากาศรอบทิศทางซึ่งในงานวิจัยที่ [14] สรุปไว้ว่าการส่งสัญญาณรบกวนนั้นผู้เล่นฝ่ายโจมตีจะคำนึงแต่รัศมีการส่งของสัญญาณรบกวนเท่านั้น แต่ไม่ได้คำนึงถึงพื้นที่รัศมีของโนดที่ใช้ส่งข้อมูลในโครงข่าย ซึ่งแตกต่างจากการกรณีที่ใช้สายอากาศระบุทิศทางตรงที่ผู้เล่นฝ่ายโจมตีจะไม่ได้เพียงคำนึงถึงแต่รัศมีของสัญญาณรบกวนที่จะต้องครอบคลุมโนดที่จะโจมตีเท่านั้น แต่จะต้องอยู่ในตำแหน่งพื้นที่บีมที่โนดภาครับนั้นหันทิศทางมาเพื่อรับบีมจากโนดภาคส่งด้วยถึงจะสามารถรบกวนสัญญาณได้สำเร็จ โดยผลการทดสอบกรณีการส่ง

สัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงนั้นจะกลับกันกับของการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงและฝั่งขาขึ้นซึ่งตามที่ได้กล่าวในข้างต้นแล้ว

4.2.5 ผลกระทบ ต่อ ESS ใน กรณี ผู้ เล่น ฝ่าย ป้องกัน ส่ง ข้อมูล แต่ละ ทิศทาง ด้วย ความน่าจะเป็นแบบยูนิฟอร์ม



รูปที่ 4.20: ผลต่างระหว่าง ESS ในกรณีผู้เล่นฝ่ายป้องกันส่งข้อมูลโดยใช้ทฤษฎีเกมกับการส่งแบบยูนิฟอร์มในการส่งข้อมูลฝั่งขาขึ้น



รูปที่ 4.21: ผลต่างระหว่าง ESS ในกรณีผู้เล่นฝ่ายป้องกันส่งข้อมูลโดยใช้ทฤษฎีเกมกับการส่งแบบยูนิฟอร์มในการส่งข้อมูลฝั่งขาลง

จากรูปที่ 4.20 และ 4.21 เป็นความสัมพันธ์ระหว่างผลต่างของ ESS ในกรณีที่ผู้เล่นฝ่ายป้องกันส่งข้อมูลโดยใช้ทฤษฎีเกมกับ ESS ที่ส่งแบบยูนิฟอร์มเทียบกับค่าบีมวิดท์ แสดงให้เห็นว่าในกรณีของการส่งข้อมูลฝั่งขาขึ้น เมื่อค่าบีมวิดท์ต่ำกว่า 45 องศา การส่งข้อมูลแบบทฤษฎีเกมจะไม่ได้เพิ่มความสามารถในการหลบหลีกผู้เล่นฝ่ายโจมตี นั้นก็เพราะว่าจากผลที่กล่าวใน หัวข้อ 4.2.1 ทำให้รู้ว่าแผนที่ดีที่สุดของผู้เล่นฝ่ายป้องกันคือการส่งข้อมูลไปยัง GW 2 ตัวแบบสุ่ม ซึ่งการเลือกรูปแบบทรีในการส่งก็ไม่ได้แตกต่างจากการส่งแบบยูนิฟอร์ม ส่วนในกรณีเมื่อบีมวิดท์มีค่ามากกว่า 45 องศา จะเห็นได้ว่าในโครงข่ายตารางขนาด 2x3,

3x3, 3x4 การส่งแบบทฤษฎีเกมจะสามารถเพิ่มความสามารถในการหลบหลีกผู้เล่นฝ่ายโจมตีได้ เนื่องจากบีมวิดท์ที่เพิ่มขึ้นทำให้เกิดพื้นที่ที่เกิดจากการซ้อนทับกันของบีมแล้วทำให้ผู้เล่นฝ่ายโจมตีเลือกพื้นที่นั้นในการดักฟังแล้วได้จำนวนเซสชั่นที่มากขึ้น ซึ่งถ้าผู้เล่นฝ่ายป้องกันยังคงส่งข้อมูลแบบ ยูนิฟอร์มแล้ว จะทำให้จำนวนเซสชั่นที่ปลอดภัยจะน้อยกว่าครึ่งหนึ่งของจำนวนเซสชั่นทั้งหมด การส่งแบบทฤษฎีเกมจึงจำเป็นที่จะต้องใช้ในกรณีนี้ อย่างไรก็ตามในโครงข่ายตารางขนาด 2x2 จะเห็นได้ว่าการส่งข้อมูลแบบทฤษฎีเกมไม่ได้เพิ่มความสามารถในการหลบหลีกผู้โจมตีได้เลย เพราะว่าโครงข่ายมีขนาดเล็กมากจนไม่ว่าผู้เล่นฝ่ายป้องกันจะพยายามส่งข้อมูลด้วยทฤษฎีเกมแบบไหนก็ไม่สามารถหลบหลีกผู้เล่นฝ่ายโจมตีได้ดีไปกว่าการส่งข้อมูลแบบยูนิฟอร์ม

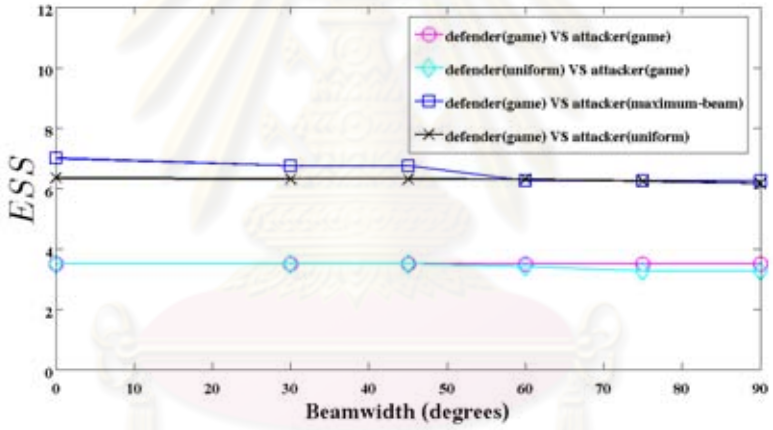
เมื่อพิจารณาการส่งข้อมูลฝั่งขาลงพบว่าการส่งข้อมูลแบบทฤษฎีเกมจะเพิ่มความสามารถในการหลบหลีกผู้เล่นฝ่ายโจมตีได้มากกว่าในกรณีของการส่งข้อมูลฝั่งขาขึ้นมาก เนื่องจากในการส่งข้อมูลฝั่งขาลงนั้น แผนการเล่นที่ดีที่สุดของผู้เล่นฝ่ายโจมตีคือเลือกพื้นที่ที่เกิดจากบีมที่ส่งมาจากจุดเชื่อมต่อแต่ละตัวซ้อนทับกันมากที่สุด ซึ่งเปรียบเสมือนเป็นหลุมพรางที่อยู่ตามเส้นทางต่าง ๆ ทำให้ถ้าหากผู้เล่นฝ่ายป้องกันเลือกส่งข้อมูลแบบยูนิฟอร์มแล้ว หมายความว่าจะเดินไปในทุกเส้นทางด้วยความน่าจะเป็นที่เท่ากันซึ่งจะมีโอกาสตกหลุมพรางได้มากกว่าในกรณีที่ส่งข้อมูลโดยใช้ทฤษฎีเกมซึ่งจะสามารถหลบหลีกเส้นทางที่คิดว่าจะมีหลุมพรางได้

