บทที่ 3

ระเบียบวิธีที่นำเสนอในการจัดเส้นทางแบบเฟ้นสุ่ม ด้วยทฤษฎีเกม

ในบทนี้จะกล่าวถึงระเบียบวิธีที่นำเสนอ โดยในหัวข้อที่ 3.1 กล่าวถึงแบบจำลองของโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทางที่พิจารณาในวิทยานิพนธ์นี้ รวมทั้งอธิบายถึงความแตกต่างระหว่างการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลงในโครงข่ายไร้สายแบบเมชที่มีสายอากาศระบุทิศทาง และยังได้อธิบายถึงความแตกต่างของการโจมตีแบบดักฟังข้อมูลกับการรบกวนสัญญาณในโครงข่ายและหัวข้อที่ 3.2 จะกล่างถึงสัญลักษณ์ต่าง ๆ ที่ถูกนิยามขึ้น

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

3.1 แบบจำลองโครงข่าย

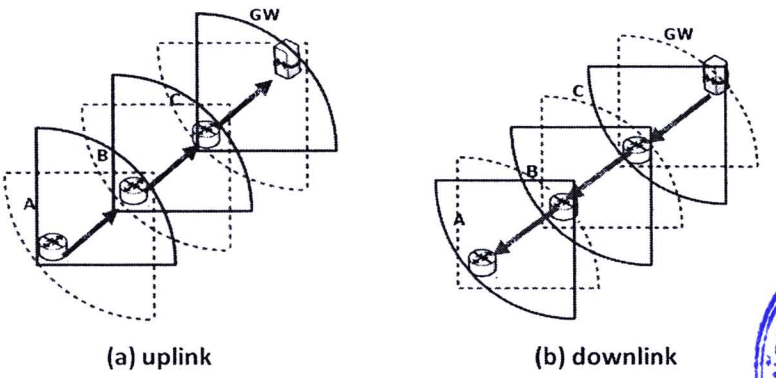
วิทยานิพนธ์นี้กำหนดให้แบบจำลองโครงข่ายไร้สายแบบเมชมีจุดเชื่อมต่อสองชนิดคือเกตเวย์ซึ่งเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตผ่านสายสื่อสารและจุดเชื่อมต่อซึ่งทำหน้าที่รับส่งข้อมูลผ่านตัวกลางไร้สายและส่งข้อมูลกับอินเทอร์เน็ตผ่านเกตเวย์ในลักษณะหลายช่วงเชื่อมต่อ เนื่องจากในวิทยานิพนธ์นี้มองในระดับผู้ให้บริการโครงข่ายอินเทอร์เน็ต 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



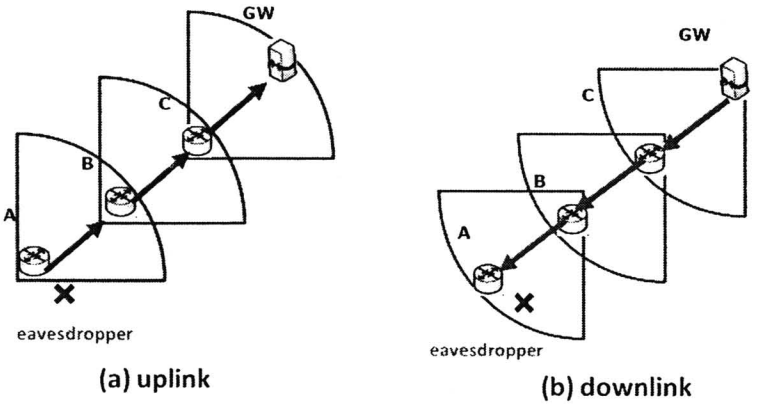
รูปที่ 3.1: ความแตกต่างระหว่างการส่งข้อมูลฝั่งขาขึ้นและฝั่งขาลง

