ใบรับรองวิทยานิพนธ์

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

วิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)

ปริญญา

วิศวกรรมคอมพิวเตอร์ วิศวกรรมคอมพิวเตอร์

สาขา **ภาควิชา**

เรื่อง อัลกอริทึมหลบหลีกการรบกวนในเครือข่ายตัวรับรู้ไร้สายโดยใช้การเปลี่ยนช่องสัญญาณแบบสเปกตรัลมัลติเพล็กซิง

Jamming Avoidance Algorithm in Wireless Sensor Networks Using Channel Surfing from Spectral Multiplexing

นามผู้วิจัย นายประธาน สมบูรณ์

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก .....

(ผู้ช่วยศาสตราจารย์ชัยพร ใจแก้ว, Ph.D.)

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม .....

(อาจารย์ศิวรักษ์ ศิวโมกษธรรม, Ph.D.)

หัวหน้าภาควิชา .....

(ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ, Ph.D.)

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์รับรองแล้ว

.....

(รองศาสตราจารย์กัญจนา ธีระกุล, D.Agr.)

คณบดีบัณฑิตวิทยาลัย

วันที่ ..... **เดือน** ..... **พ.ศ.** .....

วิทยานิพนธ์

เรื่อง

อัลกอริทึมหลบหลีกการรบกวนในเครือข่ายตัวรับรู้ไร้สาย โดยใช้การเปลี่ยนช่องสัญญาณแบบสเปกตรัลมัลติเพล็กซิง

Jamming Avoidance Algorithm in Wireless Sensor Networks Using Channel Surfing from Spectral Multiplexing

โดย

นายประธาน สมบูรณ์

เสนอ

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์
เพื่อความสมบูรณ์แห่งปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์)
พ.ศ. 2555

ประธาน สมบูรณ์ 2555: อัลกอริทึมหลบหลีกการรบกวนในเครือข่ายตัวรับรู้ไร้สายโดยใช้การเปลี่ยนช่องสัญญาณแบบสเปกตรัลมัลติเพล็กซิง ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: ผู้ช่วยศาสตราจารย์ชัยพร ใจแก้ว, Ph.D. 60 หน้า

การสื่อสารของเครือข่ายตัวรับรู้ไร้สายโดยทั่วไปเป็นแบบหลายฮ็อบ หากช่องสัญญาณที่ใช้ในการสื่อสารของโหนดบนเส้นทางถูกรบกวนจะทำให้การส่งข้อมูลจากต้นทางไม่สามารถรับประกันได้ว่าจะไปถึงปลายทางได้ ย่อมส่งผลให้เครือข่ายไม่มีความน่าเชื่อถือในการใช้งาน ดังนั้นงานวิจัยนี้ จึงได้นำเสนอวิธีการหลบหลีกการรบกวน ด้วยการปรับปรุงเทคนิคการเปลี่ยนช่อง สัญญาณแบบสเปกตรัลมัลติเพล็กซิงที่มีอยู่เดิม โดยหากโหนดมีการตรวจพบว่ามีการส่งสัญญาณรบกวนเกิดขึ้นกับช่องสัญญาณที่ใช้งานอยู่ โหนดจะทำการเปลี่ยนช่องสัญญาณไปใช้งานช่อง สัญญาณอื่นที่ไม่ถูกรบกวนในรูปแบบการสุ่มเทียม ซึ่งจะทำให้การสื่อสารกับโหนดรอบข้างสามารถกลับมาใช้งานใหม่ได้อีกครั้ง และเพื่อเป็นการลดจำนวนการเปลี่ยนช่องสัญญาณโดยไม่จำเป็นของโหนดในเครือข่าย การเปลี่ยนช่องสัญญาณจึงเกิดขึ้นเฉพาะกับโหนดที่อยู่ภายใต้พื้นที่การรบกวนและขอบของพื้นที่การรบกวนเท่านั้น ไม่ได้เกิดขึ้นกับโหนดทั้งหมดบนเครือข่าย และเพื่อให้การรับส่งข้อมูลทำได้อย่างมีประสิทธิภาพและได้ประสิทธิผลสูงสุด โหนดที่อยู่บริเวณขอบของพื้นที่การรบกวนจะมีกระบวนการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณให้มีช่วงเวลาที่ตรงกัน ซึ่งจะช่วยให้เครือข่ายสามารถเพิ่มปริมาณข้อมูลที่รับส่งได้ (Packet Delivery Ratio) และช่วยลดปริมาณโอเวอร์เฮดที่เกิดขึ้นให้น้อยที่สุด

จากการทดลองบนอุปกรณ์จริงที่ใช้ตัวรับส่งสัญญาณไร้สายตามมาตรฐาน IEEE 802.15.4 จำนวน 14 ตัว พบว่าขั้นตอนวิธีที่นำเสนอสามารถเพิ่มปริมาณข้อมูลที่รับส่งได้จากวิธีการแบบเดิมโดยเฉลี่ย 12.97% ส่วนปริมาณโอเวอร์เฮดที่เกิดขึ้นบนเครือข่ายต่อปริมาณข้อมูลที่รับได้นั้น ทั้งวิธีการที่นำเสนอและวิธีการแบบเดิมให้ผลที่ไม่แตกต่างกัน

_____ / ___ / ___

ลายมือชื่อนิสิต ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

Prathan Somboon 2012: Jamming Avoidance Algorithm in Wireless Sensor Networks Using Channel Surfing from Spectral Multiplexing. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Assistant Professor Chaiporn Jaikaeo, Ph.D. 60 pages.

Communication within wireless sensor networks is usually multi-hop. If a communication channel of any node on a path from a source to a corresponding sink is intentionally disrupted, e.g., via jamming attack, proper data delivery is no longer guaranteed, resulting in unreliable services. This research proposes a method to avoid jamming attack by improving an existing channel surfing technique based on spectral multiplexing. When a node detects jamming on its current communication channel, it will change the channel to another undisturbed channel on a predetermined pseudorandom sequence in order to reestablish communication with its adjacent nodes. To avoid unnecessary channel switching, only nodes being jammed or located at the edge of disturbed regions, called boundary nodes, not all nodes in the entire network, will undergo channel surfing. To achieve the highest performance in communication, these boundary nodes will synchronously switch to different communication channels. Compared to an existing method, the proposed method can increase the amount of information transferred and greatly reduce the amount of overhead.

Experiments with 14 sensor nodes equipped with IEEE 802.15.4 transceivers showed that the proposed method, on average, can increase the packet delivery ratio over the existing method by 12.97 percents. The message overhead per data packet received generated by both methods, are not significantly different.

_____ _____ ___ / ___ / ___

Student's signature Thesis Advisor's signature

กิตติกรรมประกาศ

ผู้วิจัยขอกราบขอบพระคุณ ผศ. ดร. ชัยพร ใจแก้ว อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก และ ดร. ศิวรักษ์ ศิวโมกษธรรม อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ที่คอยให้คำแนะนำปรึกษา ทั้งในการเรียน การค้นคว้าวิจัย ตลอดจนการตรวจแก้ไขวิทยานิพนธ์จนกระทั่งเสร็จสมบูรณ์ และขอกราบขอบพระคุณผู้แทนบัณฑิตวิทยาลัยที่ได้ให้ความกรุณาตรวจแก้ไขวิทยานิพนธ์ให้สมบูรณ์ยิ่งขึ้น

ขอกราบขอบพระคุณอาจารย์ภาควิศวกรรมคอมพิวเตอร์ทุกท่าน ที่ได้อบรมสั่งสอนและมอบความรู้อันเป็นประโยชน์อย่างยิ่งในการนำไปใช้ประโยชน์ต่อไป และขอขอบพระคุณเจ้าหน้าที่ภาควิชาวิศวกรรมคอมพิวเตอร์ทุกท่าน ที่ให้ความช่วยเหลือและคำแนะนำ

ขอกราบขอบพระคุณสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ที่สนับสนุนเงินทุนในการศึกษา และเงินทุนวิจัย ในโครงการทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST)

ด้วยความดีหรือประโยชน์อันใดเนื่องจากวิทยานิพนธ์นี้ ขอมอบแด่คุณพ่อ คุณแม่ ผู้อบรมและให้กำลังใจผู้วิจัยมาตลอดในทุกเรื่อง

ประธาน สมบูรณ์

มีนาคม 2555

สารบัญ

หน้า

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

ภาพผนวกที่

คำอธิบายสัญลักษณ์และคำย่อ

JAWSN	=	Jamming Avoidance Algorithm in Wireless Sensor Network
DSSS	=	Direct Sequence Spread Spectrum
FHSS	=	Frequency Hopping Spread Spectrum
PDR	=	Packet Delivery Ratio
PN	=	Pseudo Noise
UWB	=	Ultra Wide Band
SNR	=	Signal to Noise Ratio
PRG	=	Pseudo-random Generator
RSSI	=	Received Signal Strength Indication

อัลกอริทึมหลบหลีกการรบกวนในเครือข่ายตัวรับรู้ไร้สาย โดยใช้การเปลี่ยนช่องสัญญาณแบบสเปกตรัลมัลติเพล็กซิง

Jamming Avoidance Algorithm in Wireless Sensor Networks Using Channel Surfing from Spectral Multiplexing

คำนำ

ในปัจจุบันเครือข่ายตัวรับรู้ไร้สาย (Wireless sensor network) ถูกนำมาประยุกต์ใช้มากขึ้น เนื่องจากความสะดวกในการใช้งานและการติดตั้งเครือข่าย เพื่อการตรวจวัดคุณสมบัติต่างๆ ของสิ่งแวดล้อมที่สนใจ เพื่อสร้างองค์ความรู้ใหม่ หรือตอบสนองต่อการเปลี่ยนแปลงที่เกิดขึ้นของสภาพแวดล้อมได้โดยอัตโนมัติ ทำให้นักวิทยาศาสตร์และวิศวกรสามารถใช้ประโยชน์จากเครือข่ายตัวรับรู้ไร้สายได้หลายรูปแบบ เช่น ติดตามการเคลื่อนไหวของวัตถุ ตรวจสอบความปลอดภัยโครงสร้าง ประเมินความปลอดภัยในพื้นที่เสี่ยงภัย เพิ่มผลผลิตทางการเกษตร เป็นต้น

อุปกรณ์พื้นฐานของเครือข่ายตัวรับรู้ไร้สายประกอบด้วยสองส่วนหลักๆ ได้แก่ โหนดตัวรับรู้ (Sensor node) และสถานีฐาน (Base station) โดยโหนดตัวรับรู้จะประกอบด้วยหน่วยประมวลผล (Processor) ตัวรับรู้ (Sensor) และโมดูลสื่อสารไร้สาย (Wireless communication module) ทำงานโดยใช้พลังงานจากแบตเตอรี่ธรรมดา และสื่อสารกับโหนดอื่นๆ บริเวณใกล้เคียงในรูปแบบเครือข่ายแอดฮ็อกแบบหลายฮ็อบ (Multi-hop ad hoc network) โดยข้อมูลที่ตรวจวัดได้จะถูกส่งผ่านเป็นทอดๆ ระหว่างโหนดด้วยกันจนกระทั่งถึงสถานีฐาน เพื่อรวบรวมข้อมูลเหล่านั้นและนำไปประมวลผลต่อไป แต่ด้วยการส่งข้อมูลเป็นทอดๆ ผ่านโหนดตัวรับรู้ตัวอื่นไปยังสถานีฐานนั้น หากช่องสัญญาณที่ใช้ในการสื่อสารของโหนดตัวรับรู้ตัวใดตัวหนึ่งหรือหลายตัวระหว่างเส้นทางไปยังสถานีฐานถูกรบกวน จนทำให้การส่งข้อมูลจากต้นทางไม่สามารถรับประกันได้ว่าจะไปถึงปลายทางได้ ย่อมส่งผลให้เครือข่ายไม่มีความน่าเชื่อถือในการใช้งาน

การส่งสัญญาณรบกวน (Jamming) บนช่องสัญญาณการสื่อสารของเครือข่ายตัวรับรู้ไร้สายนั้น หากเกิดขึ้นตามธรรมชาติโดยไม่ได้ตั้งใจ เช่น การมีอุปกรณ์อื่นที่มีการใช้ความถี่เดียวกันหรือใกล้เคียงกันทำงานอยู่ในพื้นที่เดียวกันกับโหนดตัวรับรู้ การวางโหนดตัวรับรู้คนละเครือข่ายที่มีการ

ใช้งานช่องสัญญาณที่อยู่ติดกันหรือช่องสัญญาณเดียวกันในพื้นที่เดียวกัน เป็นต้น การหลบหลีกการรบกวนจากสถานการณ์ดังกล่าวอาจสามารถทำได้จากกระบวนการกล้ำสัญญาณ (Modulation) ด้วยการใช้กระบวนการกระจายสเปกตรัมแบบลำดับตรง (Direct sequence spread spectrum) ที่มีใช้อยู่บนโหนดตัวรับรู้ไร้สายในปัจจุบัน ซึ่งการกระจายสเปกตรัมแบบลำดับตรงตามมาตรฐาน IEEE 802.15.4 ในย่าน 2.4 GHz จะมีทั้งหมด 16 ช่องสัญญาณ โดยมีแถบกัน (Guard band) 5 MHz และแต่ละช่องสัญญาณไม่มีการเหลื่อมกัน ดังนั้นจึงสามารถเลือกใช้ช่องสัญญาณได้โดยไม่มีการซ้อนทับกัน ซึ่งในงานวิจัยนี้ก็ได้ยึดตามมาตรฐานดังกล่าว แต่หากการส่งสัญญาณรบกวนนั้นเกิดจากความตั้งใจ จากบุคคลที่ต้องการทำลายการสื่อสาร เช่น การนำอุปกรณ์รบกวนสัญญาณที่ทำขึ้นมาเฉพาะกิจมาวางไว้ในเครือข่าย เป็นต้น การหลบหลีกการรบกวนด้วยกระบวนการกล้ำสัญญาณที่มีอยู่อาจทำได้ยาก เนื่องจากการรบกวนที่เกิดขึ้นจากอุปกรณ์รบกวนสัญญาณนั้นนอกจากจะมีการส่งสัญญาณรบกวนออกมาแล้ว อาจมีการใช้กระบวนการในการกล้ำสัญญาณแบบเดียวกันกับโหนดตัวรับรู้ และสามารถเปลี่ยนช่องสัญญาณในการโจมตีได้อีกด้วย ทำให้กระบวนการกล้ำสัญญาณที่มีอยู่เพียงอย่างเดียวไม่เพียงพอที่จะสามารถหลบหลีกการรบกวนที่เกิดขึ้นได้

เพื่อหลีกเลี่ยงปัญหาการรบกวนที่เกิดขึ้นดังกล่าว จึงได้มีการนำกระบวนการกระจายสเปกตรัมแบบกระโดดความถี่ (Frequency hopping spread spectrum) มาใช้ในการหลบหลีกการรบกวนร่วมกับกระบวนการกล้ำสัญญาณที่มีอยู่ ซึ่งกระบวนการกระจายสเปกตรัมแบบกระโดดความถี่นี้ถูกนำไปพัฒนาเป็นเทคนิคในการควบคุมช่องสัญญาณที่เรียกว่า กระบวนการเปลี่ยนช่องสัญญาณ (Channel surfing algorithm) โดยหากมีการตรวจพบว่าเกิดการรบกวนขึ้นที่ช่องสัญญาณที่กำลังใช้งานอยู่ โหนดจะทำการเปลี่ยนไปใช้งานช่องสัญญาณอื่นที่ไม่ถูกรบกวน ซึ่งจะทำให้การสื่อสารบนเครือข่ายสามารถกลับมาใช้งานได้อีกครั้ง

การควบคุมช่องสัญญาณด้วยกระบวนการเปลี่ยนช่องสัญญาณนั้น โดยปกติแล้วจะทำให้เกิดการสูญเสียข้อมูลขึ้นบนเครือข่าย เนื่องจากเมื่อมีการรบกวนเกิดขึ้นจะต้องมีกระบวนการทำงานเพื่อตรวจสอบการรบกวนและการเปลี่ยนไปใช้งานช่องสัญญาณใหม่ ดังนั้นโหนดทุกตัวจึงต้องรอเวลาเพื่อที่จะสร้างการสื่อสารบนช่องสัญญาณใหม่ ซึ่งหากเครือข่ายยิ่งมีขนาดใหญ่ระยะเวลาในการรอจะยิ่งนาน และหากการรบกวนไม่ได้เกิดขึ้นแบบถาวร แต่เกิดขึ้นแบบชั่วคราวบนแต่ละช่องสัญญาณ จะทำให้การเปลี่ยนช่องสัญญาณเกิดขึ้นบ่อยครั้ง ซึ่งส่งผลให้การสูญเสียข้อมูลยิ่งจะมีมากขึ้นและปริมาณข้อมูลที่รับส่งได้ก็จะลดลงตามไปด้วย

ดังนั้นงานวิจัยนี้ จึงสนใจปัญหาการหลบหลีกการรบกวนที่เกิดขึ้นแบบชั่วคราวนี้ ด้วยการใช้เทคนิคการเปลี่ยนช่องสัญญาณแบบสเปกตรัลมัลติเพล็กซิง โดยหากโหนดมีการตรวจพบว่ามีการรบกวนเกิดขึ้นกับช่องสัญญาณที่ใช้งานอยู่ โหนดก็จะทำการเปลี่ยนช่องสัญญาณไปใช้งานช่องสัญญาณอื่นที่ไม่ถูกรบกวน ซึ่งจะทำให้การสื่อสารบนเครือข่ายสามารถกลับมาใช้งานใหม่ได้อีกครั้ง และเพื่อเป็นการลดจำนวนการเปลี่ยนช่องสัญญาณโดยไม่จำเป็นของโหนดในเครือข่าย การเปลี่ยนช่องสัญญาณนั้นจะเกิดขึ้นเฉพาะกับโหนดที่อยู่ภายใต้พื้นที่การรบกวนและขอบของพื้นที่การรบกวนเท่านั้น ไม่ได้เกิดขึ้นกับโหนดทั้งหมดบนเครือข่าย ซึ่งในงานวิจัยจะมุ่งเน้นเพื่อทำให้เครือข่ายสามารถเพิ่มปริมาณข้อมูลที่รับส่งได้และช่วยลดปริมาณโอเวอร์เฮดที่เกิดขึ้นให้น้อยที่สุด

วัตถุประสงค์

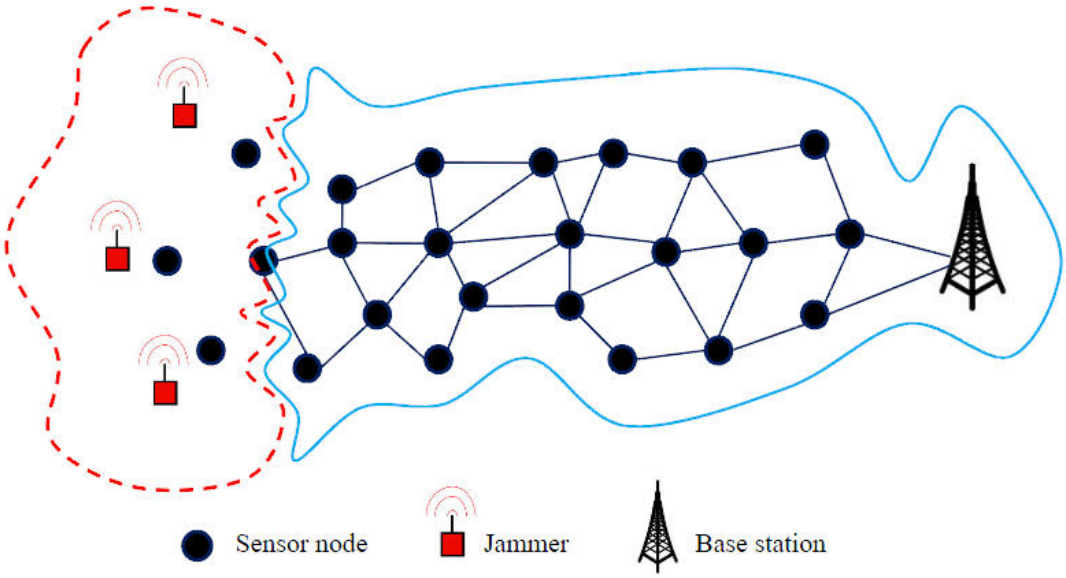
พัฒนากระบวนการให้โหนดตัวรับรู้ไร้สายทำงานได้ในสภาวะที่มีการส่งคลื่นรบกวนเพื่อลดปริมาณโอเวอร์เฮดที่เกิดขึ้น และเพิ่มค่า Packet Delivery Ratio (PDR) ในการรับส่งข้อมูล