จากรูปที่ 4.20 และ 4.21 แสดงให้เห็นว่าการเพิ่มความสามารถในการหลบหลีกของการส่งข้อมูลด้วยทฤษฎีเกมเทียบกับบีมวิดท์ส่วนใหญ่นั้นจะเป็นฟังก์ชั่นเพิ่มแบบขั้นบันได ซึ่งหมายความว่ายิ่งบีมวิดท์มีค่ามากขึ้นก็จะยิ่งเพิ่มหลุมพรางในโครงข่ายมากขึ้นด้วยทำให้การส่งข้อมูลแบบทฤษฎีเกมจึงยิ่งจำเป็นและยิ่งเพิ่มความสามารถในการหลบหลีกได้มากขึ้นเรื่อย ๆ แต่อย่างไรก็ตามในโครงข่ายตารางขนาด 2x3 กรณีการส่งข้อมูลฝั่งขาลง กลับพบว่าการส่งข้อมูลแบบทฤษฎีเกมแทบจะไม่เพิ่มความสามารถในการหลบหลีกให้มากขึ้นเลยเมื่อบีมวิดท์มีค่ามากขึ้น เพราะจากรูปที่ 4.3 ผู้เล่นฝ่ายโจมตีจะเลือกดักฟังในพื้นที่ระหว่างจุดเชื่อมต่อ 2 และจุดเชื่อมต่อ 5 เสมอ เปรียบเสมือนการมีหลุมพรางอยู่ระหว่างเส้นทางและจำนวนเส้นทางนั้นมีน้อยมากเมื่อเทียบกับในโครงข่ายแบบตารางขนาด 3x3 และ 3x4 ทำให้ไม่ว่าการส่งข้อมูลแบบทฤษฎีเกมจะพยายามหลบหลีกหลุมพรางอย่างไร แต่ด้วยจำนวนเส้นทางที่น้อยจึงไม่สามารถหลบหลีกได้ดีไปกว่านี้ จากผลการทดลองทำให้ทราบว่าสถานการณ์ไหนผู้เล่นฝ่ายป้องกันควรจะส่งข้อมูลแบบทฤษฎีเกมและสถานการณ์ไหนควรจะส่งข้อมูลแบบยูนิฟอร์ม ทำให้สามารถเลือกรูปแบบในการส่งข้อมูลได้เหมาะสมกับสถานการณ์

4.2.6 ผลกระทบต่อ ESS ในกรณีผู้เล่นฝ่ายโจมตีเลือกพื้นที่ในการโจมตีแบบยูนิฟอร์มและแบบพื้นที่ทับซ้อนบีมที่มากที่สุด

จากหัวข้อที่ผ่านมาจะเป็นการเทียบความแตกต่างระหว่างผู้เล่นฝ่ายป้องกันที่ใช้ทฤษฎีเกมในการเลือกรูปแบบทรีกับการเลือกรูปแบบทรีแบบยูนิฟอร์ม ส่วนในหัวข้อนี้จะเป็นการเปรียบเทียบการเลือกรูปแบบพื้นที่โจมตีของผู้เล่นฝ่ายโจมตี ซึ่งจะมีวิธีเลือก 3 แบบ แบบแรกคือแบบทฤษฎีเกม แบบที่สองคือแบบพื้นที่ของบีมที่มีการทับซ้อนมากที่สุดหมายถึงผู้เล่นฝ่ายโจมตีจะเลือกตำแหน่งโจมตีในพื้นที่มีบีมซ้อนทับกันมากที่สุดโดยถ้าเกิดมีพื้นที่

ซ้อนทับกันของบีมมากกว่า 1 ตำแหน่งก็จะทำการแบ่งค่าความน่าจะเป็นในการเลือกพื้นที่นั้น ๆ เท่ากันและแบบสุดท้ายคือแบบยูนิฟอร์มหมายถึงผู้เล่นฝ่ายโจมตีเลือกพื้นที่ในการโจมตีทั้งหมดด้วยค่าความน่าจะเป็นที่เท่ากัน โดยจะยกตัวอย่างผลการทดสอบของโครงข่ายแบบตารางขนาด 3x3 ดังรูปที่ 4.7 กำหนดให้ทุกโนดมีระยะห่างกัน 20 หน่วยและให้รัศมีการส่งสัญญาณไร้สายเท่ากับ 25 หน่วย โดยมีเกตเวย์ 2 ตัวอยู่ที่มุมซ้ายบนและมุมขวาล่าง ทำการทดสอบ 4 กรณีโดย กรณีแรกจะเป็นกรณีที่ผู้เล่นฝ่ายป้องกันและฝ่ายโจมตีใช้ทฤษฎีเกมในการเลือกแผนของตัวเองทั้งคู่ กรณีที่สองจะเป็นกรณีที่ผู้เล่นฝ่ายป้องกันเลือกแผนแบบยูนิฟอร์มส่วนผู้เล่นฝ่ายโจมตีเลือกโจมตีแบบทฤษฎีเกม กรณีที่สามจะเป็นกรณีที่ผู้เล่นฝ่ายป้องกันใช้ทฤษฎีเกมในการเลือกแผนส่วนผู้เล่นฝ่ายโจมตีเลือกพื้นที่ที่เกิดการซ้อนทับกันของบีมมากที่สุด และกรณีสุดท้ายจะเป็นกรณีที่ผู้เล่นฝ่ายป้องกันใช้ทฤษฎีเกมในการเลือกแผนส่วนผู้เล่นฝ่ายโจมตีจะเลือกพื้นที่โจมตีเป็นแบบยูนิฟอร์ม ซึ่งจะแสดงผลการทดสอบแยกเป็นการส่งข้อมูลฝั่งขาขึ้นและการส่งข้อมูลฝั่งขาลงตามลำดับดังรูปที่ 4.22 และ 4.23

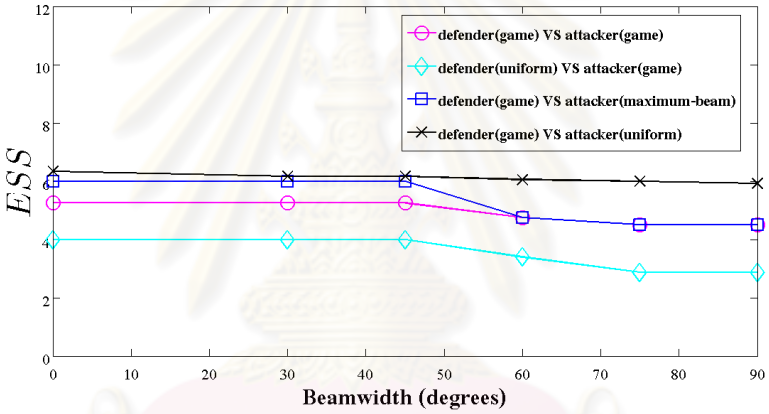


รูปที่ 4.22: ความแตกต่างของค่า ESS เมื่อผู้เล่นแต่ละฝ่ายเลือกรูปแบบแผนการเล่นด้วยวิธีต่าง ๆ กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นและกรณีการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาลง

จากรูปที่ 4.22 แสดงให้เห็นว่ากรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นนั้นที่ค่าบีมวิดท์ต่ำกว่า 45 องศา ผู้เล่นฝ่ายโจมตีที่เลือกพื้นที่ดักฟังข้อมูลด้วยความน่าจะเป็นแบบยูนิฟอร์มจะสามารถดักฟังข้อมูลได้มากกว่าผู้โจมตีที่เลือกพื้นที่ในการดักฟังแบบพื้นที่ซ้อนทับกันของบีมมากที่สุด เพราะว่าจากหัวข้อที่ 4.2.1 ทำให้ทราบว่าพื้นที่ดักฟังที่ดีที่สุดของผู้โจมตีคือพื้นที่ซ้อนทับกันของบีมบริเวณรอบ ๆ เกตเวย์ แต่ในที่นี้พื้นที่ซ้อนทับกันมากที่สุดของบีมกลับไปอยู่บริเวณของจุดเชื่อมต่อที่อยู่ตรงกลางของโครงข่ายทำให้ผู้โจมตีดักฟังข้อมูลได้น้อยกว่าการเลือกพื้นที่แบบสุ่มหรือแบบยูนิฟอร์ม แต่เมื่อบีมวิดท์ยิ่งกว้างทำให้เกิดพื้นที่ในการซ้อนทับกันของบีมมากขึ้นเป็นผลให้เกิดพื้นที่ทับซ้อนของบีมบริเวณรอบเกตเวย์เพิ่มขึ้นทำให้ผู้โจมตีที่เลือกพื้นที่การซ้อนทับกันของบีมมากที่สุดสามารถดักฟังข้อมูลได้มากขึ้นเท่ากับการเลือกพื้นที่แบบสุ่ม ส่วนในกรณีของการส่งสัญญาณรบกวนนั้นจะเหมือนกับในกรณี

ของการดักฟังข้อมูลแต่บีมที่เลือกเพื่อดักฟังข้อมูลนั้นจะเปลี่ยนเป็นการส่งสัญญาณรบกวนไปยังบีมที่หันมารับข้อมูลของโนดปลายทาง

