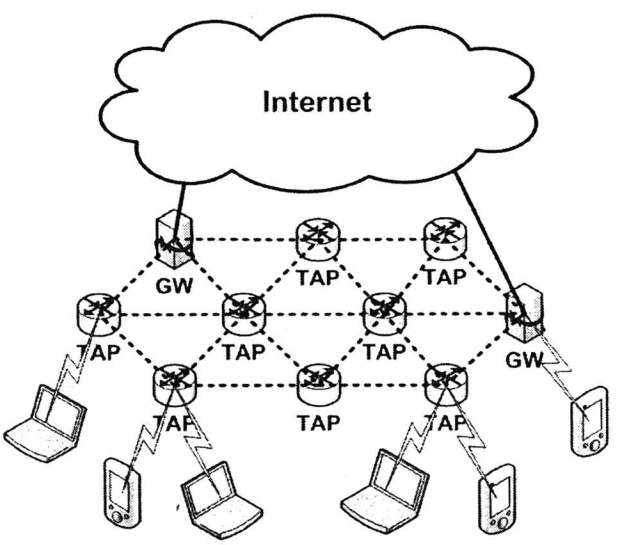
บทที่ 1

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

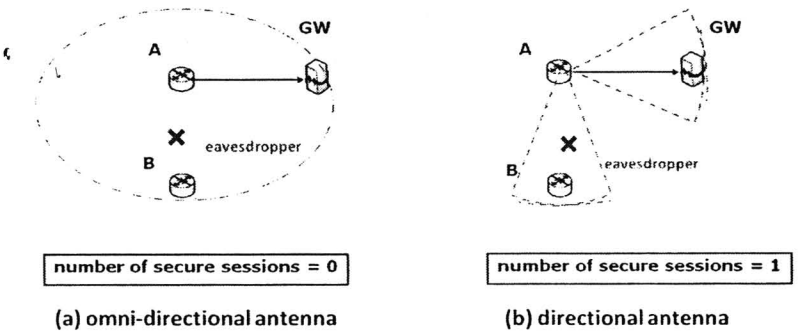
เนื่องจากเป็นการส่งแบบโครงข่ายแอดฮอกทำให้ใช้ตัวกลางไร้สายเป็นตัวส่งข้อมูล จึงติดตั้งง่าย รวดเร็ว รวมทั้งประหยัดต้นทุนเนื่องจากไม่ต้องมีการวางสายและค่าบำรุงซ่อมแซมสาย ยิ่งไปกว่านั้นยังมีความน่าเชื่อถือ (reliability) สูง เนื่องจากรูปแบบของโครงข่าย

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