การตรวจเอกสาร

ในส่วนนี้จะเป็นการอธิบายถึงความรู้พื้นฐานและงานวิจัยที่ผ่านมาที่เกี่ยวข้องกับงานวิจัยนี้ ซึ่งได้แก่ การโจมตีจากอุปกรณ์รบกวนสัญญาณ อุปกรณ์รบกวนสัญญาณ การป้องกันการโจมตีและกระบวนการเปลี่ยนช่องสัญญาณ

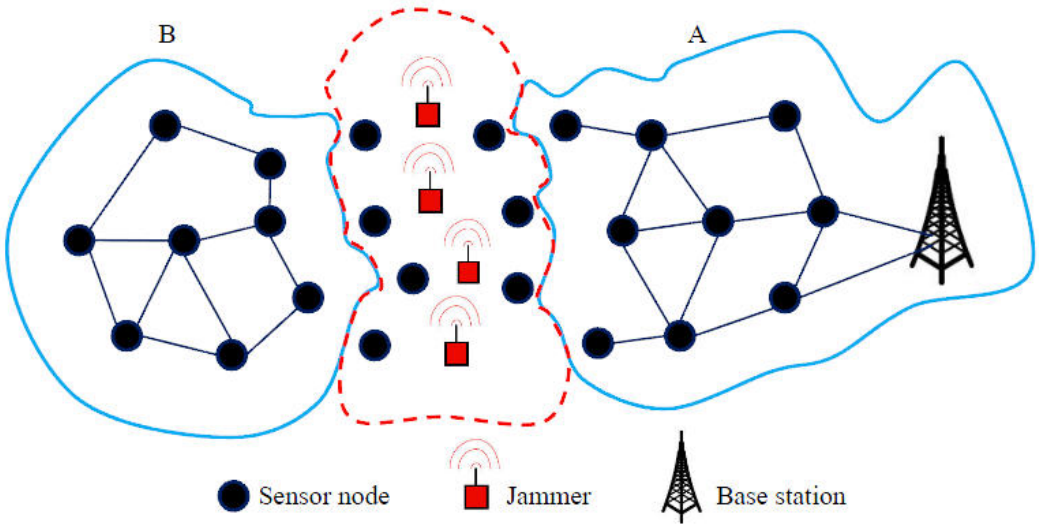
1. การโจมตีจากอุปกรณ์รบกวนสัญญาณ

การโจมตีจากอุปกรณ์รบกวนสัญญาณตามงานวิจัยของ Aritides *et al*. (2009) ผลกระทบส่วนใหญ่จะเกิดขึ้นที่ระดับชั้นล่างๆ โดยเฉพาะชั้นกายภาพ (Physical layer) เนื่องจากการโจมตีส่วนใหญ่จะเป็นการโจมตีมายังช่องสัญญาณที่ใช้ในการสื่อสาร ซึ่งมีผลกระทบกับสัญญาณวิทยุโดยตรง และเนื่องจากโพรโทคอลบนมาตรฐาน IEEE 802.15.4 ที่นิยมใช้ในปัจจุบันมีการทำงานส่วนใหญ่อยู่ในระดับชั้นล่างๆ คือ ชั้นกายภาพ และชั้น MAC ซึ่งได้กำหนดขนาดกำลังส่งของโหนดที่ต่ำประมาณ 0 dBm อีกทั้งมีการแบ่งช่องสัญญาณที่ใช้กับบางช่วงความถี่ที่น้อยเกินไป จึงทำให้ง่ายต่อการถูกโจมตี

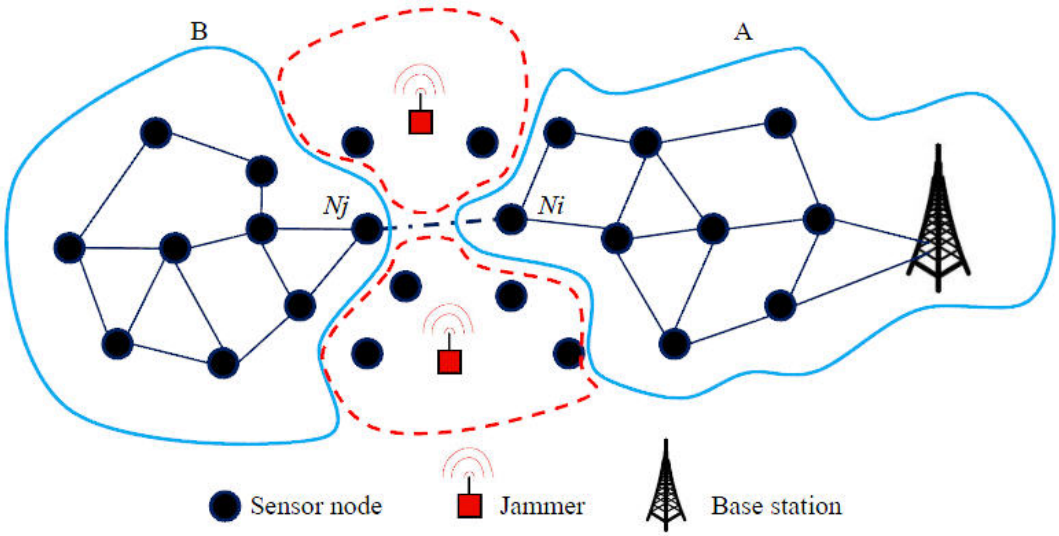


(ก) การโจมตีบริเวณขอบของเครือข่าย

ภาพที่ 1 การโจมตีจากอุปกรณ์รบกวนสัญญาณ



(ข) การโจมตีบริเวณใจกลางของเครือข่ายแบบที่ 1



(ค) การโจมตีบริเวณใจกลางของเครือข่ายแบบที่ 2

ภาพที่ 1 (ต่อ)

เหตุการณ์การโจมตีที่เกิดจากอุปกรณ์รบกวนสัญญาณบนเครือข่ายตัวรับรู้ไร้สายนั้นมีหลายลักษณะตามงานวิจัยของ Loukas *et al*. (2009) ดังแสดงตามภาพที่ 1 โดยภาพที่ 1 (ก) เป็นการโจมตีโหนดตัวรับรู้ที่บริเวณขอบของเครือข่ายทำให้โหนดภายใต้พื้นที่การรบกวนไม่สามารถที่จะส่งข้อมูลมายังโหนดอื่นใกล้เคียงที่อยู่นอกพื้นที่การรบกวนได้ ภาพที่ 1 (ข) เป็นการโจมตีบริเวณใจ

กลางของเครือข่าย ทำให้เครือข่ายถูกแบ่งออกเป็น 2 โซน คือ โซน A และโซน B ซึ่งโหนดตัวรับรู้ทั้งสองโซนไม่สามารถสื่อสารข้อมูลถึงกันได้ เนื่องจากมีพื้นที่การรบกวนปิดกั้นเส้นทางในการสื่อสารทั้งหมดไว้ และภาพที่ 1 (ค) เป็นการโจมตีบริเวณใจกลางเครือข่ายเช่นเดียวกัน แต่เนื่องจากพื้นที่การรบกวนไม่ได้ปิดกั้นเส้นทางการสื่อสารไว้ทั้งหมด จึงทำให้โหนด Ni ที่โซน A สามารถสื่อสารข้อมูลกับโหนด Nj ที่โซน B ได้ แต่อย่างไรก็ตามการสื่อสารข้อมูลนั้นก็ยังคงทำได้ไม่สมบูรณ์ เพราะเส้นทางการสื่อสารยังอยู่ใกล้กับพื้นที่การรบกวนมาก ทำให้ยังคงได้รับผลกระทบจากการโจมตีนั้นอยู่

ในงานวิจัยของ Aritides *et al*. (2009) การรบกวนที่เกิดจากอุปกรณ์รบกวนสัญญาณนั้นมีความแตกต่างจากการรบกวนที่เกิดจากการแทรกสอด (Interference) เนื่องจากการรบกวนที่เกิดจากการแทรกสอดนั้นเกิดจากการมีอุปกรณ์ที่ใช้ความถี่เดียวกันหรือใกล้เคียงกันแล้วอยู่ในพื้นที่เดียวกันและไม่ได้ตั้งใจที่จะทำลายการสื่อสาร แต่การรบกวนที่เกิดจากอุปกรณ์รบกวนสัญญาณนั้นเกิดจากความตั้งใจในการสร้างอุปกรณ์ขึ้นมาโดยเฉพาะกิจ ซึ่งมีเป้าหมายเพื่อทำลายการสื่อสารบนเครือข่ายโดยจะทำการส่งสัญญาณรบกวนด้วยกำลังส่งที่สูงมายังช่องสัญญาณโดยตรง ทำให้ค่า Signal to Noise Ratio (SNR) มีค่าลดต่ำลงมาก จนส่งผลให้โหนดตัวรับรู้ไร้สายภายใต้พื้นที่การรบกวนไม่สามารถที่จะสื่อสารข้อมูลกันได้บนช่องสัญญาณดังกล่าว

2. อุปกรณ์รบกวนสัญญาณ

อุปกรณ์รบกวนสัญญาณเป็นอุปกรณ์ที่สร้างขึ้นมาเฉพาะกิจ เพื่อจุดประสงค์ในการโจมตีอุปกรณ์ไร้สายต่างๆ ที่มีการใช้งานบนคลื่นความถี่วิทยุเดียวกัน ทำให้อุปกรณ์ไร้สายไม่สามารถสื่อสารข้อมูลกันได้ภายใต้พื้นที่การรบกวนที่เกิดจากการโจมตี โดยอุปกรณ์รบกวนสัญญาณที่ใช้ในการโจมตีเครือข่ายตัวรับรู้ไร้สายตามงานวิจัย Wenyuan *et al*. (2005) มีอยู่ด้วยกัน 4 ประเภท ได้แก่

2.1 Constant jammer

อุปกรณ์รบกวนสัญญาณประเภทนี้จะทำงานด้วยการส่งบิตข้อมูลแบบสุ่มไปยังช่องสัญญาณอย่างต่อเนื่อง ส่งผลต่อกระบวนการในการตรวจสอบช่องสัญญาณ ทำให้การสื่อสารของโหนดบนช่องสัญญาณเสียระบบ ข้อมูลที่รับได้เกิดการปลอมปนของบิตข้อมูล

2.2 Deceptive jammer

เป็นอุปกรณ์รบกวนสัญญาณที่ใช้วิธีการส่งแพ็กเกตข้อมูลที่ปลอมขึ้นมาไปยังช่องสัญญาณอย่างต่อเนื่อง ทำให้ปริมาณการรับส่งข้อมูลที่มีอยู่อย่างจำกัดนั้นเต็ม ส่งผลให้การรับส่งแพ็กเกตข้อมูลจริงบนช่องสัญญาณดังกล่าวไม่สามารถทำได้

2.3 Random jammer

เป็นอุปกรณ์รบกวนสัญญาณที่ใช้วิธีการส่งบิตข้อมูลแบบสุ่มไปยังช่องสัญญาณ แต่การโจมตีจะใช้การสุ่มช่วงเวลาในการโจมตี โดยจะมีทั้งช่วงเวลาที่หลับและช่วงเวลาที่ตื่นเพื่อทำการโจมตี ซึ่งการทำงานทั้ง 2 อย่างนี้จะสลับกันตามช่วงเวลาที่กำหนด ทำให้อุปกรณ์รบกวนสัญญาณประเภทนี้ประหยัดพลังงานและสามารถทำงานอยู่ได้เป็นระยะเวลานาน

2.4 Reactive jammer

อุปกรณ์รบกวนสัญญาณประเภทนี้จะใช้การคอยฟังว่ากำลังมีการใช้งานช่องสัญญาณที่เป็นเป้าหมายหรือไม่ หากมีการใช้งานช่องสัญญาณดังกล่าวก็จะทำการโจมตีด้วยการส่งบิตข้อมูลแบบสุ่มหรือแพ็กเกตข้อมูลที่ปลอมขึ้นมาออกไปยังช่องสัญญาณ เป็นผลทำให้เกิดการปลอมปนของสัญญาณข้อมูล แต่หากไม่ตรวจพบว่ามีการใช้งานช่องสัญญาณก็จะเปลี่ยนไปตรวจสอบเพื่อโจมตีช่องสัญญาณถัดไป ซึ่งอุปกรณ์รบกวนสัญญาณประเภทนี้เป็นประเภทที่เราสนใจจะศึกษาในงานวิจัย เนื่องจากสามารถตรวจสอบการใช้งานช่องสัญญาณและเปลี่ยนช่องสัญญาณในการโจมตีได้ ทำให้สามารถโจมตีได้หลายช่องสัญญาณ ซึ่งยากต่อการป้องกันการโจมตีที่เกิดขึ้น อีกทั้งการโจมตียังเกิดขึ้นเฉพาะช่องสัญญาณที่มีการใช้งานเท่านั้น ทำให้อุปกรณ์รบกวนสัญญาณประเภทนี้มีประสิทธิภาพที่สูง เพราะประหยัดพลังงานและสามารถโจมตีได้ตรงตามเป้าหมาย

3. การป้องกันการโจมตี

การป้องกันการโจมตีจากอุปกรณ์รบกวนสัญญาณ มีวิธีการต่างๆ ที่นิยมนำมาใช้ในการป้องกันการโจมตี ซึ่งตามงานวิจัยของ Aritides *et al*. (2009) มีอยู่ด้วยกัน 7 วิธี ได้แก่

3.1 ลดขนาดกำลังส่ง

การลดขนาดของกำลังส่งให้ต่ำลง (Regulated Transmitted Power) เป็นการป้องกันการถูกตรวจจับได้ เนื่องจากโดยปกติก่อนการโจมตีจะต้องมีการตรวจหาตำแหน่งที่ตั้งของเป้าหมายก่อนถึงจะทำการโจมตีได้ ดังนั้นหากลดขนาดกำลังส่งของโหนดลง จะทำให้ยากต่อการตรวจพบ ซึ่งจะช่วยป้องกันการโจมตีที่จะเกิดขึ้นได้ ซึ่งในปัจจุบันยังมีการใช้วิธีการนี้อยู่ เช่น ใน SunSPOT node ของบริษัท Sun Microsystems ที่มีความสามารถในการตรวจสอบกำลังส่งและปรับกำลังส่งของโหนดให้มีความเหมาะสมได้ แต่อย่างไรก็ตามการปรับขนาดกำลังส่งของโหนดก็ย่อมส่งผลต่อระยะการสื่อสารข้อมูลที่ต้องเปลี่ยนแปลงไป

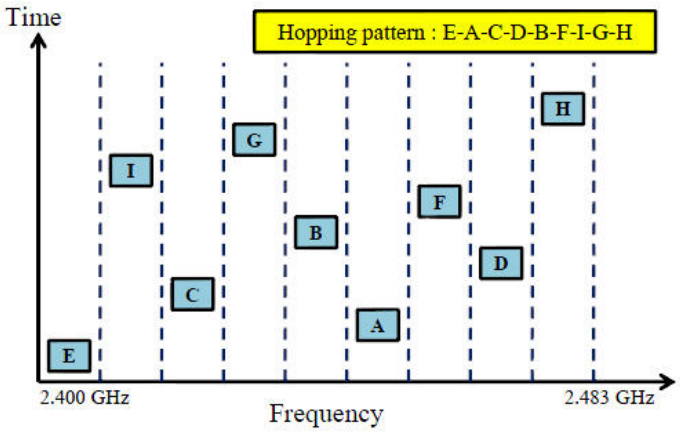
3.2 เสาอากาศแบบโพลาไรเซชัน

เสาอากาศแบบโพลาไรเซชัน (Antenna polarization) เป็นวิธีการที่ใช้โครงสร้างของเสาอากาศมาช่วยในการป้องกันการโจมตี โดยการออกแบบให้เสาอากาศสามารถที่จะระบุทิศทางในการส่งสัญญาณรบกวนออกมาได้ เมื่อสามารถที่จะรู้ทิศทางในการโจมตีก็จะช่วยให้สามารถหลบหลีกการโจมตีจากทิศทางดังกล่าวได้ แต่ปัญหาของวิธีการนี้อยู่ที่การวิเคราะห์หรือแยกแยะองค์ประกอบของสัญญาณเพื่อให้รู้ทิศทางนั้น ยังต้องใช้เครื่องมือที่มีความสามารถสูง และราคาค่อนข้างแพงจึงไม่เหมาะที่จะนำมาใช้กับเครือข่ายตัวรับรู้ไร้สายที่ต้องการต้นทุนต่ำ

3.3 การส่งแบบกำหนดทิศทาง

โหนดตัวรับรู้ไร้สายที่ใช้อยู่ในปัจจุบันส่วนใหญ่มักจะใช้เสาอากาศแบบรอบทิศทาง (Omni-directional antenna) ซึ่งจะรับและส่งข้อมูลออกไปทุกทิศทาง จึงทำให้ง่ายต่อการถูกรบกวน ดังนั้นหากมีการใช้เสาอากาศแบบทิศทาง (Directional antenna) ที่สามารถกำหนดทิศทางในการส่ง (Directional transmission) ข้อมูลไปยังโหนดเป้าหมายที่ต้องการเพียงทิศทางเดียว ก็จะช่วยลดการรบกวนที่เกิดขึ้นได้ แต่ปัญหาหลักของการใช้เสาอากาศแบบทิศทางนั้น คือ การจะเลือกเส้นทางในการส่งข้อมูลไปยังเป้าหมายหลายๆ เส้นทางไม่สามารถทำได้ เพราะทิศทางในการส่งนั้นได้ถูกกำหนดไว้แล้วด้วยเสาอากาศ ดังนั้นทำให้เสาอากาศแบบทิศทางไม่เป็นที่นิยมในการนำมาใช้กับเครือข่ายตัวรับรู้ไร้สายที่ต้องการเส้นทางไปยังเป้าหมายหลายๆ เส้นทาง

3.4 การกระจายสเปกตรัมแบบกระโดดความถี่



ภาพที่ 2 การกระจายสเปกตรัมแบบกระโดดความถี่

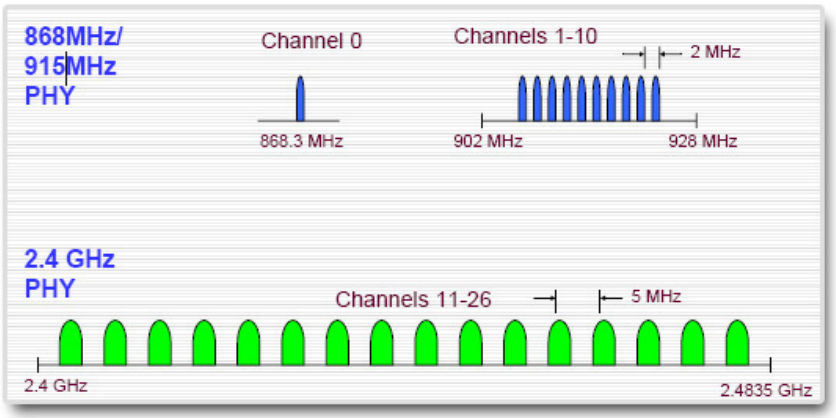
การกระจายสเปกตรัมแบบกระโดดความถี่ (FHSS: Frequency Hopping Spread Spectrum) เป็นวิธีที่ใช้การเปลี่ยนความถี่จากค่าหนึ่งไปเป็นอีกค่าหนึ่งตลอดเวลา โดยการเปลี่ยนความถี่นี้เป็นการกระโดดตามฟังก์ชั่นของเวลา เมื่อเวลาเปลี่ยนไป ความถี่ที่ใช้ก็จะเปลี่ยนไปด้วย โดยในการทำงานจะต้องมีการกำหนดความถี่ต่างๆ ที่จะใช้งานและลำดับการใช้งานความถี่ให้ชัดเจน โดยผู้ส่งจะทำการส่งตามลำดับ ส่วนผู้รับก็ต้องมีความสามารถในการเปลี่ยนความถี่ตามที่ผู้ส่งทำการส่งจึงจะสามารถรับข้อมูลที่ส่งมาได้ครบถ้วน ซึ่ง FHSS มีข้อดีหลายอย่างในการใช้งานกับเครือข่ายตัวรับรู้ไร้สาย ได้แก่