ยิ่งไปกว่านั้นจากกราฟยังแสดงให้เห็นว่าในโครงข่ายนี้ผู้เล่นฝ่ายโจมตีเป็นฝ่ายที่ต้องการใช้ทฤษฎีเกมมากกว่าผู้เล่นฝ่ายป้องกัน เพราะในกรณีที่ผู้เล่นฝ่ายโจมตีเลือกพื้นที่ในการโจมตีแบบอื่น ๆ ที่ไม่ใช้ทฤษฎีเกมค่า ESS จะแตกต่างเมื่อเทียบกับตอนใช้ทฤษฎีเกมมากกว่าความแตกต่างกรณีผู้เล่นฝ่ายป้องกันที่ใช้ทฤษฎีเกมกับไม่ใช้ทฤษฎีเกม นั้นหมายความว่ากรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้นหรือการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาลงพื้นที่ในการโจมตีที่ดีที่สุดของผู้เล่นฝ่ายโจมตีจะมีจำนวนน้อยและจำเป็นที่จะต้องนำทฤษฎีเกมมาใช้ ซึ่งพื้นที่นั้นก็คือพื้นที่บริเวณรอบเกตเวย์ ผิดกับกรณีของผู้เล่นฝ่ายป้องกันที่สามารถส่งข้อมูลรูปแบบทรีออกไปแบบสุ่มซึ่งอาจจะได้ผลดีไม่เท่ากับการเลือกรูปแบบทรีด้วยเกมแต่ค่าของ ESS ก็ไม่แตกต่างกันมากนักเมื่อเทียบกับกรณีของผู้เล่นฝ่ายโจมตี



รูปที่ 4.23: ความแตกต่างของค่า ESS เมื่อผู้เล่นแต่ละฝ่ายเลือกรูปแบบแผนการเล่นด้วยวิธีต่าง ๆ กรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงและกรณีการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้น

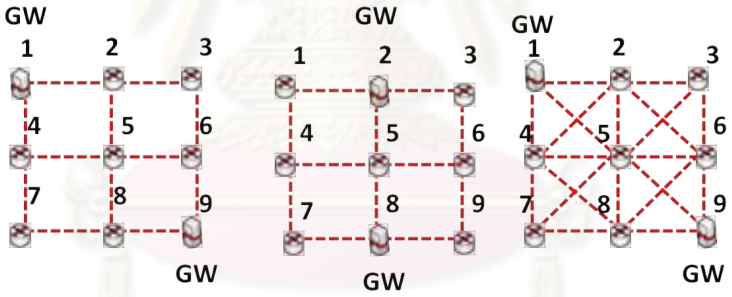
จากรูปที่ 4.23 แสดงให้เห็นว่ากรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลงหรือการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นนั้น จากหัวข้อที่ 4.2.1 ทำให้ทราบว่าพื้นที่ในการโจมตีที่ดีที่สุดคือบริเวณพื้นที่ซ้อนทับกันของบีมที่จุดเชื่อมต่อแต่ละตัวเป็นผลทำให้การเลือกพื้นที่โจมตีด้วยจำนวนการซ้อนทับของบีมที่มากที่สุดสามารถโจมตีโครงข่ายได้ร้ายแรงกว่าในกรณีการเลือกพื้นที่โจมตีแบบสุ่มหรือแบบยูนิฟอร์ม

ยิ่งไปกว่านั้นจากกราฟยังแสดงให้เห็นว่าในโครงข่ายนี้ผู้เล่นฝ่ายป้องกันเป็นฝ่ายที่ต้องการใช้ทฤษฎีเกมมากกว่าผู้เล่นฝ่ายโจมตี เนื่องจากความแตกต่างกันของค่า ESS ในกรณีที่ผู้เล่นฝ่ายป้องกันใช้และไม่ใช้ทฤษฎีเกมมีค่ามากกว่ากรณีที่ผู้เล่นฝ่ายโจมตีเลือกใช้พื้นที่ซ้อนทับของบีมมากที่สุดกับแบบทฤษฎีเกม เนื่องจากในหัวข้อที่ 4.2.5 ได้แสดงให้เห็นแล้วว่าการส่งรูปแบบทรีด้วยทฤษฎีเกมเทียบกับแบบยูนิฟอร์มในการดักฟังข้อมูลของการส่งข้อมูลฝั่งขาลงนั้นสามารถทำให้ค่า ESS สูงกว่าแบบยูนิฟอร์มมาก เนื่องจากกรณีนี้ผู้เล่นฝ่ายป้องกันต้องการทฤษฎีเกมมาเพื่อส่งข้อมูลหลบหลีกผู้เล่นฝ่ายโจมตีที่โจมตีอยู่

บริเวณรอบ ๆ จุดเชื่อมต่อที่มีพื้นที่บีมซ้อนทับกันหนาแน่น ตรงกันข้ามกับผู้เล่นฝ่ายป้องกันที่ถึงแม้จะเลือกพื้นที่ซ้อนทับกันของบีมมากที่สุดก็สามารถโจมตีข้อมูลที่ส่งไปหาจุดเชื่อมต่อได้ใกล้เคียงกับแบบทฤษฎีเกม

4.2.7 การวิเคราะห์เปรียบเทียบระดับความปลอดภัยที่ลดลงเมื่อเกิดความเสียหายกับจุดเชื่อมต่อที่ตำแหน่งต่าง ๆ

ในหัวข้อการทดสอบนี้จะเป็นการจำลองสถานการณ์ในโครงข่ายไร้สายแบบเมชโดยจะคิดค่า ESS ที่เกิดขึ้นจากการที่มีจุดเชื่อมต่อหนึ่ง ๆ เกิดความเสียหายไม่สามารถใช้การได้ เพื่อวิเคราะห์ถึงความสำคัญของจุดเชื่อมต่อตัวนั้น ๆ ว่ามีผลต่อค่าความปลอดภัยของทั้งโครงข่ายมากน้อยแค่ไหน ทำให้ในทางปฏิบัติสามารถบำรุงรักษาและตรวจเช็คสภาพจุดเชื่อมต่อที่มีความสำคัญต่อระบบเพื่อให้โครงข่ายโดยรวมมีประสิทธิภาพในแง่ของความปลอดภัย ในหัวข้อนี้จะทดสอบโดยใช้โครงข่ายดังรูปที่ 4.24 โดยโนดแต่ละโนดจะว่างห่างกัน 20 หน่วย และกำหนดให้รัศมีในการส่งสัญญาณไร้สายมีค่า 29 หน่วย ซึ่งจะทดสอบโดยการตัดจุดเชื่อมต่อออกจากโครงข่ายทีละตัวแล้วคำนวนค่า ESS ว่าเปลี่ยนแปลงไปมากหรือน้อย หลังจากนั้นก็ได้กำหนดค่าบีมวิดท์ของโนดในโครงข่ายให้มีค่าเท่ากันทุกโนดและมีค่าเป็น 0, 30, 45, 60, 75, 90 องศาตามลำดับ



รูปที่ 4.24: โครงข่ายแบบตารางขนาด 3x3 ที่ใช้เปรียบเทียบระดับความสำคัญของจุดเชื่อมต่อที่มีผลต่อความปลอดภัยของโครงข่าย

การคำนวนในหัวข้อนี้จะคำนวนค่าความปลอดภัยโดยคิดเป็นร้อยละจาก ESS ในกรณีของการดักฟังข้อมูลหารด้วยจำนวนเซสชั่นทั้งหมดเพื่อให้ค่าความปลอดภัยอยู่ในมาตรฐานเดียวกันซึ่งผลการทดสอบจะแสดงในตารางที่ 4.4 และ 4.5

จากตารางที่ 4.6 และ 4.7 ทำให้เห็นว่าการที่จุดเชื่อมต่อใดจุดเชื่อมต่อหนึ่งเกิดการเสียหายจะไม่มีผลต่อค่าความปลอดภัยของโครงข่ายในกรณีการส่งข้อมูลฝั่งขาขึ้นแต่อย่างใด เนื่องจากแผนการเล่นของผู้ดักฟังจะดักฟังบริเวณพื้นที่รอบเกตเวย์เท่านั้นทำให้ตราบใดที่มีเกตเวย์สองตัวถึงแม้จุดเชื่อมต่อใดจุดเชื่อมต่อหนึ่งจะเสียหายไปค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดจะยังคงมีค่า 50 เท่าเดิมเสมอ ส่วนในกรณีของการส่งข้อมูลฝั่งขาลงนั้นการเสียหายของจุดเชื่อมต่อบางตัวจะมีผลต่อค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมด ซึ่งจาก

ตารางที่ 4.6: ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดกรณีการดักฟังสัญญาณเมื่อตัดจุดเชื่อมต่อแต่ละจุดออกของโครงข่ายแบบตารางขนาด 3x3 โครงข่ายที่ 1

จุดเชื่อมต่อที่เสีย	$BW = \{0, 30, 45\}$	$BW = \{60\}$	$BW = \{75, 90\}$
(TAP or TAP)	(uplink,downlink)	(uplink,downlink)	(uplink,downlink)
ไม่มี TAP เสีย	(50.00,75.00)	(50.00,67.85)	(50.00,64.28)
3 or 5 or 7	(50.00,75.00)	(50.00,66.66)	(50.00,58.00)
2 or 4 or 6 or 8	(50.00,66.66)	(50.00,61.00)	(50.00,50.00)