สำนักงานคณะกรรมการวิจัยแห่งชาติ ห้องสมุดงานวิจัย

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

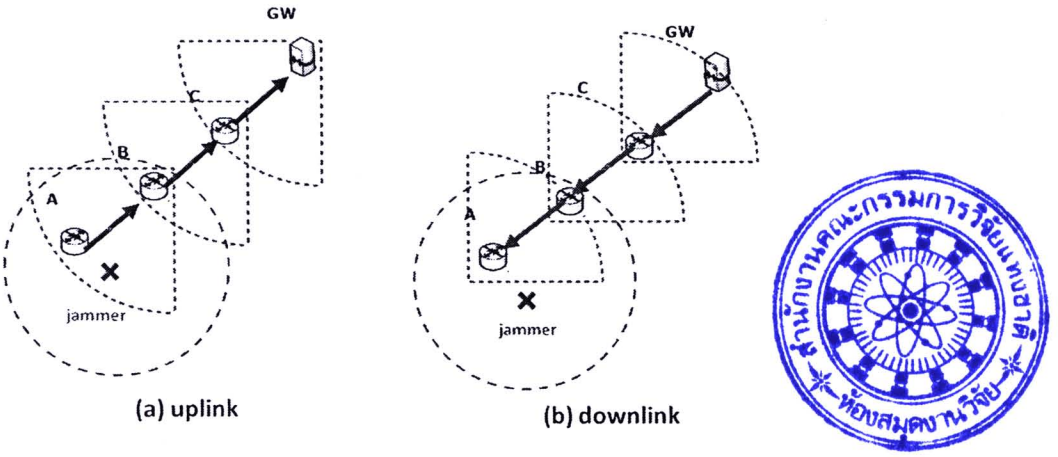
การที่จุดเชื่อมต่อสุดท้ายของเส้นทางในการส่งข้อมูลทั้งฝั่งขาขึ้น คือ เกตเวย์ และฝั่งขาลง คือ จุดเชื่อมต่อที่เป็นเจ้าของข้อมูลของเซสชั่นนั้น ๆ ไม่มีการส่งข้อมูลออกมาผ่านตัวกลางไร้สาย มีผลทำให้การดักฟังของผู้โจมตีต่อการส่งข้อมูลทั้งสองแบบมีลักษณะแตกต่างกัน ดังนั้นโครงข่ายจึงต้องมีการจัดเส้นทางที่แตกต่างกัน 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



สำนักงานคณะกรรมการวิจัยแห่งชาติ ห้องสมุดงานวิจัย

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

สำนักงานคณะกรรมการวิจัยแห่งชาติ
ห้องสมุดงานวิจัย
วันที่ 22 มิ.ย. 2555
เลขทะเบียน 246190
เลขเรียกหนังสือ

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

x_i ตัวแปรช่วย

y_j ตัวแปรช่วย

n แทนรอบของการเล่นเกม

3.3 แบบจำลองเกมของการส่งข้อมูลในโครงข่าย

ในแบบจำลองเกมของการส่งข้อมูลในโครงข่ายนั้น ผู้เล่นสองคน คือ ผู้เล่นฝ่ายป้องกันโครงข่ายและฝ่ายโจมตีโครงข่ายมีลักษณะขัดแย้งกันอย่างชัดเจน จึงสามารถจำลองด้วยเกมที่มีผู้เล่นสองค์นที่มีผลรวมเป็นศูนย์

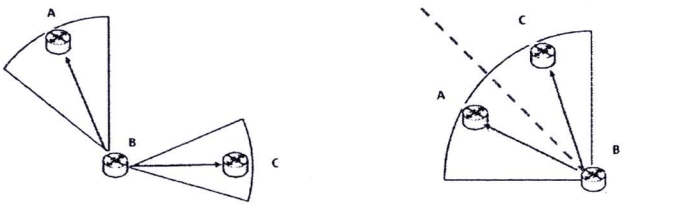
3.3.1 ผู้เล่นฝ่ายป้องกัน (defender)

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 อย่างไรก็ตามผลการทดลองในเบื้องต้นซึ่งได้นำเสนอในวิทยานิพนธ์นี้จะทดสอบโดยการกำหนดค่าบีมวิดท์ให้เท่ากันทุกโนดก่อนทั้งนี้เพื่อความสะดวกในการตรวจสอบความถูกต้องผลการทดลองที่ได้ ส่วนการปรับค่าบีมวิดท์ให้เหมาะสมกับโนดแต่ละโนดดังรูปที่ 3.4(b) นั้นจะทำในลำดับต่อไป นอกจากนี้กำหนดในวิทยานิพนธ์นี้ให้ใช้แบบจำลองสายอากาศเป็นแบบโคน (cone model) [21] นั่นคือไม่คิดผลของบีมย่อยด้านอื่นที่ไม่ได้อยู่ในทิศทางหลักที่รับส่งสัญญาณ