- ขัดขวางผู้ที่ไม่มีสิทธิ์เข้าร่วมเครือข่าย
- สามารถลดผลกระทบจากการรบกวนของโหนดตัวรับรู้ไร้สายให้น้อยลง
- ป้องกันการดักฟังข้อมูลจากผู้ไม่หวังดี
- ช่วยลดขนาดความกว้างของช่วงความถี่ที่ใช้ในการส่งข้อมูล
- สามารถใช้เครือข่ายตัวรับรู้ไร้สายหลายเครือข่ายในพื้นที่เดียวกันได้ โดยไม่ทำให้เกิดปัญหาการรบกวนกัน

ในภาพที่ 2 แกนนอนเป็นค่าความถี่ที่ใช้งาน โดยจากภาพเป็นย่านความถี่ช่วง 2.400–2.483 GHz ส่วนแกนตั้งเป็นค่าของเวลาที่เปลี่ยนไปแต่ละช่วง ซึ่งจากภาพเป็นการส่งที่มีลำดับการใช้ความถี่ (Hopping pattern) เป็น E-A-C-D-B-F-I-G-H โดยการส่งจะเริ่มจาก E และไปสิ้นสุดที่ H

อย่างไรก็ตามการกระจายสเปกตรัมแบบกระโดดความถี่ก็ยังมีข้อด้อยในเรื่องของความต้องการปริมาณการรับส่งข้อมูล (Bandwidth) เนื่องจากการส่งข้อมูลแต่ละครั้งมีข้อจำกัดในเรื่องของระยะเวลา โดยที่ความถี่หนึ่งๆจะใช้ในการรับส่งข้อมูลแค่ชั่วระยะเวลาสั้นๆ ทำให้ต้องใช้ปริมาณการรับส่งข้อมูลทั้งหมดบนความถี่ดังกล่าวในการส่งข้อมูลแค่อย่างเดียว

3.5 การกระจายสเปกตรัมแบบลำดับตรง



ภาพที่ 3 การกระจายสเปกตรัมแบบลำดับตรง

ที่มา: http://zigbee-interference.blogspot.com (2553)

การกระจายสเปกตรัมแบบลำดับตรง (DSSS: Direct Sequence Spread Spectrum) เป็นการใช้เทคนิคการรวมสัญญาณข้อมูลที่ต้องการส่งเข้ากับสัญญาณข้อมูลอีกชุดหนึ่ง เรียกว่า Pseudo Noise (PN) โดย PN นี้ได้มาจาก Pseudo-random sequence ของ 0 และ 1 ด้วยค่า Chip rate ที่สูงมาก ซึ่งแต่ละบิตข้อมูลจะถูกขยายสัญญาณเป็นหลายบิตแล้วนำไปผสมกับ PN ที่ได้ ส่งผลให้ปริมาณการรับส่งข้อมูลที่ใช้มีขนาดที่สูงขึ้นมาก แต่ PN ที่นำมารวมนี้สามารถที่จะกรองให้ได้ข้อมูลเดิมที่ฝั่งรับ ด้วย PN ตัวเดียวกัน ซึ่งตามมาตรฐาน IEEE 802.15.4 นั้นได้มีการแบ่งช่องสัญญาณในย่าน 2.4 GHz ให้มี 16 ช่องสัญญาณ (2400-2483.5 MHz) ย่าน 902-928 MHz มี 10 ช่องสัญญาณ และย่าน 868.3 MHz อีก 1 ช่องสัญญาณ ดังแสดงในภาพที่ 3

อย่างไรก็ตาม ในการใช้การกระจายสเปกตรัมแบบลำดับตรงก็มีผลกับการสร้างหน่วยประมวลผลซึ่งมีความซับซ้อนกว่าการกระจายเปกตรัมแบบกระโดดความถี่ แต่ก็มีข้อดี คือ ทำให้ผู้

ไม่หวังดีดักจับข้อมูลได้ยากเพราะสัญญาณที่ส่งจะคล้ายกับสัญญาณรบกวน และการทำให้ได้มาซึ่งข้อมูลต้นฉบับนั้นก็ทำได้ยาก ซึ่งตามมาตรฐาน IEEE 802.15.4 จะมีการใช้เทคนิคการกระจายสเปกตรัมแบบลำดับตรงนี้ในกระบวนการกล้ำสัญญาณของโหนด ดังนั้นจึงไม่มีการนำมาใช้ในการหลบหลีกการรบกวนอีก เพราะข้อจำกัดในเรื่อง Chip rate ของอุปกรณ์ที่จะนำมาใช้ที่สูงสุดในปัจจุบันอยู่ที่ 2 Mchip/s ซึ่งไม่เพียงพอในการที่จะรองรับการทำงานด้วยกระบวนการกระจายสเปกตรัมแบบลำดับตรงอีก รวมทั้งตัวโหนดเองก็ต้องการกำลังส่งที่ต่ำ คือ 0 dBm (1mW) เพื่อการประหยัดพลังงาน ทำให้เครือข่ายตัวรับรู้ไร้สายจึงมักจะใช้งานไม่ได้หากอยู่ภายใต้พื้นที่การรบกวนจากอุปกรณ์รบกวนสัญญาณ

3.6 การผสมระหว่าง FHSS และ DSSS

เป็นวิธีการที่นำการกระจายสเปกตรัมแบบลำดับตรงและการกระจายสเปกตรัมแบบกระโดดความถี่มาใช้ในการสร้างกระบวนการกล้ำสัญญาณร่วมกัน เนื่องจากโดยทั่วไปแล้วการกระจายสเปกตรัมแบบลำดับตรงจะช่วยในการลดทอนการรบกวนด้วยการใช้ปริมาณการรับส่งข้อมูลที่กว้างในการส่งข้อมูล ขณะที่การกระจายสเปกตรัมแบบกระโดดความถี่จะช่วยในการการหลบหลีกการรบกวนด้วยการเปลี่ยนความถี่ ดังนั้นหากนำเทคนิคทั้งสองนี้มาใช้ในการสร้างกระบวนการในการกล้ำสัญญาณ ก็จะช่วยให้การป้องกันการรบกวนจากอุปกรณ์รบกวนสัญญาณมีประสิทธิภาพสูงมากขึ้น แต่การสร้างกระบวนการกล้ำสัญญาณแบบใหม่นั้นค่อนข้างมีความซับซ้อนและยุ่งยาก ต้องใช้ระยะเวลานานในการทำวิจัย ดังนั้นวิธีการดังกล่าวนี้จึงยังไม่ได้มีการนำมาใช้กับโหนดตัวรับรู้ไร้สายในปัจจุบัน

3.7 เทคโนโลยีอัลตราไวด์แบนด์

เป็นวิธีการที่จะนำเทคโนโลยีอัลตราไวด์แบนด์ (UWB: Ultra Wide Band) ซึ่งใช้เทคนิคการกล้ำสัญญาณด้วยการส่ง Pulses สั้นมากๆ บนย่านความถี่ในเวลาเดียวกัน ซึ่งการส่งด้วยเทคนิคนี้จะยากมากในการสกัดกั้นหรือรบกวน เนื่องจากมีการส่งสัญญาณบนช่วงความถี่ที่กว้างมาก หากนำ มาใช้กับเครือข่ายตัวรับรู้ไร้สายจะส่งผลดีอย่างมากในการป้องกันการรบกวน แต่ในการที่จะนำเทค โนโลยีนี้มาใช้งานยังจะต้องอยู่ภายใต้เงื่อนไขที่ต้องใช้พลังงานต่ำและต้นทุนที่ต่ำ ซึ่งเทคโนโลยี UWB ตามมาตรฐานของ IEEE จะใช้ชื่อว่า IEEE 802.15.3 ซึ่งขณะนี้อยู่ในช่วงของการพัฒนายังไม่ได้มีการนำมาใช้งานจริง

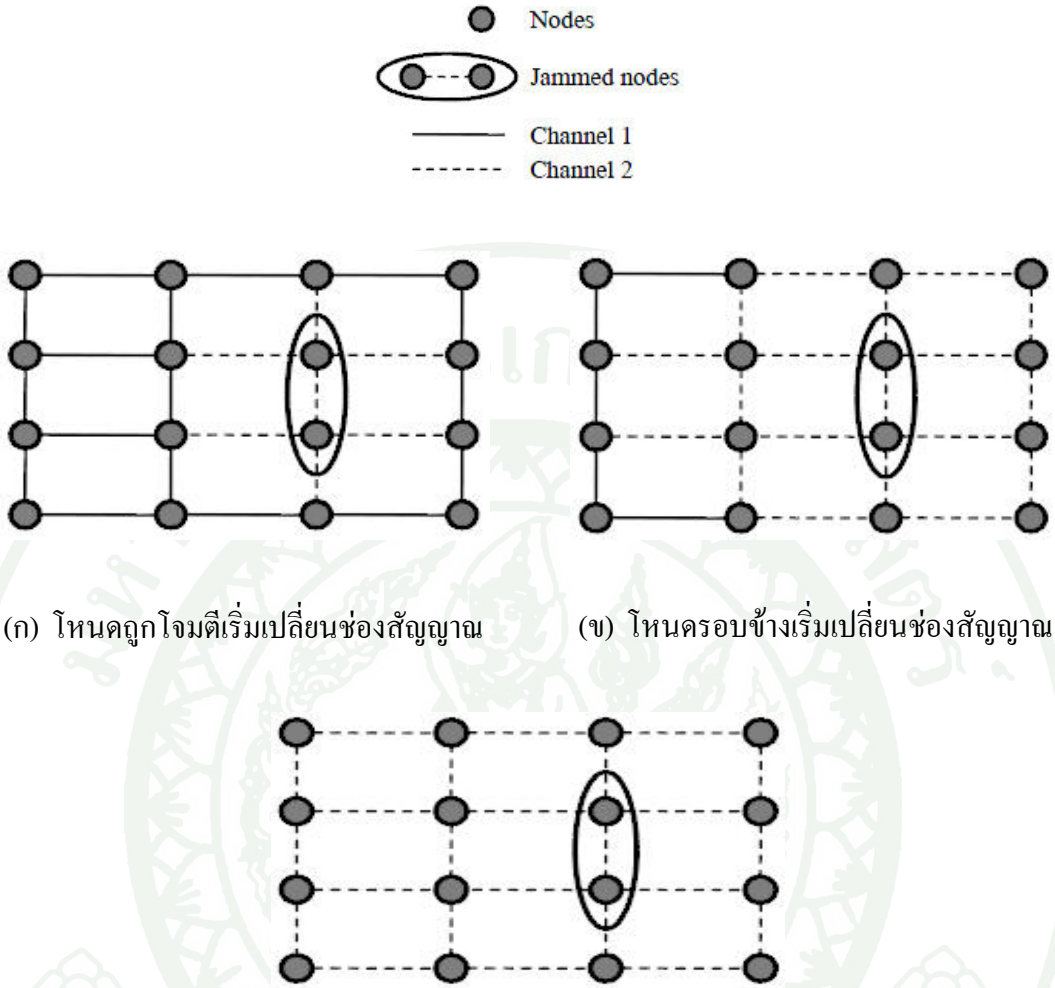
สำหรับในงานวิจัยนี้เราจะสนใจไปที่วิธีการกระจายสเปกตรัมแบบกระโดดความถี่ เนื่องจากเป็นวิธีการที่มีประสิทธิภาพในการหลบหลีกการรบกวนและจะนำไปสู่การสร้างเทคนิคการเปลี่ยนช่องสัญญาณ (Channel surfing) เพื่อหลบหลีกการรบกวน ซึ่งเราใช้ในการศึกษาสำหรับงานวิจัยนี้

4. กระบวนการเปลี่ยนช่องสัญญาณ

กระบวนการเปลี่ยนช่องสัญญาณ (Channel surfing algorithm) ตามงานวิจัยของ Wenyuan *et al*. (2004) มีพื้นฐานมาจากการกระจายสเปกตรัมแบบกระโดดความถี่ โดยแทนที่การกระโดดความถี่ (Hopping) จะเกิดขึ้นตลอดเวลาระหว่างความถี่หนึ่งไปยังอีกความถี่หนึ่งเหมือนกับในกระบวนการกระจายสเปกตรัมแบบกระโดดความถี่ แต่จะมีการเปลี่ยนไปใช้ความถี่อื่นเมื่อเกิดการโจมตีจากอุปกรณ์รบกวนสัญญาณเท่านั้น โดยเมื่อโหนดตรวจพบว่าตัวเองถูกโจมตี โหนดจะทำการเปลี่ยนไปใช้งานช่องสัญญาณใหม่ และเมื่อโหนดข้างเคียงตรวจพบว่ามีโหนดหายไปก็จะทำการเปลี่ยนไปใช้งานช่องสัญญาณใหม่เช่นเดียวกัน โดยเมื่อโหนดทำการเปลี่ยนช่องสัญญาณแล้วก็จะมีการตรวจหาโหนดข้างเคียงเพื่อที่จะสร้างการสื่อสารขึ้นมาใหม่อีกครั้ง โดยตามงานวิจัยของ Kristopher and Salem (2009) เทคนิคการเปลี่ยนช่องสัญญาณนี้สามารถแบ่งออกได้เป็น 2 แบบ คือ Coordinated channel switching และ Spectral multiplexing ดังรายละเอียดต่อไปนี้

4.1 Coordinated Channel Switching

ใน Coordinated channel switching นั้น หากเกิดการโจมตีขึ้น ซึ่งตามงานวิจัยของ Wenyuan *et al*. (2007) โหนดทั้งหมดในเครือข่ายจะเปลี่ยนไปใช้ช่องสัญญาณใหม่ที่ไม่ถูกรบกวนเพื่อให้สามารถสร้างการสื่อสารขึ้นมาใหม่และสื่อสารข้อมูลกันได้อีกครั้ง ซึ่งรูปแบบในการเปลี่ยนช่องสัญญาณจะเป็นไปตามกระบวนการในการสุ่ม (Pseudo-random) แต่การจะเปลี่ยนช่องสัญญาณของโหนดให้ครบทั้งหมดในเครือข่ายนั้นก็ต้องการระยะเวลาในการเปลี่ยนช่องสัญญาณและการสร้างการสื่อสารขึ้นมาใหม่บนช่องสัญญาณใหม่ก็ต้องการระยะเวลาเช่นเดียวกัน



(ก) โหนดถูกโจมตีเริ่มเปลี่ยนช่องสัญญาณ (ข) โหนดรอบข้างเริ่มเปลี่ยนช่องสัญญาณ

(ค) โหนดทั้งหมดเปลี่ยนไปใช้งานช่องสัญญาณที่ 2

ภาพที่ 4 ลักษณะการทำงานของ Coordinated channel switching

การทำงานของ Coordinated channel switching จะเริ่มขึ้นเมื่อโหนดในเครือข่ายบางส่วนนั้นถูกโจมตีบนช่องสัญญาณที่ 1 ดังแสดงตามภาพที่ 4 โดยเมื่อโหนดตรวจพบว่าถูกโจมตีก็จะทำการเปลี่ยนไปใช้ช่องสัญญาณที่ 2 โดยเริ่มแรกจะเปลี่ยนเฉพาะโหนดที่อยู่ภายใต้พื้นที่การรบกวนเท่านั้น ดังแสดงตามภาพที่ 4 (ก) ต่อมาโหนดข้างเคียงรอบๆ พื้นที่การโจมตีก็จะตรวจพบว่ามีโหนดหายไป ทำให้เริ่มเปลี่ยนช่องสัญญาณตาม ดังแสดงตามภาพที่ 4 (ข) จนเมื่อเวลาผ่านไปโหนดทุกตัวในเครือข่ายก็เปลี่ยนไปสื่อสารกันช่องสัญญาณที่ 2 ที่ไม่ถูกโจมตี ดังแสดงตามภาพที่ 4 (ค) โดยเมื่อโหนดเปลี่ยนช่องสัญญาณจากช่อง 1 ไปช่อง 2 เสร็จเรียบร้อยแล้ว ก็จะทำการตรวจสอบโหนดอื่นข้างเคียงและเริ่มสร้างกระบวนการสื่อสารอีกครั้งบนช่องสัญญาณใหม่

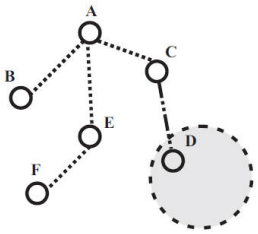
4.2 Spectral Multiplexing

การทำงานของ Coordinated channel switching จะต้องใช้การเปลี่ยนช่องสัญญาณของโหนดทั้งหมดบนเครือข่ายในการสร้างการสื่อสารขึ้นมาใหม่ ซึ่งต้องการระยะเวลาในการรอ โดยหากโหนดในเครือข่ายยิ่งมีจำนวนมากระยะเวลาในการรอจะยิ่งนาน ดังนั้นการเปลี่ยนช่องสัญญาณจึงควรจะเกิดขึ้นเฉพาะบริเวณพื้นที่ที่ได้รับผลกระทบจากการโจมตีเท่านั้น โดยโหนดที่ไม่ได้อยู่ภายใต้พื้นที่การรบกวนก็ควรที่จะทำงานตามปกติบนช่องสัญญาณเดิม แต่การเปลี่ยนช่องสัญญาณใหม่จะเกิดขึ้นเฉพาะโหนดที่อยู่ภายใต้พื้นที่การรบกวนเท่านั้น และเพื่อเป็นการทำให้โหนดที่อยู่ภายใต้พื้นที่การรบกวนและนอกพื้นที่สามารถสื่อสารข้อมูลกันได้ โหนดที่อยู่บริเวณขอบของพื้นที่การรบกวน (Boundary node) จึงควรที่จะมีการเปลี่ยนช่องสัญญาณไปมาระหว่าง 2 ช่องสัญญาณ เพื่อให้โหนด 2 โซนสามารถสื่อสารข้อมูลกันได้ ซึ่งวิธีการดังกล่าวนี้เรียกว่า Spectral multiplexing โดยตามงานวิจัยของ Wenyuan *et al*. (2006, 2007) สามารถแบ่งออกได้เป็น 2 แบบ ได้แก่ Synchronous spectral multiplexing และ Asynchronous spectral multiplexing

4.2.1 Synchronous spectral multiplexing

Synchronous spectral multiplexing จะทำงานตามช่วงเวลา (Slot time) ดังแสดงตามภาพที่ 5 โดยโหนด D เป็นโหนดที่ถูกโจมตี ซึ่งได้มีการเปลี่ยนไปทำงานบนช่องสัญญาณที่ 2 และมีการเชื่อมต่ออยู่กับโหนด C ซึ่งเป็นโหนดที่อยู่บริเวณขอบของพื้นที่การรบกวน โดยโหนด C นี้จะเป็นตัวกลางในการเชื่อมต่อระหว่างโหนดที่อยู่ภายใต้พื้นที่การรบกวน (โหนด D) กับโหนดอื่นที่อยู่นอกพื้นที่การรบกวน (A B E F) ซึ่งทำงานภายใต้สภาวะปกติบนช่องสัญญาณ 1 ที่ Slot 1 โดยโหนด C สามารถส่งแพ็กเกตไปยังโหนด A ได้ แต่ไม่สามารถรับแพ็กเกตจากโหนด D ได้ และเมื่อการทำงานบน Slot 1 สิ้นสุดลง การรับส่งข้อมูลบนช่องสัญญาณ 1 จะหยุดลง และโหนด C จะเปลี่ยนการทำงานไปยังช่องสัญญาณ 2 ที่ Slot 2 และจะทำการรับส่งข้อมูลกับโหนด D โดยโหนด C จะเก็บแพ็กเกตทั้งหมดที่รับได้จากโหนด D ไว้ในหน่วยความจำ (Buffer) เมื่อสิ้นสุด Slot 2 โหนด D จะหยุดการรับส่งข้อมูลกับโหนด C และโหนด C ก็จะทำการเปลี่ยนกลับมายังช่องสัญญาณ 1 อีกครั้ง เพื่อสื่อสารข้อมูลกับโหนด A โดยโหนด C จะเปลี่ยนช่องสัญญาณไปมาระหว่าง 2 ช่องสัญญาณนี้ จนกว่าการโจมตีจะสิ้นสุดลง ซึ่งกำหนดให้ระยะเวลาในการอยู่บนช่องสัญญาณแต่ละช่องนั้นน้อยสุดที่ 250 msec (สำหรับ CC1000 chip) และสามารถรับข้อมูลมาเก็บใน