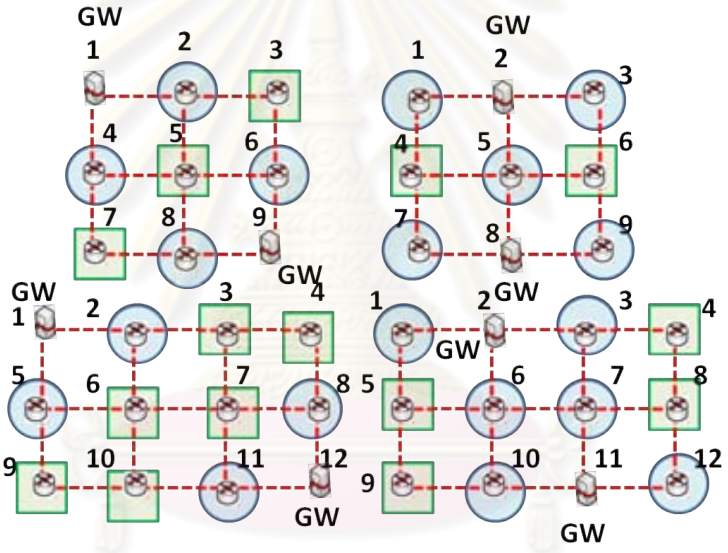
ตารางที่ 4.7: ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดกรณีการดักฟังสัญญาณเมื่อตัดจุดเชื่อมต่อแต่ละจุดออกของโครงข่ายแบบตารางขนาด 3x3 โครงข่ายที่ 2

จุดเชื่อมต่อที่เสีย	$BW = \{0, 30, 45\}$	$BW = \{60\}$	$BW = \{75, 90\}$
(TAP or TAP)	(uplink,downlink)	(uplink,downlink)	(uplink,downlink)
ไม่มี TAP เสีย	(50.00,75.00)	(50.00,67.85)	(50.00,64.28)
4 or 6	(50.00,75.00)	(50.00,66.66)	(50.00,58.00)
1 or 3 or 5 or 7 or 9	(50.00,66.66)	(50.00,61.00)	(50.00,50.00)

ผลการทดสอบทำให้เห็นว่าจุดเชื่อมต่อที่อยู่ติดกับเกตเวย์จะมีความสำคัญมากกว่าจุดเชื่อมต่อที่ไม่ติดกับเกตเวย์หรือกว่าอีกนัยนึงได้ว่าถ้าตัดจุดเชื่อมต่อที่อยู่ติดกับเกตเวย์ออกแล้วจะทำให้ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดลดลงมากกว่ากรณีที่ตัดจุดเชื่อมต่อที่ไม่ติดเกตเวย์ออก ที่เป็นเช่นนี้เพราะว่าการที่ตัดจุดเชื่อมต่อที่ติดกับเกตเวย์ออกนั้นเปรียบเหมือนกับการลดเส้นทางการส่งข้อมูลของผู้เล่นฝ่ายป้องกันที่ใช้หลบหลีกผู้เล่นฝ่ายโจมตีทำให้ผู้เล่นฝ่ายโจมตีมีโอกาสที่จะดักฟังข้อมูลได้มากขึ้นเป็นผลทำให้ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดลดลง ยิ่งไปกว่านั้นการเพิ่มของบีมวิดท์จะไม่มีผลต่อการเปลี่ยนแปลงระดับความสำคัญของจุดเชื่อมต่อแต่จะมีผลต่อค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดซึ่งถ้ายิ่งบีมวิดท์มีค่ามากความเสียหายของจุดเชื่อมต่อนั้นจะส่งผลกระทบต่อความปลอดภัยของโครางข่ายมากตามไปด้วยเช่นกัน

นอกจากนี้ยังได้ทดสอบกับโครงข่ายแบบหนาแน่นตามโครงข่ายที่ 3 ดังรูปที่ 4.24 ซึ่งกำหนดให้ค่าบีมวิดท์ทุดโนดเป็น 45 องศาตามการปรับค่าบีมวิดท์ที่เหมาะสมตามที่เคยกล่าวมา ปรากฏว่าเมื่อตัดจุดเชื่อมต่อ 2 หรือ 4 หรือ 6 หรือ 8 แล้วจะทำให้ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดของการส่งข้อมูลฝั่งขาลงเป็น 72 และเมื่อตัดจุดเชื่อมต่อ 3 หรือ 5 หรือ 7 จะทำให้ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดของการส่งข้อมูลฝั่งขาลงเป็น 76 ซึ่งมีค่าสูงกว่าโครงข่ายที่ 1 ในรูป 4.24 ซึ่งเป็นโครงข่ายแบบเบาบาง แสดงให้เห็นว่าในสถานการณ์ที่จุดเชื่อมต่อบางจุดเกิดเสียหายในโครงข่ายแบบหนาแน่นนั้นจะยังมีค่าความปลอดภัยสูงกว่าโครงข่ายแบบเบาบางในสถารการณ์เดียวกัน เพราะการที่แต่ละโนดมีองศาอิสระที่มากกว่าทำให้เมื่อมีจุดเชื่อมต่อบางจุดเกิดเสียหายก็ยังมีเส้นทางในการเลือกเพื่อหลบหลีกผู้โจมตีได้มากกว่า

ยิ่งไปกว่านั้นผลการทดสอบยังแสดงให้เห็นถึงจุดเชื่อมต่อจะแบ่งความสำคัญออกเป็นสองระดับ คือ ระดับแรกจะเป็นจุดเชื่อมต่อที่อยู่ติดกับเกตเวย์ซึ่งเมื่อติดจุดเชื่อมต่อใดจุดเชื่อมต่อหนึ่งออกแล้วค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดจะเท่ากับการตัดจุดเชื่อมต่ออื่น ๆ ที่ติดกับเกตเวย์เช่นกัน ในทำนองเดียวกับความสำคัญระดับสองจุดเชื่อมต่อที่ไม่ติดกับเกตเวย์จะให้ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดเท่ากันกับการตัดจุดเชื่อมต่อที่ไม่ติดกับเกตเวย์อื่น ๆ ซึ่งไม่ว่าจะอยู่ห่างจากเกตเวย์เป็นระยะเท่าใดก็ตามซึ่งจะแสดงจุดเชื่อมต่อที่สำคัญระดับแรกผ่านวงกลมสีน้ำเงินและที่สำคัญระดับสองด้วยสี่เหลี่ยมสีเขียวดังรูปที่ 4.25 โดยได้ทำการทดลองแบบเดียวกันกับโครงข่ายแบบตารางขนาด 3x4 อย่างไรก็ตามผลการวิเคราะห์นี้ใช้ได้กับโครงข่ายแบบตารางสมมาตรโดยถ้าเปลี่ยนรูปแบบของโครงข่ายแล้วก็จะมีผลต่อความสำคัญของจุดเชื่อมต่อแต่ละตัวแตกต่างกันแต่ในผลการทดสอบหัวข้อนี้ได้แสดงให้เห็นตัวอย่างของการคำนวนหาความสำคัญของแต่ละโนดเพื่อนำไปประยุกต์ใช้ได้ต่อไป



รูปที่ 4.25: ระดับความสำคัญของจุดเชื่อมต่อแต่ละตัวในโครงข่าย

ส่วนกรณีของการส่งสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้นค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดจะมีค่าเท่ากับกรณีดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง ในทำนองเดียวกันค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดของกรณีการส่งสัญญาณรบกวนฝั่งขาลงจะเท่ากับกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น โดยจะแสดงค่าค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดของกรณีการรบกวนสัญญาณในตารางที่ 4.8 และ 4.9 ซึ่งระดับความสำคัญของโนดยังเหมือนกรณีการดักฟังข้อมูลในรูปที่ 4.25

ตารางที่ 4.8: ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดกรณีการส่งสัญญาณรบกวนเมื่อตัดจุดเชื่อมต่อแต่ละจุดออกของโครงข่ายแบบตารางขนาด 3x3 โครงข่ายที่ 1

จุดเชื่อมต่อที่เสีย	$BW = \{0, 30, 45\}$	$BW = \{60\}$	$BW = \{75, 90\}$
(TAP or TAP)	(uplink,downlink)	(uplink,downlink)	(uplink,downlink)
ไม่มี TAP เสีย	(75.00,50.00)	(67.85,50.00)	(64.28,50.00)
3 or 5 or 7	(75.00,50.00)	(66.66,50.00)	(58.00,50.00)
2 or 4 or 6 or 8	(66.66,50.00)	(61.00,50.00)	(50.00,50.00)