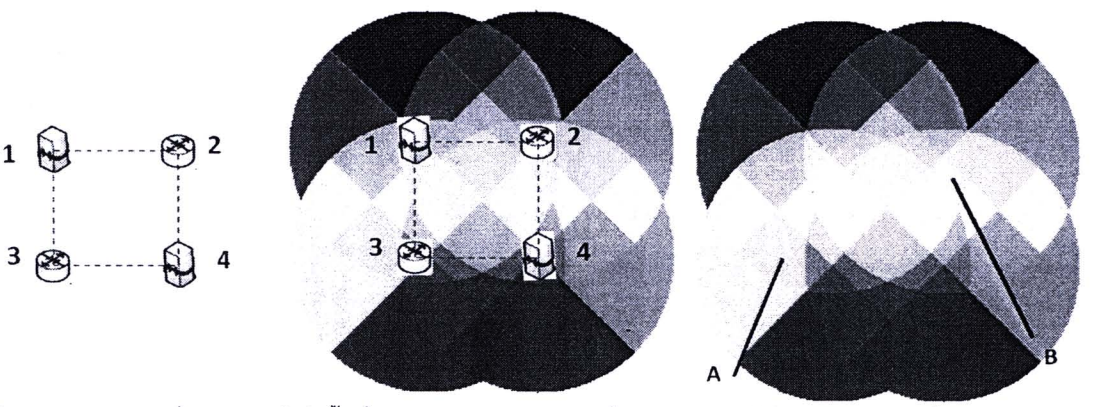
(a) ทิศทางของสายอากาศในการส่ง (b) การปรับค่าบีมวิดท์ที่เหมาะสม

สำนักงานคณะกรรมการวิจัยแห่งชาติ ห้องสมุดงานวิจัย

รูปที่ 3.4: ทิศทางและการปรับค่าบีมวิดท์ที่เหมาะสม

3.3.2 ผู้เล่นฝ่ายโจมตี (attacker)

มีแผนก์การเล่นคือการเลือกตำแหน่งในโครงข่ายเพื่อโจมตีข้อมูลที่รับส่งสัญญาณข้อมูลระหว่างจุดเชื่อมต่อทั้งหมดกับเกตเวย์ให้ได้มากที่สุด โดยจัดกลุ่มตำแหน่งที่เป็นไปได้ทั้งหมดที่ให้ผลการโจมตีออกมาเหมือนกันไว้ในแผนเดียวกันซึ่งสามารถแสดงออกมาในรูปของพื้นที่ที่เกิดจากการตัดกันของขอบเขตของบีมของสายอากาศระบุทิศทางต่าง ๆ ดังแสดงตัวอย่างพื้นที่สีที่แตกต่างกันในรูปที่ 3.3 สำหรับตำแหน่งต่าง ๆ ทุกตำแหน่งในพื้นที่ที่มีสีเหมือนกันจะหมายความว่าหากผู้เล่นฝ่ายโจมตีเลือกแผนการเล่นโดยอยู่ที่ตำแหน่งนั้น ๆ แล้วผลของการโจมตีจะสามารถดักฟังหรือส่งสัญญาณรบกวนได้ชุดของเซสชั่นที่ถูกโจมตีที่เหมือนกัน



(a) ตำแหน่งของจุดเชื่อมต่อ (b) พื้นที่กรอบคลุมการส่งของจุดเชื่อมต่อ (c) แสดงตำแหน่งที่ผู้โจมตีเลือก

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 นั้นมีความซับซ้อนในการหาผลเฉลยเพื่อแก้ปัญหาดังกล่าวในวิทยานิพนธ์นี้จึงได้ใช้หลักการของกลยุทธ์เด่นเพื่อตัดแผนที่ด้อยกว่าของผู้เล่นทั้งสองฝ่ายออกก่อนการหาผลเฉลยด้วย MSA นอกจากนี้สำหรับแผนการเล่นที่มีความเท่าเทียม ซึ่งหมายถึงแผนการเล่นเมื่อวิเคราะห์ด้วยตารางผลได้ผลเสียแล้วแผนการเล่นนั้นทำให้ได้ค่าผลได้ผลเสียเท่ากันทุกกรณี วิทยานิพนธ์นี้จะเลือกแผนที่มีบีมที่ใช้ซ้ำกับแผนการเล่นเหมาะสมที่สุดที่เลือกมาแล้วก่อนหน้ารวมถึงการใช้หลักการกลยุทธ์เด่นและแผนการเล่นที่มีความเท่าเทียมเพื่อเป็นการประหยัดต้นทุนในของระยะเวลาที่ใช้ในการประมวลผลโดยการลดความซับซ้อนในการหาผลเฉลย

หลังจากที่วิเคราะห์ปัญหาและจำลองโครงข่ายไร้สายแบบเมชซึ่งตกอยู่ภายใต้การโจมตีแบบดักฟังข้อมูลและส่งสัญญาณรบกวนแล้ว โนดในโครงข่ายจะใช้การจัดเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดจากกระบวนการหาผลเฉลยโดยกรรมวิธี MSA ที่กล่าวไว้ข้างต้นเพื่อป้องกันการโจมตีทั้งสองแบบ โดยระเบียบวิธีที่นำเสนอการจัดหาเส้นทางแบบเฟ้นสุ่มที่เหมาะสมที่สุดนั้นจะทดสอบและวิเคราะห์เกี่ยวกับระเบียบวิธีอื่น ๆ ในด้านต่าง ๆ ผ่านตัวชี้วัด ESS ในบทต่อไป