หน่วยความจำได้จนเต็มที่ 10 แพ็กเกต โดยที่ช่องสัญญาณ 1 โหนดมีอัตราการส่งข้อมูลที่ 20 แพ็กเกตต่อวินาที และที่ช่องสัญญาณ 2 ที่ 10 แพ็กเกตต่อวินาที



slot 1	A, B, C, E, F
slot 2	C, D

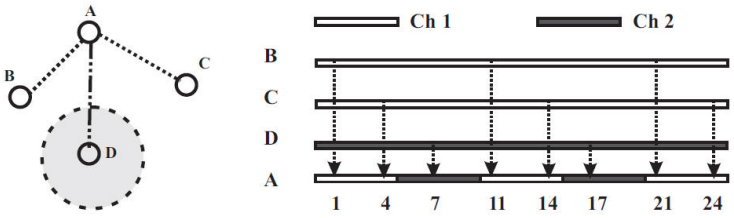
ภาพที่ 5 ลักษณะการทำงานของ Synchronous spectral multiplexing

ที่มา: Wenyuan *et al.* (2006, 2007)

อย่างไรก็ตามการใช้งาน Synchronous spectral multiplexing ก็มีสิ่งที่ต้องกังวล คือเรื่องความผิดพลาดของกระบวนการ Synchronization ซึ่งทำให้เกิด Synchronization overhead ขึ้น เนื่องจากโหนดที่เป็น Root (โหนด A) จะต้องมีการส่งแพ็กเกต SYN กระจายไปยังทุกโหนดในเครือข่ายตลอดเวลา แต่อาจมีบางช่วงเวลาที่โหนดบางตัวอาจไม่ได้มีการทำงานอยู่ในช่องสัญญาณเดียวกันที่เวลาของการ Synchronization และสัญญาณนาฬิกา (Clock) ของโหนดแต่ละตัวเองก็มีไม่เท่ากัน จึงทำให้เกิดการสูญเสียแพ็กเกต SYN จำนวนมากในการดูแลรักษาระบบทั้งหมด

4.2.2 Asynchronous spectral multiplexing

Asynchronous spectral multiplexing มีลักษณะการทำงานที่คล้ายกับ Synchronous spectral multiplexing แต่ค่อนข้างจะดีกว่าในเรื่องของการกำหนดช่วงระยะเวลา (Slot duration) ในการทำงานอยู่บนแต่ละช่องสัญญาณ ซึ่งง่ายและยืดหยุ่นกว่า และโหนดที่เป็น Root (โหนด A) ก็ไม่ต้องทำการส่งแพ็กเกต Synchronization ไปยังโหนดทั้งหมดในเครือข่ายตลอดเวลา จึงทำให้เกิด Synchronization overhead ที่น้อยกว่า ซึ่งแสดงตามภาพที่ 6 โดยโหนด A ซึ่งเป็นโหนดบริเวณขอบของพื้นที่การรบกวนจะรับแพ็กเกตจากโหนด B C และ D ซึ่งจะเปลี่ยนช่องสัญญาณไปมาระหว่างช่องสัญญาณ 1 และ 2 เพื่อรับส่งข้อมูลระหว่างโซน โดยโหนด B C และ D จะทำการส่งแพ็กเกตข้อมูลทุกๆ 10 วินาที โดยเริ่มที่ 1 4 และ 7 ตามลำดับ และโหนด A จะทำการเปลี่ยนช่องสัญญาณทุกๆ 5 วินาที เพื่อทำการรับแพ็กเกตข้อมูลจากโหนดข้างเคียง



ภาพที่ 6 ลักษณะการทำงานของ Asynchronous spectral multiplexing

ที่มา: Wenyuan *et al.* (2006, 2007)

การตัดสินใจเลือกเปลี่ยนช่องสัญญาณของโหนด A จากช่องหนึ่งไปยังอีกช่องหนึ่ง จะพิจารณาจากระยะเวลาที่สามารถอยู่ได้บนแต่ละช่องสัญญาณ หากสิ้นสุดระยะเวลาก็จะทำการเปลี่ยนไปยังช่องสัญญาณใหม่ โดยระยะเวลาดังกล่าวสามารถหาได้จากความสัมพันธ์ของอัตราการส่งข้อมูล (Traffic rate) บนแต่ละช่องสัญญาณและขนาดหน่วยความจำของโหนด ซึ่งเป็นไปตามสมการที่ 1 โดยให้ข้อกำหนดว่าระยะเวลาที่อยู่บนช่องสัญญาณที่ 1 จะต้องมีค่ามากกว่าหรือเท่ากับระยะเวลาที่อยู่บนช่องสัญญาณที่ 2 $\left(t_1 \geq t_2\right)$

$$\frac{t_1}{r_1} + \frac{t_2}{r_2} = B \qquad (1)$$

โดยที่ t_1 คือ ระยะเวลาในการอยู่บนช่องสัญญาณที่ 1 มีหน่วยเป็นมิลลิวินาที

t_2 คือ ระยะเวลาในการอยู่บนช่องสัญญาณที่ 2 มีหน่วยเป็นมิลลิวินาที

r_1 คือ อัตราการส่งข้อมูลบนช่องสัญญาณที่ 1 มีหน่วยเป็นแพ็กเกตต่อวินาที

r_2 คือ อัตราการส่งข้อมูลบนช่องสัญญาณที่ 2 มีหน่วยเป็นแพ็กเกตต่อวินาที

B คือ ขนาดหน่วยความจำของโหนด มีหน่วยเป็นไบต์

นอกจากนี้ในงานวิจัยอื่นหากช่องสัญญาณมีเป็นจำนวนมาก กระบวนการในการตัดสินใจเลือกเปลี่ยนช่องสัญญาณใหม่จะใช้กระบวนการในการสุ่ม เช่น งานวิจัยของ Sudip *et al*. (2009) ที่ใช้วิธีสุ่มหาช่องสัญญาณใหม่ด้วย Pseudo-random และงานวิจัยของ Loukas *et al*. (2009) ที่ได้ปรับปรุงกระบวนการในการกระโดดทางความถี่ (Frequency hopping) แบบเดิมใหม่ เพื่อให้มีความปลอดภัยมากยิ่งขึ้น โดยเมื่อเปลี่ยนช่องสัญญาณไปแล้วจะมีเพียงบางช่วงเวลาเท่านั้นที่สามารถ

สื่อสารข้อมูลกันได้ ซึ่งช่วงเวลาดังกล่าวก็ได้มาจากกระบวนการในการสุ่มเช่นเดียวกัน แต่อย่างไรก็ตามงานวิจัยดังกล่าว การเปลี่ยนช่องสัญญาณของโหนดก็ไม่ได้เกิดขึ้นเฉพาะกับพื้นที่ที่ได้รับผลกระทบจากการโจมตี แต่เกิดขึ้นกับโหนดทั้งหมดบนเครือข่าย

งานวิจัยที่ได้กล่าวมาทั้งหมด มีวัตถุประสงเพื่อให้โหนดสามารถสื่อสารข้อมูลกันได้ภายใต้สภาวะที่มีการโจมตีจากอุปกรณ์รบกวนสัญญาณ โดยใช้วิธีการเปลี่ยนช่องสัญญาณเพื่อหลบหลีกการรบกวน ซึ่งมีประเด็นต่างๆ ที่สามารถนำมาสรุปเปรียบเทียบได้ ดังแสดงตามตารางที่ 1

ตารางที่ 1 เปรียบเทียบงานวิจัยเกี่ยวกับการเปลี่ยนช่องสัญญาณ

งานวิจัย	พฤติกรรมการเปลี่ยน Channel	กระบวนการเลือก Channel	จำนวน Channel	ประเภท Jammer	Boundary SYNC
Sudip *et al*. (2009)	Entire network	Pseudo-random	11	Reactive	N/A
Loukas *et al*. (2009)	Entire network	Random	8	Reactive	N/A
Wenyuan *et al*. (2006, 2007)	Entire network	Pseudo-random	10	Constant	N/A
	Boundary and jammed node	Alternate	2	Constant	No
งานวิจัยนี้	Boundary and jammed node	Pseudo-random	16	Reactive	Yes

โดยปกติแล้วหากระบบเครือข่ายตัวรับรู้ไร้สายมีขนาดเล็ก มีจำนวนโหนดภายในเครือข่ายน้อย การใช้วิธีการเปลี่ยนช่องสัญญาณของโหนดทั้งหมดบนเครือข่ายย่อมทำได้อย่างรวดเร็ว และสามารถสร้างการสื่อสารให้กลับมาใหม่ภายในระยะเวลาอันสั้น ซึ่งทำให้การสูญเสียข้อมูลมีจำนวนน้อย และหากการโจมตีจากอุปกรณ์รบกวนสัญญาณเกิดขึ้นแบบถาวรที่ช่องสัญญาณช่องใดช่องหนึ่งด้วยแล้ว การเปลี่ยนช่องสัญญาณด้วยวิธีการแบบนี้จะมีประสิทธิภาพสูงสุด

แต่หากระบบเครือข่ายตัวรับรู้ไร้สายมีขนาดใหญ่ มีโหนดภายในเครือข่ายจำนวนมาก การเปลี่ยนช่องสัญญาณของโหนดทั้งหมดบนเครือข่ายต้องใช้เวลานาน และช่วงระยะเวลาในการรอที่จะสร้างเครือข่ายบนช่องสัญญาณใหม่ก็จะนานตามไปด้วย ส่งผลให้เกิดการสูญเสียข้อมูลบน

เครือข่ายจำนวนมาก และหากการโจมตีจากอุปกรณ์รบกวนสัญญาณไม่ได้เกิดขึ้นแบบถาวรบนช่องสัญญาณช่องใดช่องหนึ่ง แต่สามารถเปลี่ยนช่องสัญญาณในการโจมตีได้ การเปลี่ยนช่องสัญญาณก็จะเกิดขึ้นบ่อยครั้ง ทำให้การสูญเสียข้อมูลจะยิ่งมีมากขึ้นและอาจทำให้การสื่อสารบนเครือข่ายไม่สามารถทำได้ ซึ่งปัญหาที่เกิดขึ้นนี้สามารถแก้ไขด้วยการใช้วิธีการ Spectral multiplexing ที่ทำการเปลี่ยนช่องสัญญาณเฉพาะโหนดที่อยู่บริเวณพื้นที่ที่ได้รับผลกระทบจากการรบกวนเท่านั้น และในงานวิจัยนี้ก็ได้ใช้วิธีการดังกล่าวสำหรับเป็นพื้นฐานให้กับงานวิจัย

สำหรับงานวิจัยนี้ เน้นให้ความสนใจไปที่การโจมตีที่เกิดขึ้นแบบชั่วคราวบริเวณใจกลางของเครือข่าย โดยอุปกรณ์รบกวนสัญญาณสามารถตรวจสอบการใช้ช่องสัญญาณและเปลี่ยนช่องสัญญาณในการโจมตีได้ และกระบวนการเปลี่ยนช่องสัญญาณจะเกิดขึ้นเฉพาะกับโหนดที่ได้รับผลกระทบจากการโจมตี คือ โหนดที่อยู่ภายใต้พื้นที่และขอบของพื้นที่การรบกวนเท่านั้น โดยในการตัดสินใจเลือกช่องสัญญาณใหม่สามารถที่จะเลือกใช้ช่องสัญญาณตามมาตรฐาน IEEE 802.15.4 ในย่าน 2.4 GHz ได้ทั้ง 16 ช่องสัญญาณด้วยกระบวนการสุ่ม (Pseudo-random) และในการเปลี่ยนช่องสัญญาณของโหนดที่อยู่บริเวณขอบของเครือข่ายจะมีกระบวนการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณของโหนดให้มีระยะเวลาที่เท่ากัน ซึ่งแตกต่างจากงานวิจัยของ Wenyuan *et al*. (2006, 2007) ที่ไม่ได้สนใจศึกษาการโจมตีที่เกิดขึ้นจากอุปกรณ์รบกวนสัญญาณแบบชั่วคราวที่เกิดขึ้นบริเวณใจกลางของเครือข่าย อีกทั้งไม่มีการใช้งานช่องสัญญาณตามมาตรฐาน IEEE 802.15.4 ในย่าน 2.4 GHz ให้ครบทั้งหมด และโหนดบริเวณขอบของเครือข่ายก็ยังไม่มีกระบวน การประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณ ดังนั้นจึงไม่สามารถที่จะทำให้เกิดประสิทธิ ภาพ และไม่ได้รับประสิทธิผลสูงสุดในการทำงาน

อุปกรณ์และวิธีการ

อุปกรณ์

1. ฮาร์ดแวร์
   1.1 เครื่องคอมพิวเตอร์ที่มีประสิทธิภาพในการคำนวณสูง
      1. หน่วยประมวลผล Intel(R), Core(TM) 2 Duo, P8600, 2.40 GHz
      2. หน่วยความจำ 4 GB
   1.2 โหนดตัวรับรู้ไร้สาย Tmote Sky
   1.3 อุปกรณ์รบกวนสัญญาณ
      1. บอร์ด Arduino Uno
      2. XBee series 1 รุ่น 4214A-XBEE
      3. แบตเตอรี่ขนาด 12 VDC, 9 A
      4. บอร์ดสำหรับเชื่อมต่อ Arduino Uno กับ XBee
      5. ตัวตรวจวัดแสง (Light sensor)

2. ซอร์ฟแวร์
   2.1 ระบบปฏิบัติการลินุกซ์ (Linux) Ubuntu รุ่น 11.10
   2.2 ระบบปฏิบัติการ TinyOS รุ่น 2.1.1
   2.3 ตัวแปลภาษาเนสซี (NesC) รุ่น 1.3.3
   2.4 ตัวแปลภาษาจาวา (JAVA) รุ่น JDK 1.6

วิธีการ

เริ่มต้นจากการวิเคราะห์ปัญหา นำเสนอวิธีการแก้ไขปัญหา และทดสอบสิ่งที่ได้นำเสนอในตอนท้าย ดังรายละเอียดต่อไปนี้

1. นิยามปัญหา

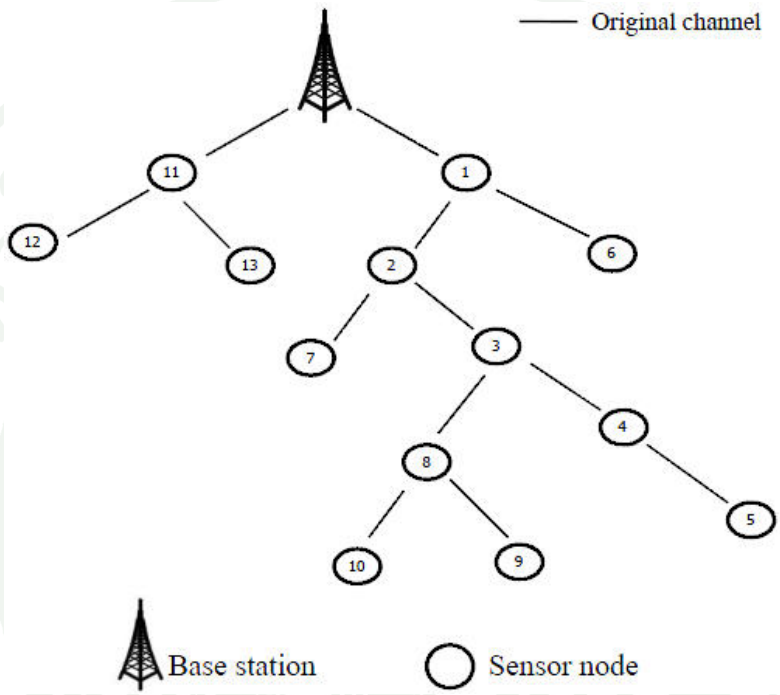
ในงานวิจัยของ Wenyuan *et al.*(2006, 2007) ที่ผ่านมา ได้มีการนำวิธีการ Spectral multiplexing มาใช้ในการหลบหลีกการรบกวนจากอุปกรณ์รบกวนสัญญาณนั้น หากมีช่องสัญญาณให้เลือกเพียง 2 ช่อง การตัดสินใจในการเลือกช่องสัญญาณคงสามารถทำได้ไม่ยากนัก แต่การจะใช้งานช่อง สัญญาณเพียง 2 ช่องนั้น ไม่สามารถทำให้เกิดประสิทธิภาพในการทำงานได้มากนัก โดยเฉพาะหากการโจมตีเกิดขึ้นกับช่องสัญญาณทั้ง 2 พร้อมกัน อีกทั้งยังไม่ทำให้เกิดประสิทธิผลสูงสุดในการทำงาน เพราะช่องสัญญาณตามมาตรฐาน IEEE 802.15.4 ในย่าน 2.4 GHz นั้นมีทั้งหมดถึง 16 ช่อง สัญญาณ แต่มีการใช้งานเพียง 2 ช่องสัญญาณเท่านั้น ดังนั้นการที่สามารถเลือกใช้ช่อง สัญญาณใหม่ตามมาตรฐาน IEEE 802.15.4 ในย่าน 2.4 GHz ที่มี 16 ช่องสัญญาณได้ทั้งหมด ย่อมจะทำให้เกิดประสิทธิภาพและได้ประสิทธิผลสูงสุดในการทำงาน

นอกจากนี้การเกิดการโจมตีที่บริเวณใจกลางของเครือข่ายนั้น หากนำวิธีการ Spectral multiplexing ที่มีอยู่เดิมมาใช้ไม่สามารถทำให้เกิดประสิทธิภาพเท่าที่ควร เพราะยังไม่มีกระบวนการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณของโหนดที่อยู่บริเวณขอบของเครือข่ายให้มีระยะเวลาที่เท่ากัน เนื่องจากในกระบวนการตรวจสอบการโจมตีนั้น โดยปกติแล้วโหนดจะมีการตรวจจับการโจมตีได้ในระยะเวลาที่ไม่เท่ากัน ทำให้กระบวนการทำงานในการเปลี่ยนช่องสัญญาณเกิดขึ้นไม่พร้อมกัน โดยเฉพาะอย่างยิ่งหากช่วงเวลาดังกล่าวมีความแตกต่างกันมากการสูญเสียข้อมูลก็จะยิ่งมีมากขึ้น เพราะโหนดที่อยู่บริเวณขอบของเครือข่ายที่ทำหน้าที่เป็นตัวรับข้อมูล ทำการเปลี่ยนช่องสัญญาณมาไม่ตรงกับช่วงเวลาของโหนดที่ต้องการส่งข้อมูล

2. ขั้นตอนวิธีที่นำเสนอในการแก้ปัญหา

ในการแก้ไขปัญหาของงานวิจัย จะทำการการปรับปรุงวิธีการเปลี่ยนช่องสัญญาณแบบ Spectral multiplexing ที่มีอยู่เดิม ซึ่งต่อจากนี้จะเรียกว่า Jamming Avoidance Algorithm for