ตารางที่ 4.9: ค่าร้อยละ ESS ต่อจำนวนเซสชั่นทั้งหมดกรณีการส่งสัญญาณรบกวนเมื่อตัดจุดเชื่อมต่อแต่ละจุดออกของโครงข่ายแบบตารางขนาด 3x3 โครงข่ายที่ 2

จุดเชื่อมต่อที่เสีย	$BW = \{0, 30, 45\}$	$BW = \{60\}$	$BW = \{75, 90\}$
(TAP or TAP)	(uplink,downlink)	(uplink,downlink)	(uplink,downlink)
ไม่มี TAP เสีย	(75.00,50.00)	(67.85,50.00)	(64.28,50.00)
4 or 6	(75.00,50.00)	(66.66,50.00)	(58.00,50.00)
1 or 3 or 5 or 7 or 9	(66.66,50.00)	(61.00,50.00)	(50.00,50.00)

4.3 การวิเคราะห์โครงข่ายสุ่ม

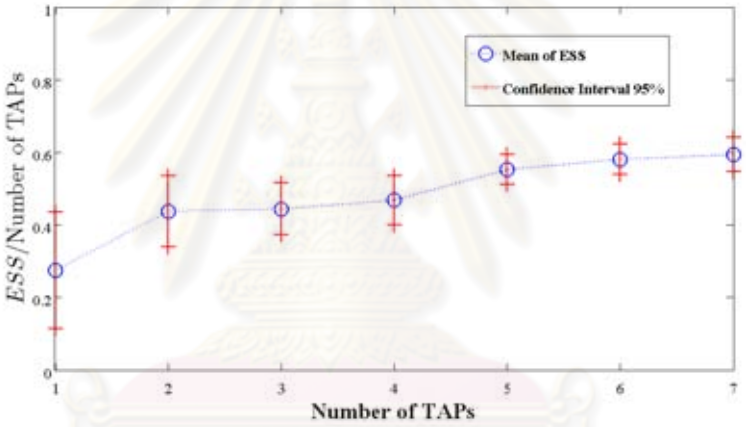
ในหัวข้อการทดสอบนี้จะเป็นการสุ่มโครงข่ายโดยใช้ Waxman topology generator [15]–[17] เป็นตัวสร้างโครงข่ายที่นิยมใช้กันอย่างแพร่หลาย ซึ่งโมเดลแบบ Waxman นี้จะมีค่าพารามิเตอร์อยู่ 4 ตัว ได้แก่ จำนวนของโนด, α, β และ โดเมน โดยในหัวข้อนี้จะแยกการทดสอบออกเป็น 2 ส่วน ส่วนแรกคือการทดสอบผลกระทบต่อ ESS ในโครงข่ายแบบสุ่มกรณีการดักฟังข้อมูลและส่วนที่สองจะเป็นการทดสอบผลกระทบต่อ ESS กรณีการส่งสัญญาณรบกวนโดยจะเพิ่มขนาดรัศมีของสัญญาณรบกวนขึ้นเรื่อย ๆ ในการทดสอบแรกนั้นพารามิเตอร์ตัวแรกคือจำนวนโนดและจากโมเดลของ Waxman ความน่าจะเป็นที่โนด u จะสามารถเชื่อมต่อกับโนด v ได้จะเป็นไปดังสมการ

$$P(u, v) = \alpha e^{\frac{-d}{\beta L}}, 0 < \alpha, 1 \leq \beta$$

- α คือพารามิเตอร์ที่กำหนดจำนวนลิงค์โดยค่ายิ่งมากจำนวนลิงค์ (link) จะมากตาม
- β คือพารามิเตอร์ควบคุมอัตราส่วนระหว่างลิงค์ที่ยาวต่อลิงค์ที่สั้น
- d คือระยะห่างระหว่างโนด u และโนด v
- L คือระยะห่างของโนด 2 ตัวใด ๆ ที่มากที่สุดในโครงข่าย

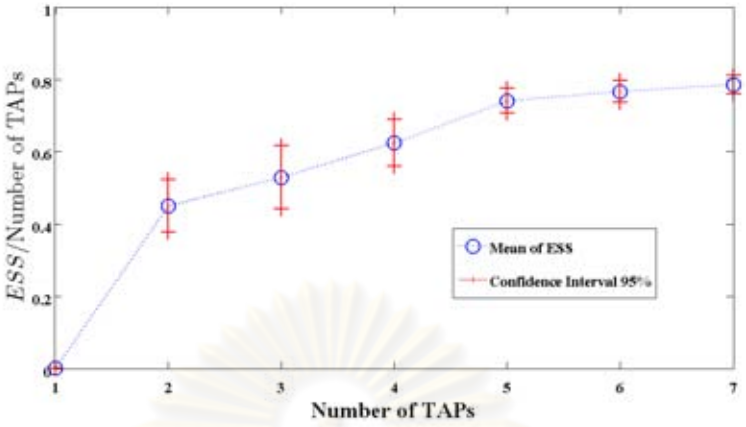
4.3.1 การวิเคราะห์ค่า ESS ในโครงข่ายสุ่มกรณีการดักฟังข้อมูล

กำหนดให้จำนวนโนดมีตั้งแต่ 3 โนดไปจนถึง 9 โนดส่วนค่า α = 1 และ β = 1 เพื่อทำให้โครงข่ายที่สุ่มออกมาเป็นโครงข่ายที่ไม่มีโครงข่ายย่อยแยกออกเป็นส่วน ๆ และมีการเชื่อมต่อกันอย่างหนาแน่นจนใกล้เคียงการเชื่อมต่อแบบเมช ส่วนพารามิเตอร์สุดท้าย domain คือช่วงที่จะใช้ในการสุ่มตำแหน่งของโนดซึ่งได้กำหนดในการทดสอบนี้เป็นช่วงสี่เหลี่ยมโดยมีค่า 10 ถึง 20 หน่วยทั้งในแนวแกนตั้งและแกนยาว เมื่อทำการสุ่มตำแหน่งของโนดในโครงข่ายออกมาแล้วในวิทยานิพนธ์นี้จะกำหนดเกตเวย์ 2 ตัวขึ้นจากโนดที่สุ่มมาได้โดยใช้ k-mean ซึ่งค่า k = 2 และกำหนดให้รัศมีในการส่งสัญญาณไร้สายของโนดทุกตัวเท่ากันหมด จากการทดสอบโครงข่ายสุ่มโดยสุ่มมาจำนวนโนดละ 20 ตัวอย่างกรณีดักฟังข้อมูลหลังจากนั้นได้คำนวนค่าเฉลี่ยของ ESS และคำนวนค่าความเชื่อมั่นที่ 95% (confedence interval 95%) และแยกกรณีการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงได้ผลดังรูปที่ 4.26 และ 4.27



รูปที่ 4.26: อัตราส่วน ESS ต่อจำนวนจุดเชื่อมต่อทั้งหมดในโครงข่ายแบบสุ่มกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาขึ้น

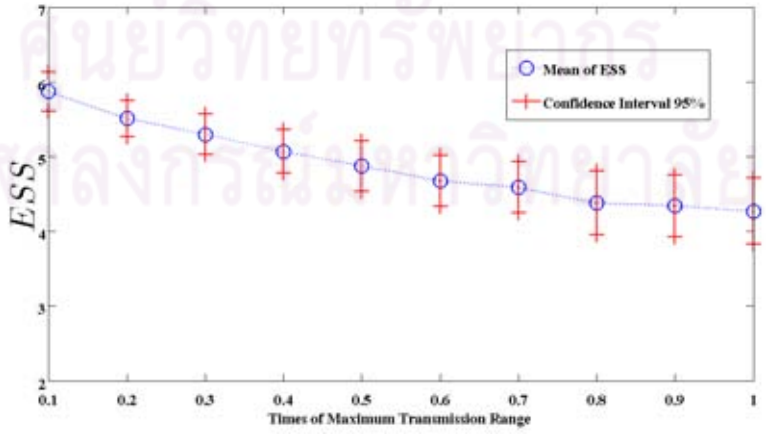
จากรูปที่ 4.26 และ 4.27 ทำให้เห็นแนวโน้มว่าเมื่อเพิ่มจำนวนโนดแล้วจะทำให้อัตราส่วนค่าเฉลี่ย ESS ต่อจำนวนเซสชั่นทั้งหมดจะเพิ่มขึ้นตาม เนื่องจากการเพิ่มของจำนวนโนดนั้นทำให้จำนวนเส้นทางในการส่งข้อมูลเพื่อหลบหลีบผู้โจมตีมีมากขึ้น อีกข้อสังเกตหนึ่งคืออัตราส่วนค่าเฉลี่ย ESS ต่อจำนวนเซสชั่นทั้งหมดในการส่งข้อมูลฝั่งขาลงจะมีค่ามากกว่าการส่งข้อมูลฝั่งขาขึ้น ทั้งนี้เป็นเพราะการดักฟังในการส่งข้อมูลฝั่งขาขึ้นนั้นพื้นที่ดีที่สุดจะเป็นพื้นที่บริเวณรอบ ๆ เกตเวย์ โดยยิ่งโครงข่ายไหนที่สุ่มออกมาแล้วมีเกตเวย์ติดกันและอยู่ตรงกลางของโครงข่ายโดยที่มีจุดเชื่อมต่ออยู่รอบ ๆ โครงข่ายนั้นค่า ESS จะต่ำมาก ในทางกลับกันการส่งข้อมูลฝั่งขาลงนั้นตำแหน่งที่ดีที่สุดในการดักฟังคือพื้นที่บริเวณจุดเชื่อมต่อต่าง ๆ เป็นผลทำให้ยิ่งจำนวนโนดเพิ่มขึ้นโอกาสที่ผู้เล่นฝ่ายโจมตีจะไปดักฟังข้อมูลบริเวณจุดเชื่อมต่อที่มีมากขึ้นก็จะยิ่งยาก ความชันของกราฟในการส่งข้อมูลฝั่งขาลงจึงสูงกว่ากรณีของการส่งข้อมูลฝั่งขาขึ้น



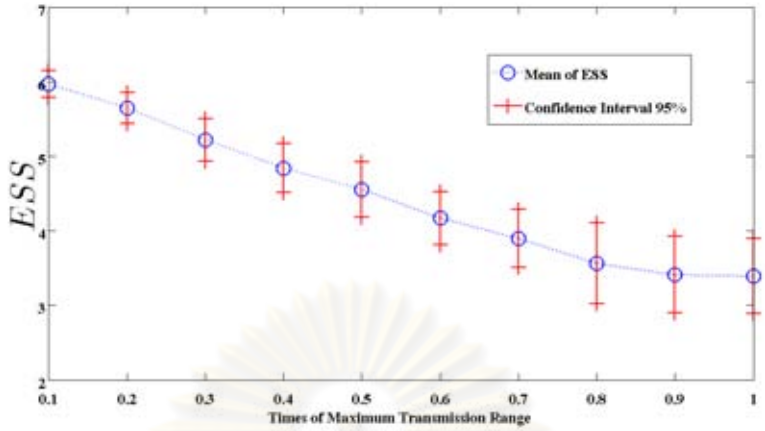
รูปที่ 4.27: อัตราส่วน ESS ต่อจำนวนจุดเชื่อมต่อทั้งหมดในโครงข่ายแบบสุ่มกรณีการดักฟังข้อมูลในการส่งข้อมูลฝั่งขาลง

4.3.2 การวิเคราะห์ค่า ESS ในโครงข่ายสุ่มกรณีการเพิ่มรัศมีของสัญญาณรบกวน

ในหัวข้อนี้จะเป็นการทดสอบผลกระทบต่อค่า ESS เมื่อผู้เล่นฝ่ายโจมตีเพิ่มรัศมีของการส่งสัญญาณรบกวนขึ้นเรื่อย ๆ โดยทำการสุ่มโครงข่าย 9 โนดขึ้นมาทั้งหมด 20 ตัวอย่างและกำหนดให้ค่า α = 0.5 และ β = 1 ค่า domain เป็นระยะทาง 10 ถึง 20 หน่วยทั้งแนวแกนตั้งและแกนนอน ซึ่งกำหนดรัศมีในการส่งสัญญาณรบกวนโดยเริ่มจาก 1 ใน 10 เท่าของรัศมีการส่งสัญญาณไร้สายของโนดอื่น ๆ ในโครงข่ายและจะเพิ่มรัศมีสัญญาณรบกวนไปทีละ 1 ใน 10 จนค่าเท่ากับรัศมีการส่งสัญญาณไร้สายของโนดในโครงข่าย จากผลการทดสอบได้แสดงโดยการหาค่าเฉลี่ย ESS และหาค่าความเชื่อมันที่ 95% ซึ่งได้แยกกรณีของการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงดังรูปที่ 4.28 และ 4.29 ตามลำดับ



รูปที่ 4.28: ผลกระทบต่อค่า ESS เมื่อผู้เล่นฝ่ายโจมตีเพิ่มรัศมีของสัญญาณรบกวนในการส่งข้อมูลฝั่งขาขึ้น



รูปที่ 4.29: ผลกระทบต่อค่า ESS เมื่อผู้เล่นฝ่ายโจมตีเพิ่มรัศมีของสัญญาณรบกวนในการส่งข้อมูลฝั่งขาลง

จากรูปที่ 4.28 และ 4.29 แสดงให้เห็นว่าการเพิ่มรัศมีของสัญญาณรบกวนนั้นมีผลทำให้ค่า ESS ลดลงเรื่อย ๆ และถ้าหากผู้เล่นฝ่ายโจมตีต้องการจะส่งสัญญาณรบกวนโนดในโครงข่ายจะต้องใช้รัศมีการส่งสัญญาณรบกวนเท่ากับรัศมีของการส่งสัญญาณไร้สายของโนดอื่น ๆ เพื่อให้ผลของการโจมตีร้ายแรงที่สุด ยิ่งไปกว่านั้นค่าเฉลี่ยของ ESS ในกรณีการส่งข้อมูลฝั่งขาลงจะต่ำกว่าในกรณีการส่งข้อมูลฝั่งขาขึ้นและความชันของกราฟในการส่งข้อมูลฝั่งขาลงจะสูงกว่า นั่นหมายความว่าการเพิ่มรัศมีของสัญญาณรบกวนและการส่งสัญญาณรบกวนมีผลต่อการส่งข้อมูลฝั่งขาลงมากกว่า เนื่องจากการส่งข้อมูลฝั่งขาลงนั้นเกตเวย์จะส่งข้อมูลไปยังจุดเชื่อมต่อต่าง ๆ ทำให้ผู้เล่นฝ่ายโจมตีสามารถส่งสัญญาณรบกวนจุดเชื่อมต่อที่ติดกับเกตเวย์ได้ง่ายโดยไปอยู่ในตำแหน่งพื้นที่บีมที่จุดเชื่อมต่อตัวนั้นหันมารับข้อมูลที่ส่งมาจากเกตเวย์ ซึ่งเมื่อเทียบกับกรณีการส่งข้อมูลฝั่งขาขึ้นผู้โจมตีจะต้องไปส่งสัญญาณรบกวนจุดเชื่อมต่ออื่น ๆ ในโครงข่ายแทนทำให้มีโอกาสที่จะรบกวนยากกว่า และในการเพิ่มรัศมีของสัญญาณรบกวนของการส่งข้อมูลฝั่งขาลงนั้นด้วยเหตุผลที่กล่าวมาทำให้เพิ่มประสิทธิภาพในการรบกวนสัญญาณได้ร้ายแรงกว่าในการส่งข้อมูลฝั่งขาขึ้นความชันของกราฟจึงมีค่าสูงกว่า

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

โครงข่ายไร้สายแบบเมชเป็นโครงข่ายที่ได้รับความสนใจเป็นอย่างมากทั้งในด้านการวิจัยและพัฒนา เนื่องจากมีข้อดีหลายประการทั้งการติดตั้งที่รวดเร็วประหยัดต้นทุนและมีความน่าเชื่อถือสูงเพราะเป็นการเชื่อมต่อกันแบบเมช แต่การสื่อสารผ่านตัวกลางไร้สายทำให้มีโอกาสถูกดักฟังข้อมูลและถูกส่งสัญญาณรบกวนการสื่อสารระหว่างโนดได้ง่าย โดยในอดีตได้มีงานวิจัยที่เสนอวิธีการจัดเส้นทางแบบเฟ้นสุ่มด้วยสายอากาศรอบทิศทาง ซึ่งถึงแม้ว่าการส่งข้อมูลไร้สายด้วยสายอากาศรอบทิศทางนั้นจะมีข้อดีในแง่ของพื้นที่ในการครอบคลุมที่กว้างแต่กลับเป็นการเพิ่มพื้นที่ให้ผู้โจมตีสามารถมาดักฟังหรือส่งสัญญาณรบกวนข้อมูลได้ร้ายแรงขึ้นอีกด้วย