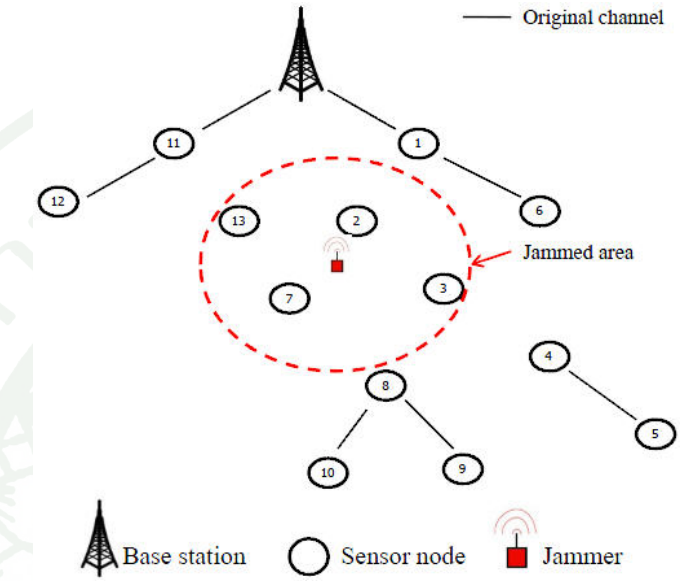
Wireless Sensor Network: JAWSN และในการสร้างระบบเครือข่ายตัวรับรู้ไร้สายเพื่อใช้ในการทดลองจะประกอบด้วย สถานีฐาน (Base station) และโหนดตัวรับรู้ (Sensor node) โดยในสภาวะปกติที่ไม่มีการโจมตีจากอุปกรณ์รบกวนสัญญาณโหนดทั้งหมดบนเครือข่ายจะสื่อสารข้อมูลกันบนช่องสัญญาณเดิม (Original channel) ตามปกติ ดังแสดงตามภาพที่ 7



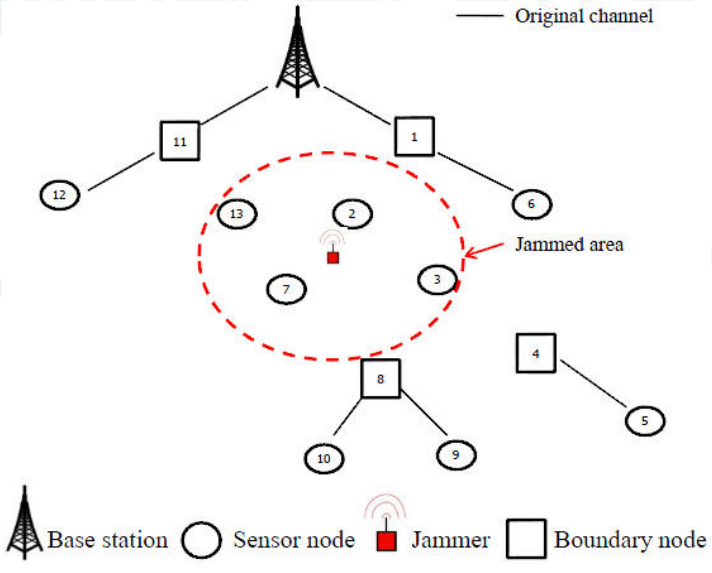
ภาพที่ 7 โครงสร้างระบบเครือข่ายตัวรับรู้ไร้สาย

โดยหากเครือข่ายเกิดการโจมตีจากอุปกรณ์รบกวนสัญญาณบริเวณใจกลางของเครือข่าย ดังแสดงตามภาพที่ 8 (ก) จะทำให้โหนด 2 3 7 และ 13 ซึ่งอยู่ภายใต้พื้นที่การรบกวนไม่สามารถสื่อสารกับโหนด 1 4 8 และ 11 ที่อยู่นอกพื้นที่การรบกวนได้ ดังนั้นโหนด 2 3 7 และ 13 จะทำการตรวจสอบการโจมตีที่เกิดขึ้น ตามกระบวนการทำงานดังแสดงในภาพที่ 9 หากตรวจพบว่าตัวเองอยู่ภายใต้พื้นที่การโจมตีจะทำการเปลี่ยนไปใช้งานช่องสัญญาณใหม่ตามลำดับของการสุ่มช่องสัญญาณที่ได้สุ่มไว้ในตาราง หลังจากเปลี่ยนช่องสัญญาณสำเร็จแล้วจะทำงานอยู่บนช่องสัญญาณดังกล่าว เพื่อจะเริ่มการสื่อสารกับโหนด 1 4 8 และ 11 บนช่องสัญญาณใหม่ต่อไป โดยหากช่อง สัญญาณใหม่นี้เกิดการโจมตีขึ้นอีก โหนด 2 3 7 และ 13 ก็จะทำงานตามกระบวนการเดิมดังที่กล่าวมาข้างต้น แต่การเปลี่ยนช่องสัญญาณใหม่นี้จะเป็นการเปลี่ยนกลับไปยังช่องสัญญาณเดิมในตอนเริ่มต้น (Original channel) ซึ่งไม่มีการถูกโจมตีแล้ว จากนั้นก็จะเริ่มการสื่อสารกับ

โหนด 1 4 8 และ 11 บนช่องสัญญาณเดิมอีกครั้ง จนกว่าจะมีการโจมตีเกิดขึ้น จึงจะเริ่มกระบวนการทำงานในแบบเดิมและเปลี่ยนช่องสัญญาณใหม่ตามลำดับการสุ่มในตารางอีกครั้งต่อไป

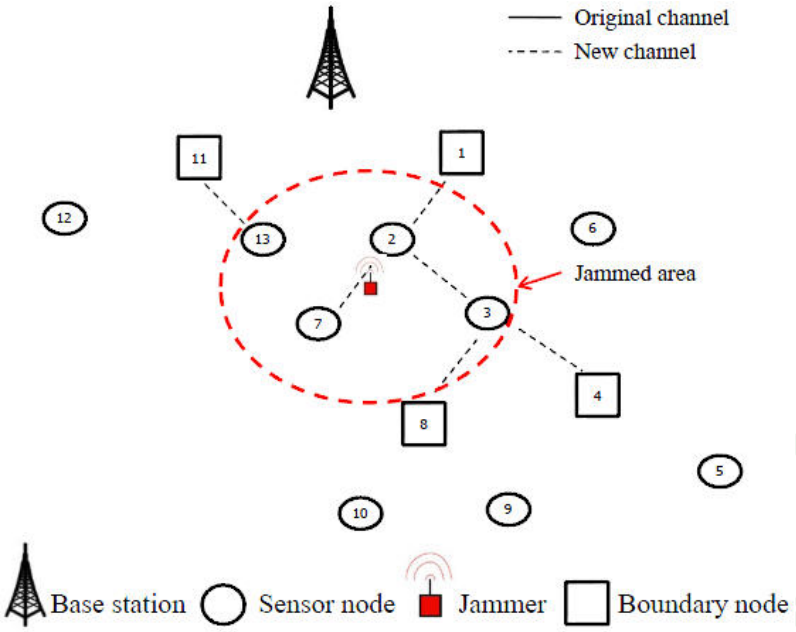


(ก) เกิดการโจมตีบริเวณใจกลางเครือข่าย



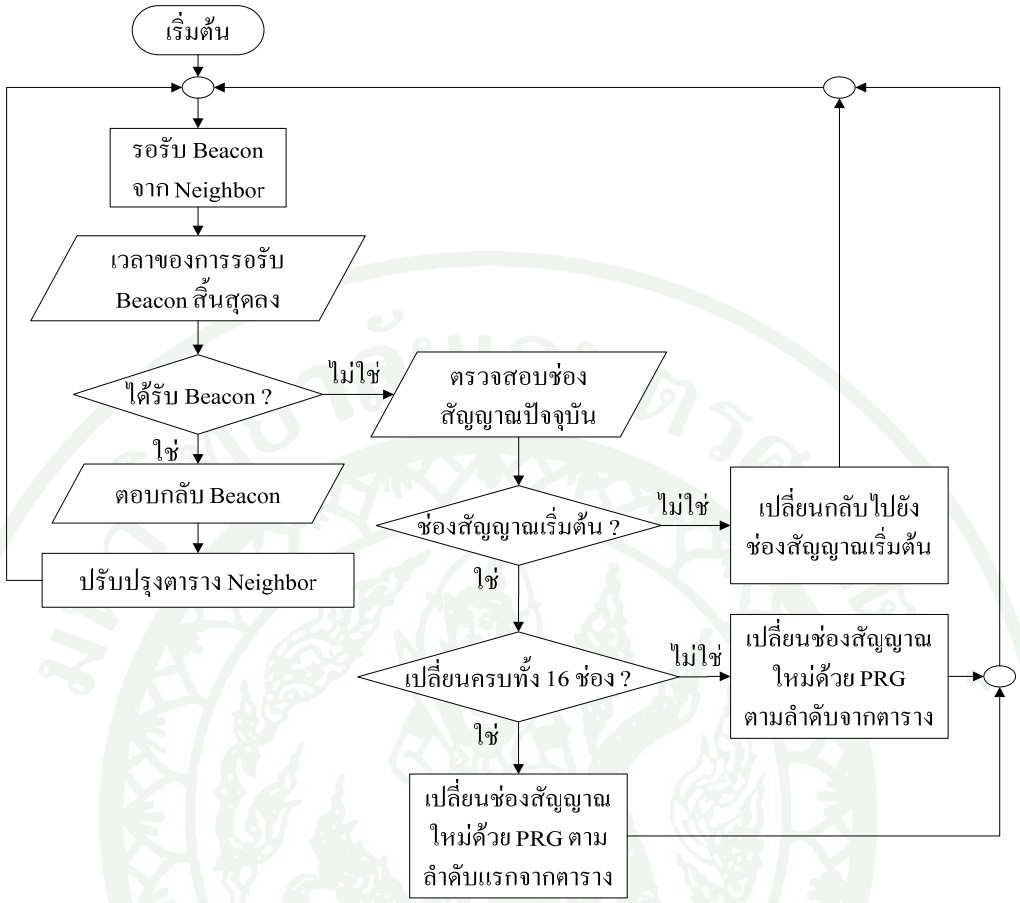
(ข) โหนดทำงานเป็น Boundary node

ภาพที่ 8 โครงสร้างระบบทดสอบที่ใช้ในการทดลอง



(ค) โหนดทำงานบนช่องสัญญาณใหม่

ภาพที่ 8 (ต่อ)



ภาพที่ 9 แผนภาพขั้นตอนการทำงานของโหนดภายใต้พื้นที่การรบกวน

การสร้างช่องสัญญาณใหม่ในลำดับถัดไปที่เก็บไว้ในตารางจะได้มาจากวิธีการในการสุ่มด้วย Pseudo-random Generator (PRG) แบบ Linear Congruential Generator (LCG) ตามสมการที่ 2 ซึ่งจะทำให้สามารถสร้างช่องสัญญาณใหม่ได้ครบทั้ง 16 ช่องสัญญาณ ตามมาตรฐาน IEEE 802.15.4 ย่าน 2.4 GHz

$$X_{n+1} = [a * X_n + c] \bmod M \qquad ; n \geq 0 \qquad (2)$$

โดยที่ M คือ จำนวนช่องสัญญาณทั้งหมด $(0 < M)$

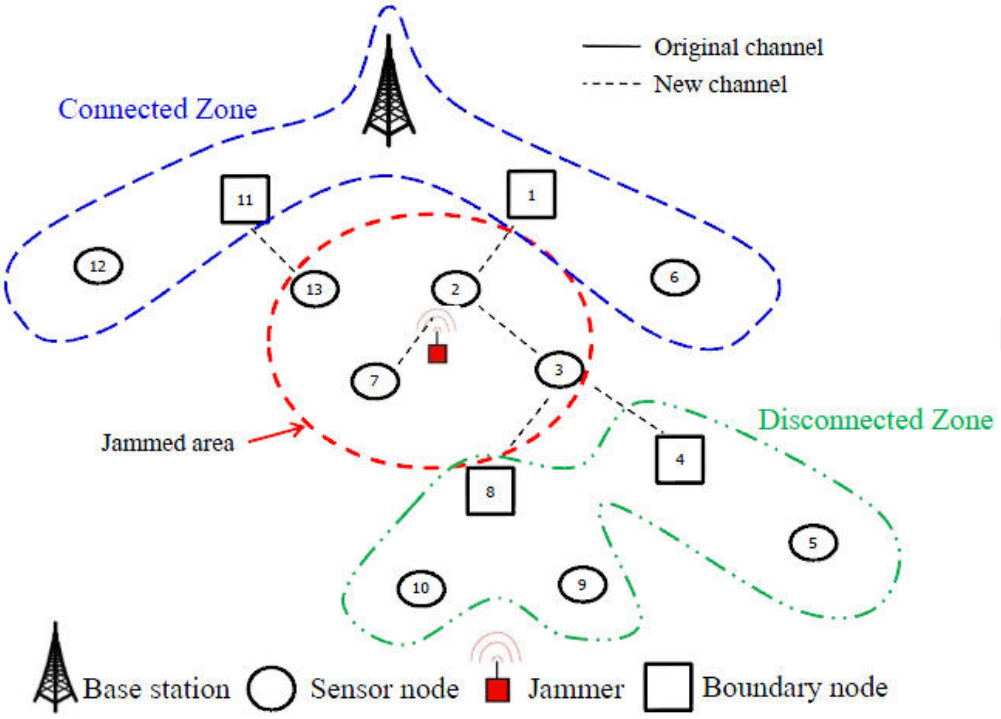
a, c คือ ค่าคงที่ $(0 < a < M,\ 0 \leq c < M)$

X_n คือ ลำดับของการสุ่ม

X_0 คือ ช่องสัญญาณเริ่มต้น $(0 \leq X_0 < M)$

จากสมการที่ 2 มีข้อกำหนดในการพิจารณาค่าตัวแปรในสมการเพิ่มเติม คือ c และ M เป็นจำนวนเฉพาะสัมพัทธ์ (Relatively prime) และ (a – 1) เป็นตัวประกอบเฉพาะ (Prime factors) ของ M โดยในการทดลองระบบงานวิจัยเพื่อให้ได้ลำดับในการสุ่มที่ไม่ซ้ำกัน จึงได้ทำการเลือกใช้ค่า c เท่ากับ 1 และค่า a เท่ากับ 5 โดยที่ M เท่ากับ 16

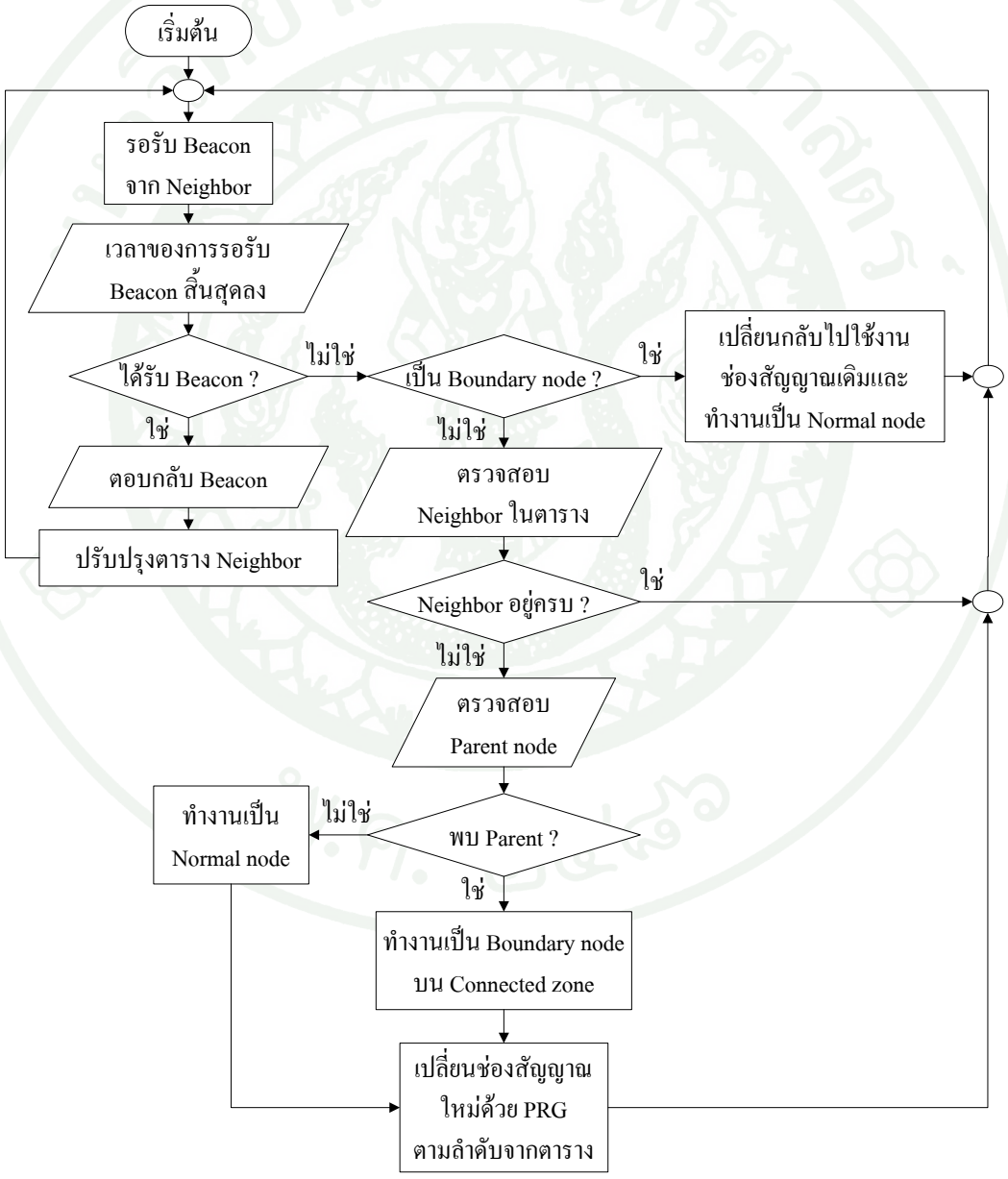
เมื่อโหนด 1 4 8 และ11 พบว่าโหนดเพื่อนบ้านหายไปจากตาราง โหนดดังกล่าวจะทำการตรวจสอบตัวเองว่าเป็นขอบของเครือข่าย แล้วจะทำงานเป็น Boundary node ดังแสดงตามภาพที่ 8 (ข) โดยในการตรวจสอบตัวเองของโหนด 1 4 8 และ 11 เพื่อพิจารณาว่าเป็นโหนดที่อยู่บริเวณขอบของพื้นที่การรบกวนนั้น จะแยกพิจารณาออกเป็น 2 กรณี คือ กรณีที่โหนดอยู่ในเขตพื้นที่เชื่อมต่อกับสถานีฐาน (Connected zone) และกรณีที่โหนดไม่ได้อยู่ในเขตพื้นที่เชื่อมต่อกับสถานีฐาน (Disconnected zone) ดังแสดงตามภาพที่ 10



ภาพที่ 10 การแบ่งพื้นที่ของโหนดเมื่อเกิดการโจมตีบริเวณใจกลางเครือข่าย

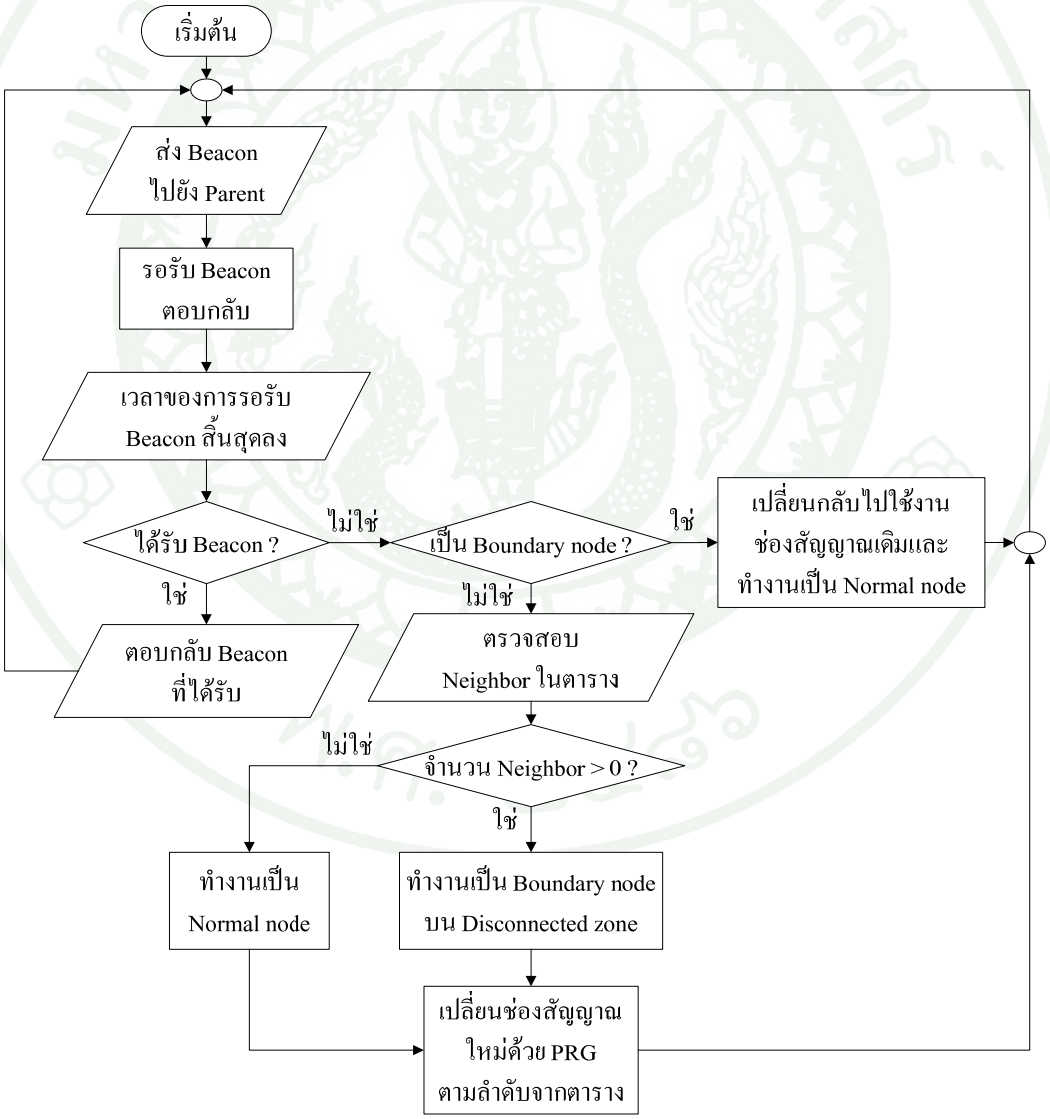
ในกรณีที่โหนดอยู่ในเขตพื้นที่เชื่อมต่อกับสถานีฐาน ได้แก่ โหนด 1 และ 11 การตรวจสอบการเป็น Boundary node จะพิจารณาจากตารางเพื่อนบ้าน (Neighbor table) ดังแสดงกระบวน การทำงานตามภาพที่ 11 โดยหากมีการตรวจสอบพบว่ามีโหนดในตารางเพื่อนบ้าน

หายไป เนื่องจากการที่ไม่ได้รับ Beacon จากเพื่อนบ้าน เพื่อใช้สำหรับการปรับปรุงค่าต่างๆ ในตาราง โหนดจะทำการตรวจสอบการมีอยู่ของโหนดแม่ (Parent node) ซึ่งหากพบโหนดแม่ โหนดดังกล่าวจะเป็นขอบของพื้นที่การรบกวน ดังนั้นโหนดจะปรับโหมดตัวเองให้ทำงานเป็น Boundary node แล้วจะทำการเปลี่ยนไปใช้งานช่องสัญญาณใหม่ตามลำดับการสุ่มเดียวกับ 2 3 7 และ 13 ซึ่งจะทำให้สามารถสื่อสารข้อมูลกับโหนดที่อยู่ภายใต้พื้นที่การโจมตีบนช่องสัญญาณใหม่ได้ ดังแสดงตามภาพที่ 8 (ค)



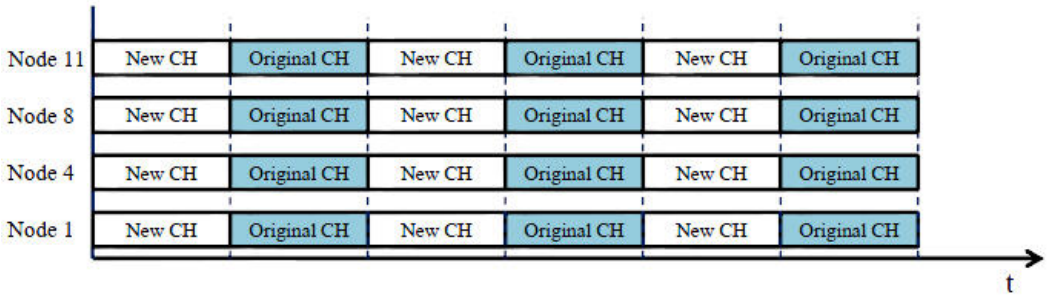
ภาพที่ 11 แผนภาพขั้นตอนการทำงานของ Boundary node ใน Connected zone

ในกรณีที่โหนดไม่ได้อยู่ในเขตพื้นที่เชื่อมต่อกับสถานีฐาน ได้แก่ โหนด 4 และ 8 การตรวจสอบการเป็น Boundary node จะพิจารณาจากโหนดแม่ โดยจะมีการส่ง Beacon ไปตรวจสอบตามช่วงเวลา ดังแสดงกระบวนการทำงานตามภาพที่ 12 โดยหากครบกำหนดเวลาในการรอรับ Beacon ตอบกลับแล้วยังไม่ได้รับการตอบกลับจากโหนดแม่ โหนดจะทำการตรวจสอบว่ายังมีโหนดเหลืออยู่ในตารางเพื่อนบ้านหรือไม่ โดยหากมีโหนดเหลืออยู่ โหนดจะเป็นขอบของพื้นที่การรบกวน ดังนั้นโหนดจะปรับโหมดตัวเองให้ทำงานเป็น Boundary node แล้วจะทำการเปลี่ยนไปใช้งานช่องสัญญาณใหม่ตามลำดับการสุ่มเดียวกับ 2 3 7 และ 13 ซึ่งจะทำให้สามารถสื่อสารข้อมูลกับโหนดที่อยู่ภายใต้พื้นที่การ โจมตีบนช่องสัญญาณใหม่ได้ ดังแสดงตามภาพที่ 8 (ค)



ภาพที่ 12 แผนภาพขั้นตอนการทำงานของ Boundary node ใน Disconnected zone

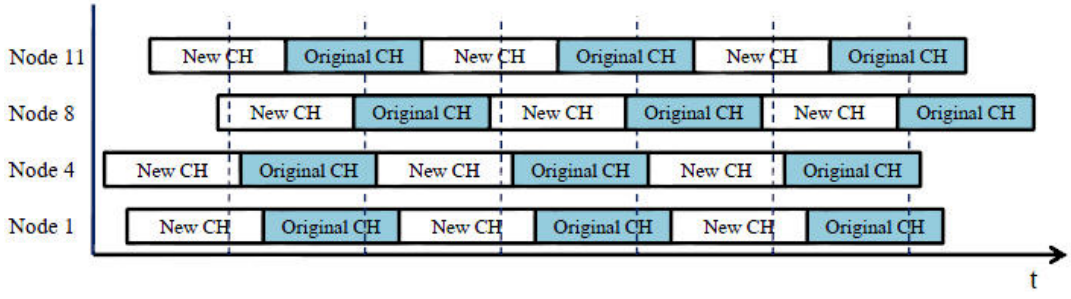
ในกระบวนการทำงานของโหนด 1 4 8 และ 11 ซึ่งเป็น Boundary node การเปลี่ยนช่องสัญญาณจะมีลักษณะสลับไปมาระหว่างช่องสัญญาณใหม่และช่องสัญญาณเดิมตามกำหนดเวลา ดังแสดงตัวอย่างการทำงานตามภาพที่ 13



ภาพที่ 13 ลักษณะการเปลี่ยนช่องสัญญาณตามกำหนดเวลาของ Boundary node

ในระหว่างการอยู่บนแต่ละช่องสัญญาณ ข้อมูลที่ Boundary node รับได้จะถูกเก็บเข้าไว้ยังหน่วยความจำ เมื่อครบกำหนดเวลาของการอยู่บนช่องสัญญาณใหม่ Boundary node ก็จะเปลี่ยนกลับมายังช่องสัญญาณเดิมเพื่อจะสื่อสารข้อมูลกับโหนดที่ไม่ถูกโจมตี และเมื่อครบกำหนดระยะเวลาของการอยู่บนช่องสัญญาณเดิมก็จะทำการเปลี่ยนไปทำงานบนช่องสัญญาณใหม่อีกครั้ง ด้วยการทำงานในลักษณะดังกล่าวนี้ จะทำให้ข้อมูลที่ได้เก็บไว้ในหน่วยความจำสามารถส่งต่อไปยังสถานีฐานได้ โดยระยะเวลาของการอยู่บนแต่ละช่องสัญญาณในงานวิจัยจะกำหนดให้ระยะเวลาในการอยู่บนช่องสัญญาณเดิมมีค่าเท่ากับระยะเวลาในการอยู่บนช่องสัญญาณใหม่ เพื่อจะทำให้ Boundary node สามารถรับส่งข้อมูลบนทั้งสองช่องสัญญาณได้ในปริมาณที่เท่ากัน

ในกระบวนการทำงานของการเปลี่ยนไปใช้ช่องสัญญาณใหม่ของ Boundary node ส่วนใหญ่จะมีการเปลี่ยนไปใช้งานช่องสัญญาณใหม่ที่ไม่พร้อมกัน เนื่องจากกระบวนการตรวจสอบการโจมตีของแต่ละโหนดมีจังหวะเวลาที่แตกต่างกัน ดังแสดงตัวอย่างตามภาพที่ 14

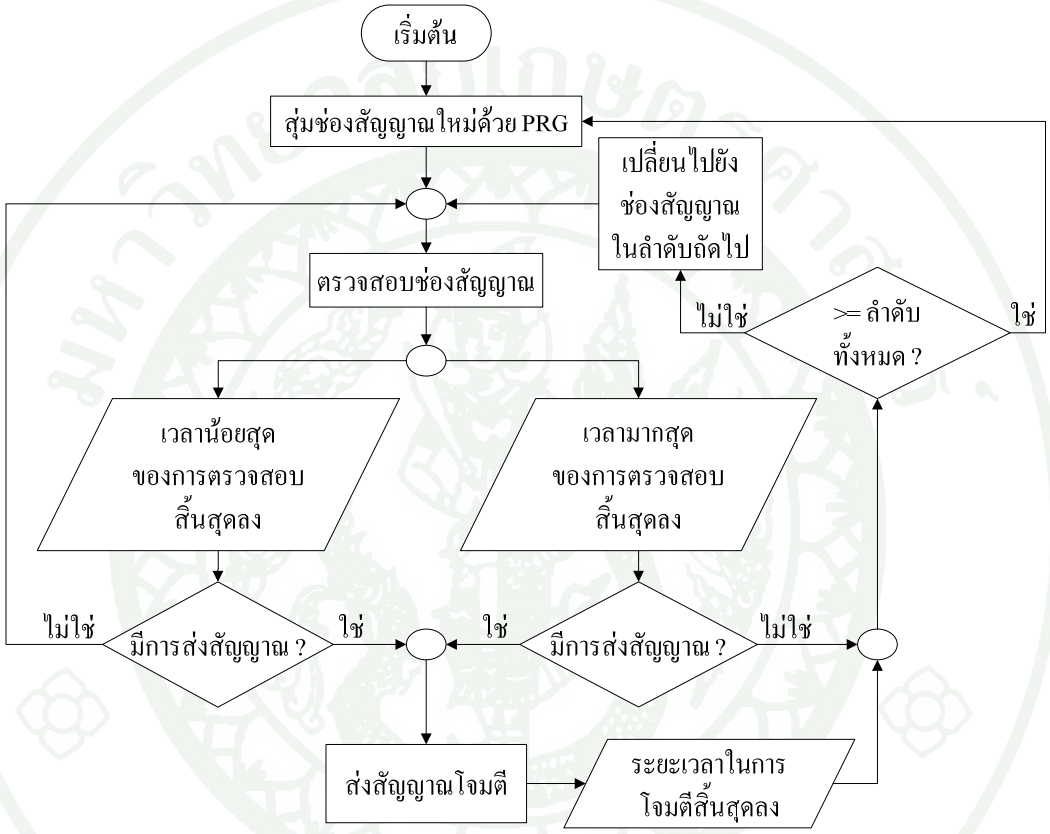


ภาพที่ 14 การเปลี่ยนช่องสัญญาณเกิดขึ้นไม่พร้อมกันของ Boundary node

จากเหตุการณ์ที่เกิดขึ้นตามภาพที่ 14 จะส่งผลทำให้การรับส่งข้อมูลเกิดการสูญหายได้หากโหนดแม่ (Parent node) เปลี่ยนมารับไม่ทันการส่งของโหนดลูก (Child node) ดังนั้นเพื่อแก้ปัญหาดังกล่าวจึงทำการเลือก Master boundary node เพื่อให้ทำหน้าที่เป็นโหนดควบคุมให้ Boundary node ทั้งหมดสามารถประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณให้พร้อมกันได้ โดยในการเลือก Master boundary node จะใช้ค่า ID ของ Boundary node ทั้งหมดบนเครือข่ายในการพิจารณา ซึ่ง Boundary node ที่มีค่า ID น้อยที่สุด จะถูกรับเลือกให้เป็น Master boundary node นอกจากนี้แล้วยังจะพิจารณาจากการแบ่งพื้นที่บนเครือข่ายร่วมด้วย ดังนั้นนอกจากจะมี ID น้อยสุดแล้ว Master boundary node จะต้องอยู่ในพื้นที่ที่ไม่ได้เชื่อมต่ออยู่กับสถานีฐานด้วย เนื่องจากหากอยู่บริเวณที่เชื่อมต่ออยู่กับสถานีฐาน ซึ่งจะต้องทำหน้าที่มารับข้อมูลจากโหนดลูกบนช่องสัญญาณใหม่ โดยหากมีการส่งข้อมูลเข้ามาจำนวนมากอาจทำให้เกิดการสูญเสียจังหวะในการควบคุม Boundary node ตัวอื่นๆ ได้ และนอกจากจะทำการควบคุมจังหวะเวลาของการเปลี่ยนช่องสัญญาณแล้ว Master boundary node ยังทำหน้าที่ในการปรับปรุงลำดับของช่องสัญญาณถัดไปให้กับโหนดอื่นๆ เพื่อให้มีลำดับช่องสัญญาณถัดมีค่าตรงกันหากเกิดการโจมตีขึ้นอีกครั้ง โดยการ Broadcast แพ็กเกตควบคุมที่ใช้สำหรับปรับปรุงลำดับช่องสัญญาณให้กับโหนดทั้งหมดบนเครือข่าย ซึ่งหากโหนดอื่นๆ ได้รับแพ็กเกตดังกล่าวก็จะทำการปรับปรุงลำดับช่องสัญญาณถัดไปให้มีค่าเดียวกับ Master boundary node และในระหว่างกระบวนการทำงานที่เกิดการโจมตี โหนด 6 5 9 10 และ 12 ซึ่งไม่ได้รับผลกระทบจากสัญญาณการโจมตีจะทำงานตามปกติ แต่จะไม่สามารถส่งข้อมูลไปยังโหนดแม่ได้ในระหว่างที่โหนดแม่ที่ทำงานเป็น Boundary node แล้วมีการเปลี่ยนไปทำงานยังช่องสัญญาณอื่น แต่จะต้องมีการรอจังหวะที่โหนดแม่เปลี่ยนกลับมายังช่องสัญญาณเดิมถึงจะสามารถสื่อสารข้อมูลกันได้ตามปกติ

สำหรับขั้นตอนการทำงานของอุปกรณ์รบกวนสัญญาณในงานวิจัย ดังแสดงตามภาพที่ 15 จะเริ่มจากกระบวน PRG เพื่อสุ่มหาลำดับช่องสัญญาณ โดยช่องสัญญาณเริ่มต้นที่ป้อนให้กับสมการจะได้มาจากอุปกรณ์ตรวจวัดแสง จากนั้นจะนำช่องสัญญาณที่สุ่มได้ไปเก็บไว้ในตารางตามลำดับที่ได้จากการสุ่ม ซึ่งในการเปลี่ยนช่องสัญญาณก็จะเปลี่ยนตามลำดับในตาราง โดยจะเริ่มจากลำดับแรกก่อน เมื่อเปลี่ยนช่องสัญญาณแล้วจะเริ่มทำการตรวจสอบการใช้งานช่องสัญญาณของโหนดตัวรับรู้ ซึ่งระยะเวลาในการตรวจสอบจะเป็นไปตามกำหนดเวลา โดยหากสิ้นสุดระยะเวลาดังกล่าวแล้วไม่พบว่ามีการใช้งานช่องสัญญาณก็จะทำการเปลี่ยนไปใช้งานช่องสัญญาณในลำดับถัดไปจากตาราง หากมีการใช้งานช่องสัญญาณจนครบทั้งหมดจากในตารางจะทำการเริ่มกระบวนการ PRG เพื่อสุ่มหาลำดับช่องสัญญาณใหม่อีกครั้งแล้วจึงเข้าสู่กระบวนการทำงานในแบบเดิม โดยในการ

ตรวจสอบการใช้งานช่องสัญญาณนั้น หากสิ้นสุดระยะเวลาในการตรวจสอบ แล้วพบว่ามีการใช้งานช่องสัญญาณ อุปกรณ์รบกวนสัญญาณจะทำการส่งสัญญาณรบกวนเพื่อทำการโจมตีโหนดตัวรับรู้ที่อยู่ในรัศมีการทำงาน ซึ่งจะใช้เวลาในการโจมตีตามกำหนดเวลาเช่นเดียวกัน และเมื่อครบกำหนดระยะเวลาดังกล่าวแล้วถึงจะทำการเปลี่ยนไปตรวจสอบช่องสัญญาณในลำดับถัดไป



ภาพที่ 15 แผนภาพขั้นตอนการทำงานของอุปกรณ์รบกวนสัญญาณ

3. การทดลอง

ในการทดลองระบบของงานวิจัยนี้ ใช้การทดสอบกับระบบเครือข่ายจริง ดังรายละเอียดต่อไปนี้

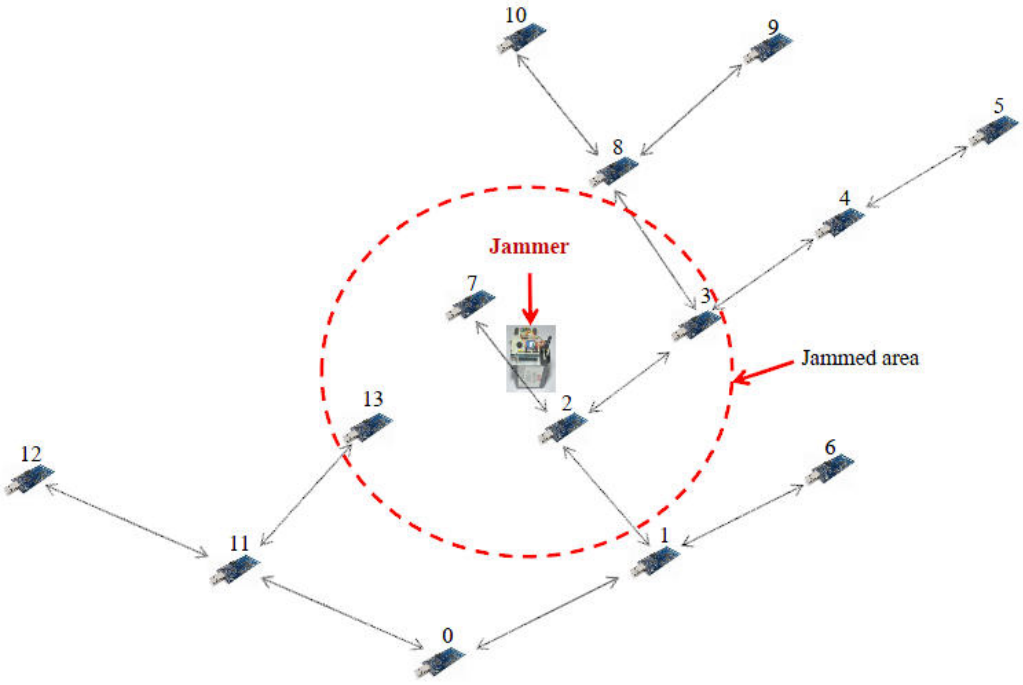
3.1 การติดตั้งระบบทดสอบ

ในระบบเครือข่ายตัวรับรู้ไร้สายในงานวิจัย โหนดตัวรับรู้ทุกตัวจะทำงานบนมาตรฐาน IEEE 802.15.4 ย่าน 2.4 GHz (ความถี่ 2400-2483.5 MHz) ที่มี 16 ช่องสัญญาณ (ช่องสัญญาณที่ 11-26) ซึ่งระบบปฏิบัติการบนโหนดจะเป็น TinyOS เวอร์ชัน 2.1.1 โดยคุณสมบัติต่างๆ ของโหนดในการติดตั้งระบบทดสอบแสดงรายละเอียดไว้ตามตารางที่ 2