ในวิทยานิพนธ์นี้จึงได้เสนอระเบียบวิธีการจัดเส้นทางแบบเฟ้นสุ่มโดยใช้สายอากาศระบุทิศทาง โดยประยุกต์ทฤษฎีเกมมาใช้เลือกการจัดเส้นทางแบบเฟ้นสุ่มเพื่อป้องกันการดักฟังข้อมูลและส่งสัญญาณรบกวนในโครงข่ายไร้สายแบบเมชในกรณีที่ร้ายแรงที่สุด ในระเบียบที่นำเสนอนั้นได้แสดงให้เห็นว่าการนำสายอากาศระบุทิศทางเข้ามาใช้ในโครงข่ายทำให้ค่า ESS มีค่าสูงขึ้น เนื่องจากเป็นการลดพื้นที่ใช้การโจมตีของผู้เล่นฝ่ายโจมตีไม่ให้สามารถโจมตีตำแหน่งที่มีหลายคู่โนดพร้อมกันได้ และแสดงระเบียบวิธีการคำนวนกรณีการส่งสัญญาณรบกวนโดยแยกได้เป็นการส่งข้อมูลฝั่งขาขึ้นและขาลง ซึ่งงานวิจัยในอดีตไม่ได้แยกคิดเป็นกรณีดังกล่าวทำให้ระเบียบที่นำเสนอในวิทยานิพนธ์ชิ้นนี้มีความเหมาะสมมากยิ่งขึ้น ผลการทดสอบพบว่า ในโครงข่ายแบบตารางการเปลี่ยนแปลงค่าบีมวิดท์ของกรณีการดักฟังข้อมูลจะมีผลต่อการส่งข้อมูลฝั่งขาลงเท่านั้นและค่า ESS ในการส่งข้อมูลฝั่งขาลงจะมากกว่าค่า ESS ในการส่งข้อมูลฝั่งขาขึ้นเสมอ และการเพิ่มการเชื่อมต่อในแนวเส้นทะแยงมุมของโครงข่ายแบบตารางจะไม่มีผลต่อค่า ESS และรูปแบบแผนการเล่นของผู้เล่นฝ่ายป้องกัน

ส่วนในกรณีการดักฟังของการส่งข้อมูลฝั่งขาขึ้นผู้เล่นฝ่ายโจมตีจะเลือกดักฟังข้อมูลในพื้นที่รอบ ๆ เกตเวย์เท่านั้น ทำให้ไม่ว่าจะย้ายตำแหน่งเกตเวย์ไปจุดใดผู้เล่นฝ่ายโจมตีก็จะยังคงโจมตีบริเวณรอบเกตเวย์ทั้งสองตัวเช่นเดิม ผลทำให้ค่า ESS กรณีการส่งข้อมูงฝั่งขาขึ้นมีค่าเป็นครึ่งหนึ่งของจำนวนเซสชั่นทั้งหมดเสมอ ถ้าหากว่าต้องการจะเพิ่มค่า ESS ของการส่งข้อมูงฝั่งขาขึ้นจะต้องเพิ่มที่จำนวนเกตเวย์แทน นอกจากนี้ยังได้เปรียบเทียบการที่ผู้เล่นแต่ละฝ่ายเลือกแผนการเล่นวิธีอื่น ๆ นอกจากทฤษฎีเกม ทำให้ทราบว่าโครงข่ายแบบหนึ่ง ๆ ทฤษฎีเกมได้ช่วยเพิ่มประสิทธิภาพให้กับผู้เล่นแต่ละฝ่ายมากน้อยแค่ไหนเมื่อเทียบกับการเลือกแผนวิธีอื่น ๆ รวมไปถึงการจำลองสถานการณ์โครงข่ายแบบตารางที่มีจุดเชื่อมต่อบางจุดเกิดเสียหายจะมีผลกระทบต่อค่า ESS โดยจุดเชื่อมต่อที่อยู่ติดกับเกตเวย์จะมีระดับความสำคัญสูงกว่าจุดเชื่อมต่อที่อยู่ถัดออกไป โดยจุดเชื่อมต่อที่ไม่ได้อยู่ติดกับเกตเวย์นั้นไม่ว่าจะห่างจากเกตเวย์มากน้อยแค่ไหนก็จะมีระดับความสำคัญเท่ากัน

สุดท้าย ได้ ทดสอบ กับ โครงข่าย แบบ สุ่ม ทำ ให้ ทราบ ว่า การ เปลี่ยนแปลง รูปแบบ ของ

โครงข่ายมีผลต่อค่า ESS และในกรณีของการดักฟังข้อมูลการส่งข้อมูลฝั่งขาลงจะมีค่าเฉลี่ย ESS สูงกว่าการส่งข้อมูลฝั่งขาขึ้นเสมอ ในทางกลับกันกรณีของการส่งสัญญาณรบกวนการส่งข้อมูลฝั่งขาขึ้นจะมีค่าเฉลี่ย ESS มากกว่าขาลงแทน เนื่องจากในกรณีการส่งข้อมูลฝั่งขาลงผู้โจมตีสามารถส่งสัญญาณรบกวนบริเวณรอบเกตเวย์ซึ่งครอบคลุมจุดเชื่อมต่อที่หันบีมมาเพื่อรับสัญญาณจากเกตเวย์ได้ทุกจุดเชื่อมต่อ ซึ่งการวิเคราะห์ทั้งหมดนี้จะเป็นประโยชน์ในการออกแบบโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทางที่มีความทนทางต่อการโจมตีที่สูงต่อไปได้ในอนาคต

5.2 ข้อเสนอแนะ

เพื่อให้งานวิจัยมีคุณค่ามากขึ้นระเบียบวิธีที่นำเสนอในวิทยานิพนธ์สามารถนำมาวิจัยต่อเพิ่มเติมหลายด้านได้ดังนี้

ด้านการจำลองโครงข่ายให้มีประสิทธิภาพและเหมือนในทางปฏิบัติมากยิ่งขึ้นโดยการคิดโอกาสที่การส่งข้อมูลจะเกิดการผิดพลาด ซึ่งคำนวนออกมาเป็นค่าความน่าจะเป็นหรืออีกวิธีคือโอกาสในการที่ข้อมูลจะถูกดักฟังหรือถูกสัญญาณรบกวนนั้นจะไม่ได้ถูกโจมตีได้เสมอไปแต่ขึ้นกับความน่าจะเป็นที่จะสามารถดักฟังหรือส่งสัญญาณรบกวนสำเร็จด้วย หรือในกรณีการส่งสัญญาณรบกวนอาจมีการคำนวนค่าอัตราส่วนสัญญาณต่อสัญญาณรบกวนเพื่อคำนวนรัศมีที่สัญญาณรบกวนจะมีผลต่อโนดในโครงข่าย และในวิทยานิพนธ์นี้ได้ใช้วิธีหาผลเฉลยแบบ MSA ซึ่งสามารถแก้ปัญหาเชิงสถิติและเชิงพลวัตได้แต่อาจจะต้องใช้เวลานานในการประมวลผลจึงอาจจะหาวิธีการคำนวนหาผลเฉลยแบบอื่นเพื่อเพิ่มประสิทธิภาพและความเร็วในการประมวลผลของการคำนวน

ด้านการจำลองด้วยทฤษฎีเกมอาจพัฒนาได้หลายอย่าง เช่น การวิเคราะห์หาจุดอานม้า คือ จุดที่ไม่ทำให้แผนการของผู้เล่นทั้งสองเลื่อนไปเลื่อนมาได้ การจำลองวิธีโดยใช้เกมแบบอื่น ๆ ที่ไม่ใช่เกมที่มีผู้เล่นสองคนรวมกันเป็นศูนย์ เช่น บางงานวิจัย [24] ได้จำลองเกมแบบมีการร่วมมือกันและขัดแย้งกันโดยมีผู้ดักฟังมาคอยดักฟังข้อมูลในโครงข่ายแต่ขณะเดียวกันก็มีผู้ที่ส่งสัญญาณรบกวนแต่มาส่งสัญญาณรบกวนผู้ดักฟังซึ่งเป็นการร่วมมือระหว่างฝ่ายป้องกันและผู้ส่งสัญญาณรบกวนโครงข่าย นอกจากนี้ในกรณีที่มีผู้โจมตีมากกว่าหนึ่งคน เช่น 2 คนจะสามารถแยกเป็นกรณีผู้โจมตีแต่ละคนร่วมมือกันเพื่อโจมตีผู้เล่นฝ่ายป้องกันหรือแบบต่างคนต่างโจมตีซึ่งการคำนวณควรจะคำนวนในกรณีที่ผู้โจมตีร่วมมือกันเพื่อคิดกรณีที่ถูกโจมตีร้ายแรงที่สุดโดยทำให้สามารถการันตีค่าความคาดหวังของเซสชั่นที่ปลอดภัยได้

ด้านรูปแบบของโครงข่ายในวิทยานิพนธ์นี้ไม่ได้เสนอรูปแบบหรือค่าบีมวิดท์ที่ทำให้ค่า ESS สูงที่สุด แต่ได้วิเคราะห์ถึงผลกระทบในด้านต่าง ๆ ที่มีผลต่อความปลอดภัยของโครงข่าย ซึ่งการพัฒนาอาจทำได้โดยหารูปแบบที่ดีที่สุดของการวางโนดจำนวนหนึ่ง ๆ หรือคำนวนเป็นอัลกอริทึมหาค่าบีมวิดท์ที่ทำให้ค่าความปลอดภัยต่อโครงข่ายสูงที่สุดแต่อย่างไรก็ตามในทางปฏิบัติการที่จะทำให้บีมวิดท์มีความแคบมาก ๆ นั้นเป็นไปได้ยาก ซึ่งยิ่งโนดเกิดมีการเคลื่อนที่จะทำให้สายอากาศระบุทิศทางที่มีค่าบีมวิดท์แคบ ๆ ยิงบีมไปยังเป้าหมายได้ยากขึ้นด้วย จึงควรมีการกำหนดค่าบีมวิดท์ที่ต่ำที่สุดโดยที่อุปกรณ์สามารถรองรับได้ ซึ่งอาจจะยอมให้เซกเตอร์ที่เกิดจากโนดต้นทางส่งไปยังโนดปลายทางที่มีหลายโนดอยู่ในเซกเตอร์เดียวกันได้ การทำลักษณะนี้อาจทำให้ค่า ESS ตกลงไปแต่ก็สามารถทำให้แบบจำลองมีความใกล้เคียงในทางปฏิบัติมากยิ่งขึ้น

สุดท้ายอาจใช้วิธีการป้องกันการโจมตีประเภทอื่น ๆ มาใช้ร่วมกับการจัดเส้นทางแบบเฟ้นสุ่ม เช่น ในกรณีการดักฟังอาจจะใช้การแบ่งข้อมูลออกเป็นชุด ๆ และส่งกระจายตามทิศทางต่าง ๆ ออกไปทำให้การจัดเส้นทางแบบเฟ้นสุ่มมีประสิทธิภาพมากยิ่งขึ้น เป็นต้น

รายการอ้างอิง

[1] IEEE 802.11 Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 2007.

[2] IEEE 802.16 Working Group on Broadband Wireless Access Standards webpage, [Online].http://www.ieee802.org/16/ [2010, Sep 21]

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

[4] Wishart, R., Portmann, M., and Indulska, J. "Evaluation of Wireless Mesh Network Handoff Approaches for Public Safety and Disaster Recovery Networks," in *Proc. IEEE ATNAC*, Adelaide, SA, (December 2008): 7–10.

[5] Peppas, N., and Turgut, D. "A Hybrid Routing Protocol in Wireless Mesh Networks," in *Proc. IEEE MILCOM*, Orlando, FL, USA, (October 2007): 29–31.

[6] Zhao, Z., and Guan, H. "Max–Min Thoughput Tree Topology Construction in Wireless Mesh Networks," in *Proc. IEEE WCSP*, Nanjing , (November 2009): 13–15.

[7] Ahourai, F., Tabandeh, M., Jahed, M., and Afsari, B. "A Fair Routing Algorithm for Wireless Mesh Networks Based on Game Theory," in *Proc. IEEE ICN*, Gosier, Guadeloupe, (March 2009): 1–6.

[8] Javadi, F., Rubaiyat Kibria, M., and Jamalipour, A. "Bilateral Shapley Value based Cooperative Gateway Selection in Congested Wireless Mesh Networks," in *Proc. IEEE GLOBECOM*, New Orleans, LO, Nov.: 30–Dec.:4, 2008.

[9] Ranjitkar, A. , Lee, S. W., and Ko, Y. B. "Distributed Web–Topology Formation with Directional Antenna in Mesh Environment," in *Proc. IEEE NCM*, Gyeongju, (September 2008): 2–4.

[10] Ramamurthi, V., Reaz, A., Dixit, S., and Mukherjee, B. "Directionality As Need – Achieving Connectivity in Wireless Mesh Networks," in *Proc. IEEE MILCOM*, Beijing , (May 2008): 19–23.

[11] Shila, D. M., and Anjali, T. "Defending Selective Forwarding Attacks in WMNs," in *Proc. IEEE EIT*, Ames, IA, (May 2008): 18–20.

[12] Shila, D. M., and Anjali, T., "A Game Theoretic Approach to Gray Hole Attacks in Wireless Mesh Networks," in *Proc. IEEE MILCOM*, San Diego, CA, (November 2008): 16–19.

[13] Lu, X., Wicker, F., Lio, P., and Towsley, D. "Security Estimation Model with Directional Antennas," in *Proc. IEEE MILCOM*, San Diego, CA, (November 2008): 16–19.

[14] บวรรัตน์ จินดาเลิศอุดมดี, *การใช้ทฤษฎีเกมเพื่อวิเคราะห์การจัดเส้นทางแบบเฟ้นสุ่มในโครงข่ายไร้สายแบบเมชที่มีการรบกวนและดักฟังสัญญาณ.* วิทยานิพนธ์ปริญญา มหาบัณฑิต, สาขา วิชา วิศวกรรม ไฟฟ้า คณะ วิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2552.

[15] Piechowaik, M., and Zwierzykowski, P. "Efficiency Analysis of Multicast Routing Algorithms in Large Networks," in *Proc. IEEE ICNS*, Athens, (January 2008): 22.

[16] Piechowaik, M., and Zwierzykowski, P. "Performance of Fast Multicast Algorithms in Real Networks," in *Proc. IEEE EURCON*, Warsaw, (December 2007): 26.

[17] Naldi, M., *Connectivity of Waxman topology models*, Computer Communications 29, (2005)

[18] Owen, G. *GAME THEORY*, Third edition, Academic, CA Press (1995).

[19] Saha, D., Toy, Bandyopadhyay, S., Ueda, S., and Tanaka, T. "An Adaptive Framework for Multipath Routing via Maximally Zone-disjoint Shortest Paths in Ad hoc Wireless Networks with Directional Antenna," in *Proc. IEEE GLOCOM*, (December 2003): 1–5.

[20] Bohacek, S., Hespansha, J. P., Lee, J., Lim, C., and Obraczka, K., "Game Theoretic Stochastic Routing for Fault Tolerance and Security in Computer Networks," in *Proc. IEEE TPDS*, (September 2007).

[21] Wong, N., Ng, T. S., and Balukrishnan, V. "A Geometrical Approach to Robust Minimum Variance Beamforming," in *Proc. IEEE ICASSP*, (April 2003): 6–10.

[22] วิทวัส ว่องอภิวัฒน์กุล, *การประยุกต์ทฤษฎีเกมแบบไม่ร่วมมือในการประเมินความเชื่อถือได้ของโครงข่ายแบบหลายระดับ.* วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2548.

[23] Melakessou, F., and Engel, T. “Network Traffic Simulator 2.0: Simulating The Internet Traffic,” in *Proc. IEEE OSSC*, Guiyang, (September 2009): 18–20.

[24] Han, Z., Marina, N., Debbah, M., and Hjorungnes, A. “Physical Layer Security Game: How to Date a Girl with Her Boyfriend on the Same Table,” in *Proc. IEEE GAMENETS*, (June 2009): 26.

ประวัติผู้เขียนวิทยานิพนธ์

ภัทร บุญญกาญจน์ เกิดเมื่อวันที่ 21 กันยายน พ.ศ. 2530 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาชั้นมัธยมศึกษาจากโรงเรียนสวนกุหลาบวิทยาลัยในปี พ.ศ. 2548 จากนั้นได้เข้าศึกษาต่อที่คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมไฟฟ้า จุฬาลงกรณ์มหาวิทยาลัย จนสำเร็จหลักสูตรวิศวกรรมศาสตรบัณฑิตในปี พ.ศ. 2551 จากนั้นได้เข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต ณ จุฬาลงกรณ์มหาวิทยาลัย จนสำเร็จการศึกษาในปี พ.ศ. 2553

บทความทางวิชาการจากวิทยานิพนธ์

[1] P. Boonyakarn, P. Komolkiti, and C. Aswakul “Game-Based Analysis of Eavesdropping Defense Strategy in WMN with Directional Antenna," in *Proc. International Joint Conference on Computer Science and Software Engineering, JCSSE*, Nakhon Pathom, Thailand, May. 11–13, 2011.