ตารางที่ 2 คุณสมบัติของโหนดในการติดตั้งระบบทดสอบ

Parameters	Value
ลักษณะการส่งสัญญาณ	
- การส่งข้อมูล	Unicast
- ความเร็วการส่ง	250 kpbs
- กำลังส่ง	-5 dBm
ลักษณะข้อมูล	
- ขนาดแพ็กเกตข้อมูล	20 Byte
- ขนาดหน่วยความจำ	600 Byte
ลักษณะการเชื่อมต่อ	
- การหาเส้นทาง	Static route
- Topology	Cluster tree
ลักษณะการวางโหนด	
- ระยะห่าง	5 เมตร
- พื้นที่	Line of sight
จำนวนครั้งของการทดลอง	5 ครั้ง

ในการศึกษาถึงประสิทธิภาพของวิธีการที่นำเสนอ ได้แบ่งการทดลองออกเป็น 2 ส่วน คือ การทดลองเครือข่ายแบบเต็มระบบ และการทดลองเครือข่ายแบบย่อย โดยในการทดลองเครือข่ายแบบเต็มระบบจะเป็นการศึกษาถึงประสิทธิภาพการทำงานของวิธีการที่นำเสนอในภาพรวมทั้งหมด ทั้งในส่วนของการโจมตีบริเวณใจกลางของเครือข่าย และการโจมตีบริเวณขอบของเครือข่าย และเนื่องจากตัวอุปกรณ์รบกวนสัญญาณที่ใช้ในการทดลองมีกำลังส่งที่ไม่มากประมาณ 0 dBm จึงต้องทำการลดกำลังส่งของ Tmote Sky แต่ละตัวลงให้เหลือเพียงประมาณ -5 dBm เพื่อไม่ให้โหนดสามารถสื่อสารข้อมูลกันได้หากเกิดการโจมตีขึ้น และเพื่อให้โหนดสามารถสื่อสารข้อมูลกันได้อย่างมีประสิทธิภาพในสภาวะที่ไม่มีการโจมตีหรือเมื่อมีการทำงานตามกระบวนการเปลี่ยนช่องสัญญาณ โดยในการทดลองไม่ได้วางโหนดให้อยู่ห่างไกลกันมากนัก เนื่องจากข้อจำกัดเรื่องของกำลังส่งที่มีน้อย โดยให้โหนดแต่ละตัวอยู่ห่างกันประมาณ 5 เมตร ดังแสดงตามภาพที่ 16 และเพื่อให้เห็นภาพการวางตำแหน่งอุปกรณ์ที่ชัดเจนขึ้นจึงได้สร้างภาพแบบจำลองระบบเครือข่ายขึ้น มา ดังแสดงในภาพที่ 16 (ก) ซึ่งสามารถใช้เทียบกับการวางอุปกรณ์ในระบบเครือข่ายจริงในการทดลองดังแสดงตามภาพที่ 16 (ข) ได้



(ก) แบบจำลองระบบเครือข่าย

ภาพที่ 16 เครือข่ายแบบเต็มระบบในการทดลอง

(ข) การวางตำแหน่งอุปกรณ์ในระบบเครือข่ายจริง

ภาพที่ 16 (ต่อ)

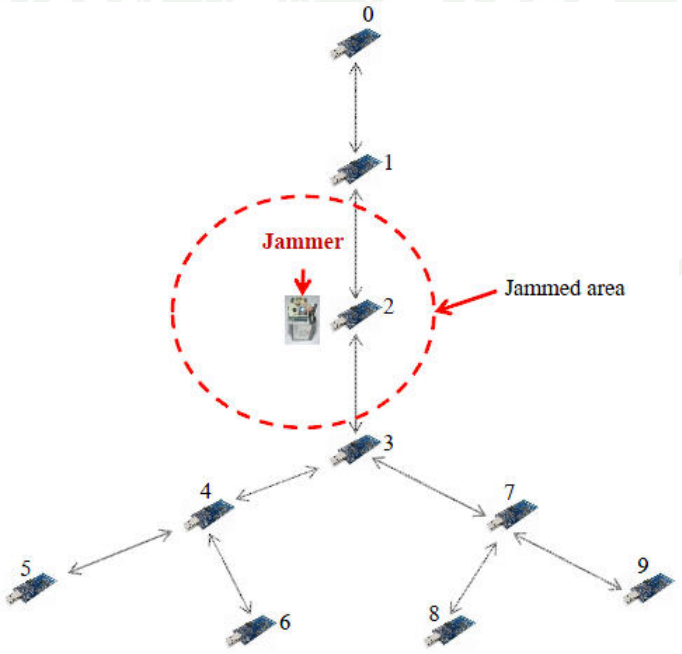
โดยในการทดลองเครือข่ายแบบเต็มระบบมีคุณสมบัติต่างๆ ของโหนดเพิ่มเติม ในการติดตั้งระบบทดสอบดังแสดงรายละเอียดไว้ตามตารางที่ 3

ตารางที่ 3 คุณสมบัติของโหนดในเครือข่ายแบบเต็มระบบ

Parameters	Value
Tmote sky	14 โหนด
Jammer	Reactive 16 ช่องสัญญาณ
Packet Inter-arrival time	5, 10, 15, 20 และ 25 วินาที
Jammer เริ่มทำงาน	10 นาที
ระยะเวลาการตรวจสอบช่องสัญญาณ	1 นาที
ระยะเวลาการโจมตี	5 นาที
ระยะเวลาการทดลองเก็บผล	3 ชั่วโมง

ในการทดลองด้วยช่วงเวลาของการส่งแพ็กเกตข้อมูลที่แตกต่างกัน คือ 5 10 15 20 และ 25 วินาที ตามลำดับ หากช่วงเวลาระหว่างแพ็กเกตข้อมูลยิ่งสั้น การรับส่งข้อมูลจะมีปริมาณมาก แต่หากช่วงเวลาระหว่างแพ็กเกตข้อมูลยิ่งนาน การรับส่งข้อมูลจะมีปริมาณที่น้อยเมื่อสิ้นสุดระยะเวลาของการทดลองเก็บผล

เนื่องจากในการพิจารณาประสิทธิภาพการทำงานของวิธีการ JAWSN ในส่วนของการทำงานที่มีการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณของ Boundary node นั้น หากพิจารณาเครือข่ายแบบเต็มระบบดังที่กล่าวมาข้างต้น อาจทำให้ไม่เห็นผลที่ชัดเจนมากนัก เนื่องจากการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณของ Boundary node จะมีประสิทธิภาพสูงสุดก็ต่อ เมื่อเกิดการโจมตีบริเวณใจกลางเครือข่าย แต่จากระบบเครือข่ายข้างต้นนั้น มีมากกว่าหนึ่งเส้นทางที่มายังสถานีฐาน โดยบางเส้นทางมีการถูกโจมตีเฉพาะบริเวณขอบเครือข่าย ซึ่งการประสานจังหวะเวลาของการเปลี่ยนช่องสัญญาณไม่ได้มีผลต่อการถูกโจมตีแบบนี้ ดังนั้นเพื่อให้เห็นถึงประสิทธิภาพการทำงานของวิธีการ JAWSN ที่ชัดเจนขึ้นจึงได้ทำการติดตั้งระบบทดสอบแบบย่อยเพิ่มเติม โดยจะเป็นระบบทดสอบที่มีเส้นทางมายังสถานีฐานเพียงเส้นทางเดียว และมีการโจมตีเฉพาะที่บริเวณใจกลางเครือข่าย โดยโหนดภายใต้พื้นที่การโจมตีจะมีเฉพาะโหนด 2 เท่านั้น และมี Boundary node เพียง 2 โหนด คือ โหนด 1 และโหนด 3 ดังแสดงตามภาพที่ 17



ภาพที่ 17 เครือข่ายแบบย่อยในการทดลอง

โดยในการทดลองเครือข่ายแบบย่อยมีคุณสมบัติต่างๆ ของโหนดเพิ่มเติม ในการติดตั้งระบบทดสอบดังแสดงรายละเอียดไว้ตามตารางที่ 4

ตารางที่ 4 คุณสมบัติของโหนดในเครือข่ายแบบย่อย

Parameters	Value
Tmote sky	10 โหนด
Jammer	Reactive 2 ช่องสัญญาณ
Packet Inter-arrival time	15 วินาที
Jammer เริ่มทำงาน	10 นาที
ระยะเวลาการตรวจสอบช่องสัญญาณ	1 นาที
ระยะเวลาการโจมตี	1 ชั่วโมง
ระยะเวลาการทดลองเก็บผล	1.30 ชั่วโมง

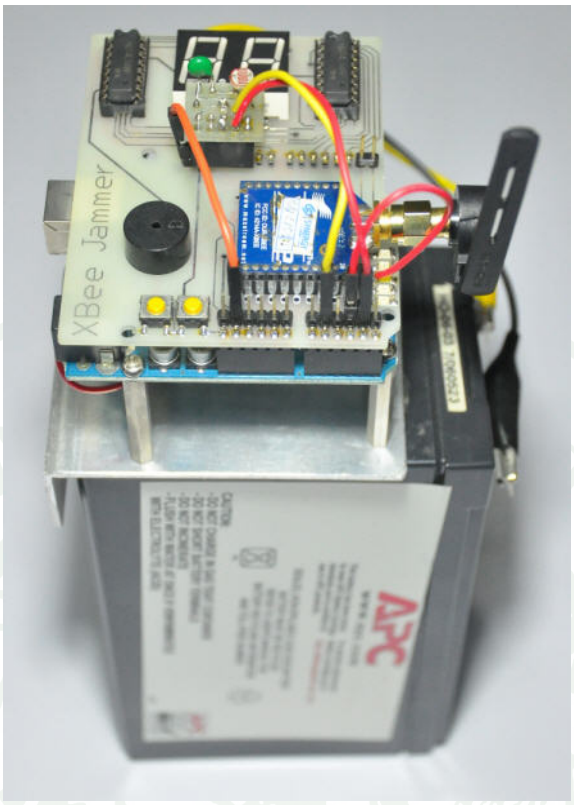
ในการทดลองระบบเครือข่ายย่อยนี้จะเน้นพิจารณาเฉพาะช่วงเวลาที่โหนดถูกโจมตี ดังนั้นจึงเลือกใช้ช่วงเวลาของการส่งแพ็กเกตข้อมูลเพียงค่าเดียว คือ ที่ 15 วินาที เนื่องจากเป็นค่าที่อยู่กึ่งกลางระหว่างช่วงเวลาของการส่งแพ็กเกตข้อมูลที่ใช้ในการทดลองทั้งหมด และในการทดลองจะทำการโจมตีช่องสัญญาณด้วยระยะเวลาที่นานกว่าการทดลองเครือข่ายแบบเต็มระบบ คือ ประมาณ 1 ชั่วโมง จึงทำการเปลี่ยนไปโจมตีบนช่องสัญญาณใหม่ ซึ่งจะทำให้สามารถศึกษาถึงประสิทธิภาพในส่วนของการทำงานที่มีการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณของ Boundary node ได้อย่างชัดเจนมากขึ้น

การทดลองระบบเครือข่ายในงานวิจัยนอกจากแพ็กเกตข้อมูลที่ใช้รับส่งข้อมูลระหว่างโหนดแล้ว ยังมีในส่วนของแพ็กเกตควบคุมต่างๆ ที่ช่วยให้กระบวนการทำงานสามารถดำเนินไปได้ ซึ่งแพ็กเกตควบคุมมีทั้งหมด 7 ประเภท แต่ละประเภทก็มีหน้าที่การทำงานแตกต่างกันไป โดยในงานวิจัยที่นำเสนอกับงานวิจัยเดิมมีการใช้แพ็กเกตควบคุมที่ไม่เท่ากัน ซึ่งวิธีการที่นำเสนอมีการใช้แพ็กเกตควบคุมที่มากกว่าอยู่ 2 ประเภท คือ Time packet และ Channel packet ดังแสดงรายละเอียดตามตารางที่ 5

ตารางที่ 5 แพ็กเกตควบคุมในการทดลอง

ประเภทแพ็กเกต	หน้าที่	JAWSN	Wenyuan
Link packet	ตรวจสอบปริมาณ LQI	X	X
Alarm packet	เตือนการเป็น Boundary ไปยัง parent	X	X
Check packet	ตรวจสอบ Link ก่อนส่ง Data packet	X	X
Neighbor packet	ตรวจสอบ Neighbor	X	X
Start packet	สั่งให้ระบบเครือข่ายเริ่มทำงาน	X	X
Time packet	Boundary synchronization	X	
Channel packet	ปรับปรุงลำดับช่องสัญญาณ	X	

การโจมตีโหนดตัวรับรู้ในเครือข่ายจะใช้การโปรแกรมไมโครคอนโทรลเลอร์ AVR บนบอร์ด Arduino Uno เพื่อควบคุมโมดูล XBee Series 1 รุ่น 4214A-XBEE ของบริษัท MaxStream ให้ทำงานเป็นอุปกรณ์รบกวนสัญญาณแบบ reactive ดังแสดงตามภาพที่ 18 ซึ่งส่วนประกอบต่างๆ ทางด้านฮาร์ดแวร์จะแสดงไว้ท้ายเล่มในส่วนของภาคผนวก และเพื่อไม่ให้โมดูล XBee หยุดรอเวลาเมื่อมีโหนดอื่นใช้งานช่องสัญญาณตามกลไก IEEE 802.15.4 จึงทำการปรับค่า Clear Channel Assessment (CCA) ให้มีค่าต่ำสุด ทำให้ความสามารถในการจับสัญญาณว่ามีอุปกรณ์อื่นส่งสัญญาณอยู่ลดน้อยลง และในการตรวจสอบการใช้งานช่องสัญญาณของโหนดอื่น จะทำการพิจารณาจากค่าความแรงของสัญญาณ (Received Signal Strength Indication: RSSI)



ภาพที่ 18 อุปกรณ์รบกวนสัญญาณ

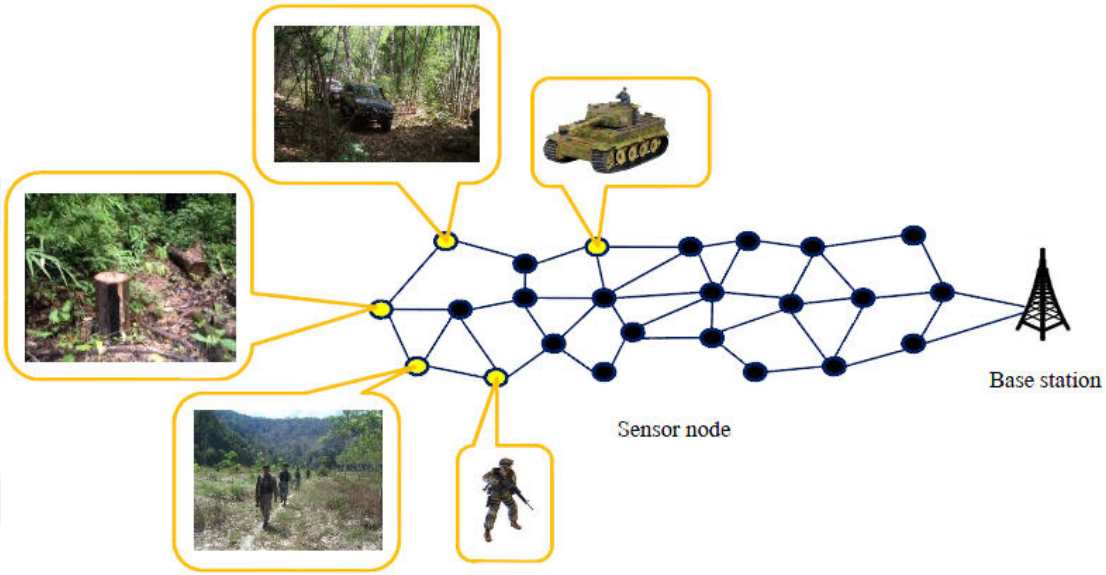
ในการพิจารณาประสิทธิภาพการทำงานในส่วนของการเลือกใช้งานช่องสัญญาณได้ทั้ง 16 ช่องสัญญาณตามมาตรฐาน IEEE 802.15.4 ย่าน 2.4 GHz ของวิธีการ JAWSN นั้น ไม่ได้ทำการทดลองเปรียบเทียบให้เห็นผลที่ชัดเจนกับวิธีการเดิม แต่สามารถทำการวิเคราะห์ประสิทธิภาพการทำงานจากการทดลองที่ผ่านมาข้างต้นได้ ซึ่งจะได้กล่าวไว้ในส่วนของการวิจารณ์ผล

3.2 ชุดคำสั่ง

ในการทดสอบขั้นตอนวิธีที่นำเสนอจะทำผ่านระบบเครือข่ายจริง โดยทำการโปรแกรมตัว Tmote sky ผ่านระบบปฏิบัติการ TinyOS รุ่น 2.1.1 ด้วยภาษา NesC ให้ทำงานเป็นระบบเครือข่ายตัวรับรู้ไร้สาย และให้สามารถหลบหลีกการรบกวนเมื่อเกิดการโจมตีจากอุปกรณ์รบกวนสัญญาณ และเพื่อให้ง่ายต่อการคัดแยกและเก็บข้อมูลที่ต้องการที่ส่งมาจากโหนด จึงสร้างโปรแกรมภาษาจาวาให้ทำงานร่วมด้วย ซึ่งโปรแกรมดังกล่าวจะใช้ในการเก็บรวบรวมข้อมูลเท่านั้น ไม่ได้ทำงานในส่วนของขั้นตอนวิธีที่นำเสนอ

3.3 การประเมินผล

ในการประเมินวิธีการที่นำเสนอจะขอยกตัวอย่างเหตุการณ์ที่อาจจะเกิดการโจมตีจากอุปกรณ์รบกวนสัญญาณขึ้น โดยส่วนใหญ่จะเกี่ยวข้องกับงานทางด้านความมั่นคงปลอดภัยต่างๆ โดยเฉพาะการวางโหนดไว้ตามแนวชายแดนเพื่อติดตามการเคลื่อนไหวของกลุ่มคนที่กระทำผิดกฎหมาย ทั้งการลักลอบขนยาเสพย์ติด การตัดไม้ทำลายป่า การเคลื่อนย้ายกำลังพลและยุทโธปกรณ์ต่างๆ เป็นต้น ดังแสดงตามภาพที่ 19



ภาพที่ 19 สถานการณ์ที่จะเกิดการโจมตีจากอุปกรณ์รบกวนสัญญาณ

ในการประเมินผลจะพิจารณาจากโหนดทั้งหมดบนเส้นทางที่เชื่อมต่อมายังสถานีฐาน เนื่องจากเป็นการทดสอบกับระบบเครือข่ายจริงทำให้จำนวนโหนดที่ใช้ในการทดลองมีอยู่ค่อนข้างจำกัด ดังนั้นเมื่อเกิดการโจมตีขึ้นจึงมีผลกระทบกับโหนดทั้งหมดที่อยู่บนเส้นทาง ซึ่งในการทดลองสามารถแยกพิจารณาผลได้ 3 ลักษณะ คือ ผลจากการโจมตีที่เกิดขึ้นบริเวณขอบของเครือข่าย ผลจากการโจมตีที่เกิดขึ้นบริเวณใจกลางเครือข่าย และผลรวมจากการโจมตีทั้งหมด โดยตัวชี้วัดประสิทธิภาพการทำงานจะประกอบด้วย 2 ตัวชี้วัด ได้แก่

- ปริมาณข้อมูลที่รับส่งได้ (PDR) เป็นจำนวนแพ็กเกตข้อมูลทั้งหมดที่ส่งออกไปจากโหนดทุกตัวในระบบเทียบกับจำนวนแพ็กเกตข้อมูลทั้งหมดที่รับได้ ณ สถานีฐาน โดยจะพิจารณาตามสมการที่ 3

$$\text{PDR (\%)} = \frac{\text{Total received data packet}}{\text{Total sended data packet}} \text{ x } 100 \qquad (3)$$

- ปริมาณโอเวอร์เฮด เป็นจำนวนแพ็กเกตควบคุมทั้งหมดที่ส่งออกไป เพื่อที่จะทำให้สามารถกู้คืนระบบการสื่อสารของเครือข่ายขึ้นมาใหม่ได้ โดยคิดออกมาเป็นสัดส่วนของจำนวนแพ็กเกตควบคุมทั้งหมดที่ส่งออกไปเทียบกับจำนวนแพ็กเกตข้อมูลทั้งหมดที่รับได้โดยไม่ซ้ำของเดิม ซึ่งพิจารณาได้ตามสมการที่ 4

$$\text{Overhead (packet)} = \frac{\text{Total sended control packet}}{\text{Total received data packet}} \qquad (4)$$

โดยทั้ง 2 ตัวชี้วัดจะพิจารณาเปรียบเทียบกับวิธีการเปลี่ยนช่องสัญญาณแบบ spectral multiplexing ที่มีอยู่เดิมในงานวิจัยของ Wenyuan *et al*. (2006, 2007)

ผลและวิจารณ์

ผล

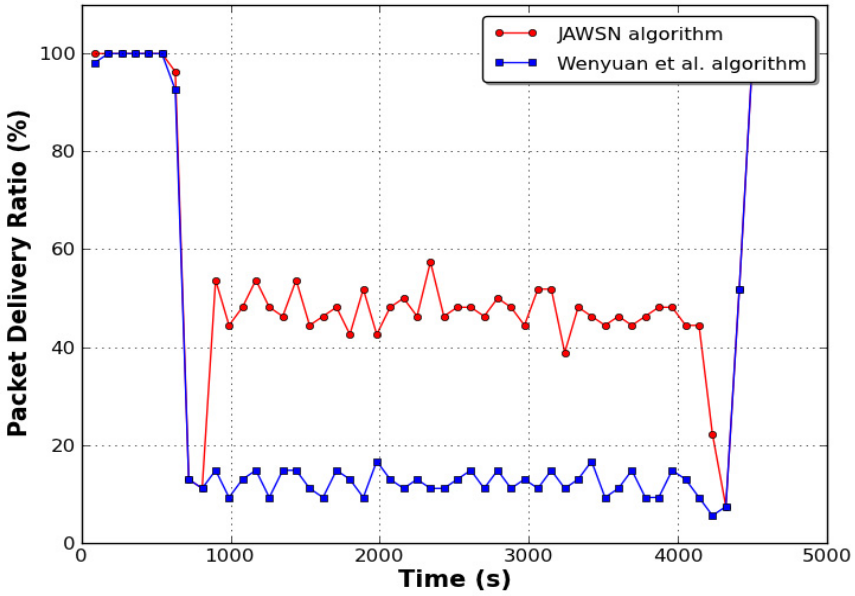
ผลการทดลองจะทำการแยกตามตัวชี้วัด ได้แก่ ปริมาณข้อมูลที่รับส่งได้ (PDR) และปริมาณโอเวอร์เฮด โดยลำดับการเสนอจะเริ่มต้นจากการเปรียบเทียบปริมาณข้อมูลที่รับส่งได้ ต่อมาจะทำการเปรียบเทียบปริมาณโอเวอร์เฮด โดยทั้ง 2 ตัวชี้วัดจะเป็นการเปรียบเทียบระหว่างวิธีการ JAWSN กับวิธีการ spectral multiplexing เดิมในงานวิจัยของ Wenyuan *et al*. (2006, 2007) โดยในการนำเสนอผลการทดลองจะแยกพิจารณาเป็น 2 กรณี คือ การทดลองระบบเครือข่ายแบบย่อย และการทดลองระบบเครือข่ายแบบเต็มระบบ ดังรายละเอียดดังต่อไปนี้

1. ผลการทดลองระบบเครือข่ายแบบย่อย

1.1 เปรียบเทียบปริมาณข้อมูลที่รับส่งได้ (PDR)

ผลการทดลองแสดงด้วยกราฟตามเวลาจริง (Real time) โดยจะเป็นการประมาณการปริมาณแพ็กเกตข้อมูลที่จะได้รับ ณ สถานีฐาน เมื่อเทียบกับเวลาการทำงานของทั้งระบบ เนื่องจากการโจมตีจากอุปกรณ์รบกวนสัญญาณที่เกิดขึ้นทำให้โหนดที่ได้รับผลกระทบ โดยเฉพาะโหนดที่อยู่ภายใต้พื้นที่การโจมตีและหลังพื้นที่การโจมตีไม่สามารถส่งข้อมูลมายังสถานีฐานตามกำนดเวลาได้ ดังนั้นจึงต้องมีการประมาณการปริมาณแพ็กเกตข้อมูลที่จะได้รับเข้ามา ซึ่งแกน Y จะแสดงถึงปริมาณข้อมูลที่รับส่งได้ (PDR) และแกน X เป็นระยะเวลาการทำงานของเครือข่าย ดังแสดงตามภาพที่ 20

จากการทดลองปริมาณข้อมูลที่รับส่งได้เมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN จะให้ค่าเฉลี่ยประมาณ 53.99% และวิธีการแบบเดิมจะให้ค่าเฉลี่ยประมาณ 28.15%



ภาพที่ 20 ความสัมพันธ์ระหว่างค่า PDR กับระยะเวลาการทำงานของเครือข่าย

1.2 เปรียบเทียบปริมาณโอเวอร์เฮด

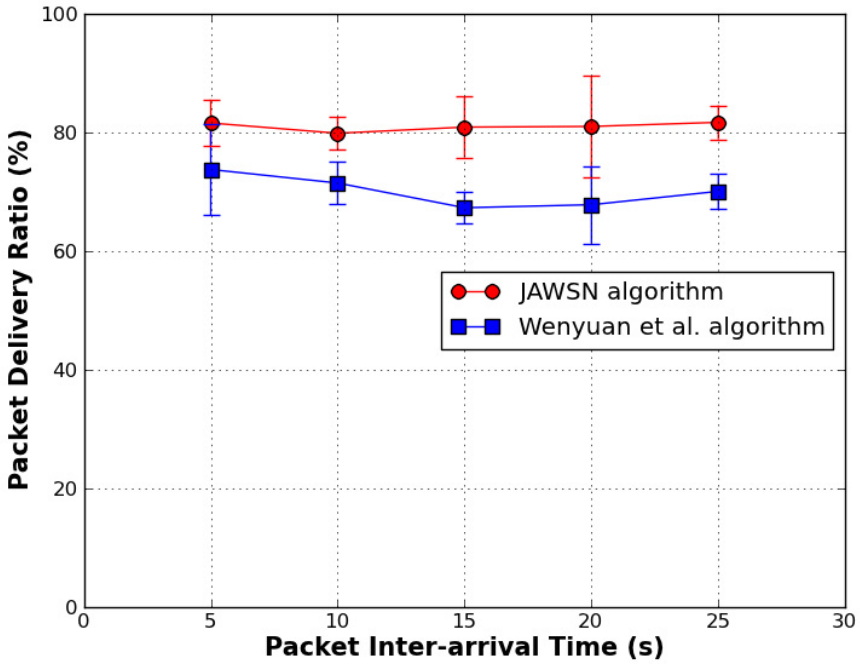
จากการทดลองระบบเครือข่ายแบบย่อยเพื่อพิจารณาถึงปริมาณโอเวอร์เฮดที่เกิดขึ้นกับโหนดทั้งหมดบนเครือข่าย ไม่สามารถนำมาแสดงในรูปแบบของกราฟตามเวลาจริงได้ เนื่องจากการโจมตีจากอุปกรณ์รบกวนสัญญาณที่เกิดขึ้น และปริมาณโอเวอร์นั้น ไม่สามารถที่จะใช้การประมาณการเหมือนกับการหาค่า PDR ที่แต่ละโหนดมีช่วงเวลาของการส่งแพ็กเกตข้อมูลที่ไม่แตกต่างกันมากนัก แต่ในส่วนของปริมาณโอเวอร์เฮดในแต่ละโหนดนั้นจะมีปริมาณที่ค่อนข้างแตกต่างกันมาก ดังนั้นปริมาณโอเวอร์เฮดที่เกิดขึ้นทั้งหมดจึงต้องรอให้สิ้นสุดระยะเวลาของการเก็บข้อมูล ซึ่งโหนดทั้งหมดจะเปลี่ยนกลับมาใช้งานช่องสัญญาณเดียวกันและสื่อสารกันตามปกติจึงจะสามารถเก็บข้อมูลได้ โดยเมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN มีปริมาณโอเวอร์เฮดในสัดส่วน 56.41 แพ็กเกต และวิธีการเดิมมีปริมาณโอเวอร์เฮดในสัดส่วน 81.06 แพ็กเกต

2. ผลการทดลองระบบเครือข่ายแบบเต็มระบบ

2.1 เปรียบเทียบปริมาณข้อมูลที่รับส่งได้ (PDR)

ผลการทดลองแสดงด้วยกราฟ โดยแกน Y จะแสดงถึงปริมาณข้อมูลที่รับส่งได้ (PDR) และแกน X เป็นช่วงเวลาของการส่งแพ็กเกตข้อมูล (Packet Inter-arrival Time) ซึ่งการพิจารณาผลในแต่ละช่วงเวลาของการส่งแพ็กเกตข้อมูล เพื่อดูช่วงของความเชื่อมั่น (Confident interval) จะใช้ระดับความเชื่อมั่น (Confident level) ที่ 95% ซึ่งในการทดลองเครือข่ายแบบเต็มระบบ จะแยกพิจารณาผลของปริมาณข้อมูลที่รับส่งได้เป็น 3 กรณี คือ ผลจากการโจมตีบริเวณขอบของเครือข่าย ผลจากการโจมตีบริเวณใจกลางเครือข่าย และผลรวมของการโจมตีทั้งหมด

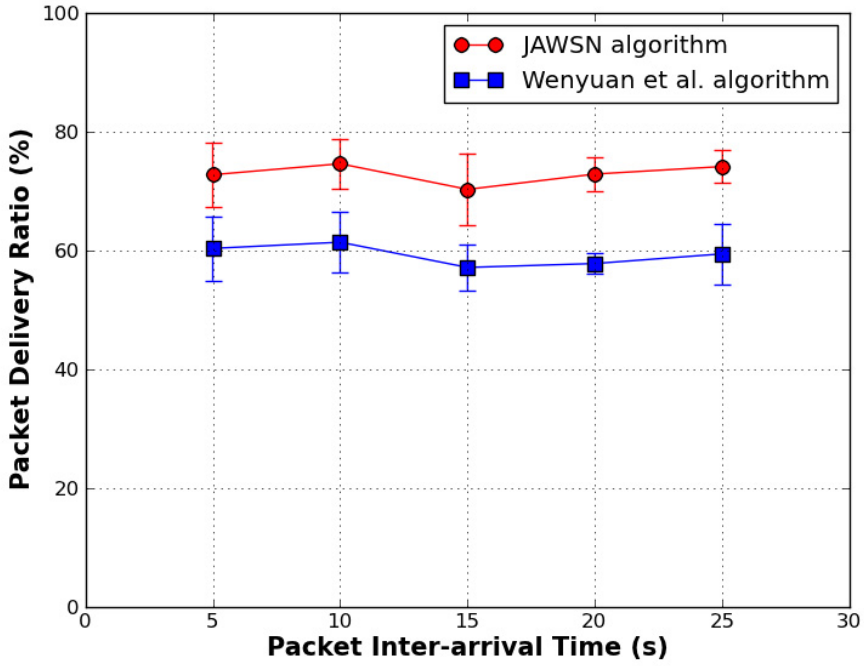
- ผลจากการโจมตีบริเวณขอบของเครือข่าย แสดงได้ตามภาพที่ 21



ภาพที่ 21 ความสัมพันธ์ระหว่างค่า PDR กับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล เมื่อพิจารณาผลจากการโจมตีบริเวณขอบของเครือข่าย

จากการโจมตีบริเวณขอบของเครือข่าย ผลของปริมาณข้อมูลที่รับส่งได้เมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN ให้ค่า PDR เฉลี่ยประมาณ 80.97% ส่วนวิธีการของ Wenyuan ให้ค่า PDR เฉลี่ยประมาณ 70.05%

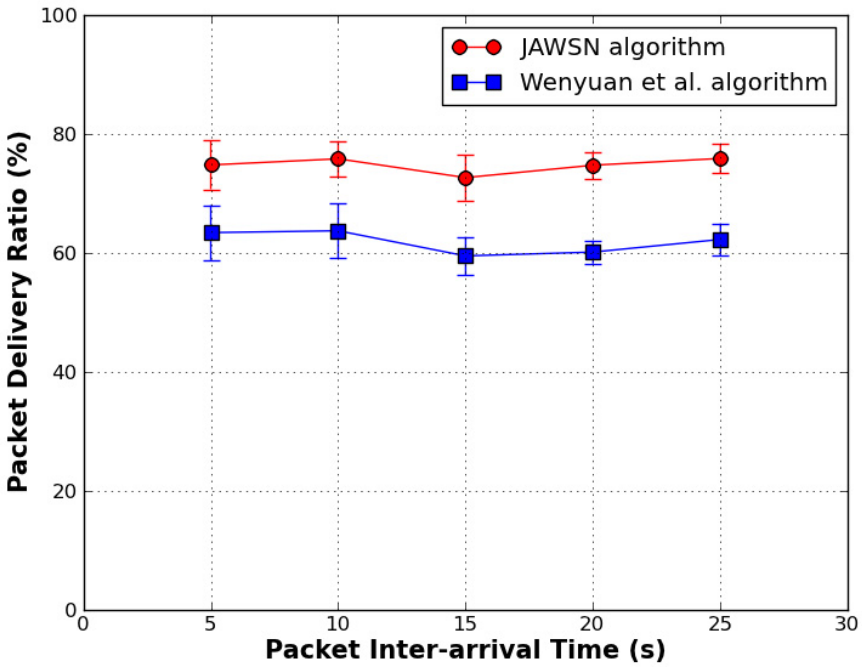
- ผลจากการโจมตีบริเวณใจกลางเครือข่าย แสดงได้ตามภาพที่ 22



ภาพที่ 22 ความสัมพันธ์ระหว่างค่า PDR กับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล เมื่อพิจารณาผลจากการโจมตีบริเวณใจกลางเครือข่าย

จากการโจมตีบริเวณใจกลางเครือข่าย ผลของปริมาณข้อมูลที่รับส่งได้เมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN ให้ค่า PDR เฉลี่ยประมาณ 72.89% ส่วนวิธีการของ Wenyuan ให้ค่า PDR เฉลี่ยประมาณ 59.19%

- ผลรวมจากการโจมตีทั้งหมด แสดงได้ตามภาพที่ 23



ภาพที่ 23 ความสัมพันธ์ระหว่างค่า PDR กับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล เมื่อพิจารณาผลรวมจากการโจมตีทั้งหมด

จากผลรวมของการโจมตีทั้งหมด ปริมาณข้อมูลที่รับส่งได้เมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN ให้ค่า PDR เฉลี่ยประมาณ 74.74% ส่วนวิธีการของ Wenyuan ให้ค่า PDR เฉลี่ยประมาณ 61.77%

2.2 เปรียบเทียบปริมาณโอเวอร์เฮด

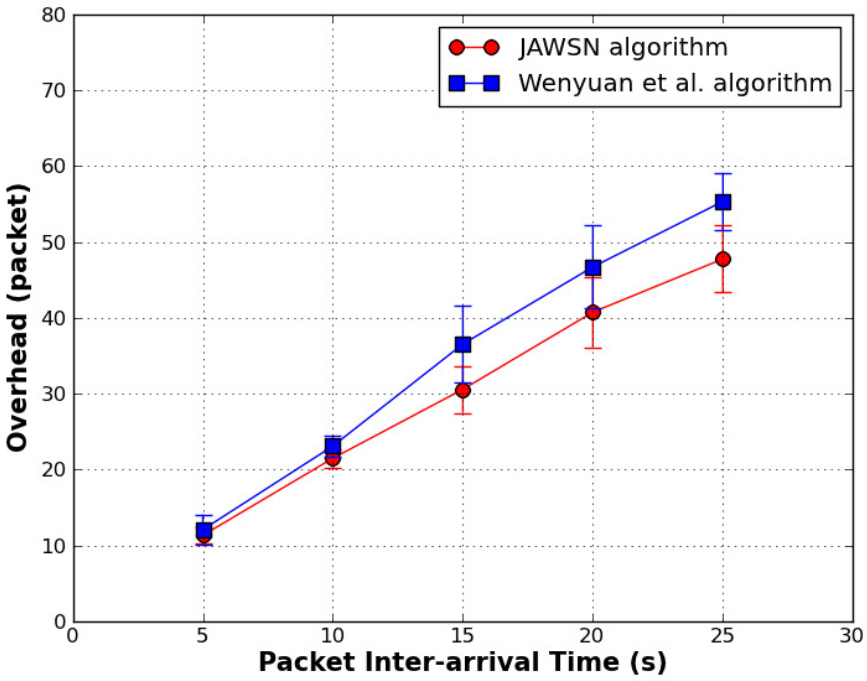
ผลการทดลองแสดงด้วยตารางและกราฟ โดยในส่วนของตารางจะเป็นค่าเฉลี่ยของปริมาณแพ็กเกตควบคุมที่ส่งออกไปทั้งหมด โดยการทดลองเครือข่ายแบบเต็มระบบจะแยกพิจารณาผลเป็น 3 กรณี เช่นเดียวกับการพิจารณาในส่วนของค่า PDR ดังแสดงตามตารางที่ 6

ตารางที่ 6 แพ็กเกตควบคุมที่ส่งออกทั้งหมดเมื่อสิ้นสุดระยะเวลาการเก็บข้อมูล

ลักษณะการเก็บข้อมูล	JAWSN	Wenyuan	ผลต่าง
การโจมตีบริเวณขอบของเครือข่าย	42,675 packet	41,387 packet	1,288 packet
การโจมตีบริเวณใจกลางเครือข่าย	135,775 packet	124,454 packet	11,321 packet
ผลรวมการโจมตีทั้งหมด	178,450 packet	165,842 packet	12,608 packet

ในส่วนของกราฟจะเป็นความสัมพันธ์ระหว่างปริมาณโอเวอร์เฮดกับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล (Packet Inter-arrival Time) ซึ่งแกน Y จะแสดงถึงปริมาณโอเวอร์เฮด และแกน X เป็นช่วงเวลาของการส่งแพ็กเกตข้อมูล และในการพิจารณาผลในแต่ละช่วงเวลาของการส่งแพ็กเกตข้อมูล เพื่อดูช่วงของความเชื่อมั่นจะใช้ระดับความเชื่อมั่นที่ 95% ซึ่งจะแยกพิจารณาผลเป็น 3 กรณี เช่นเดียวกัน

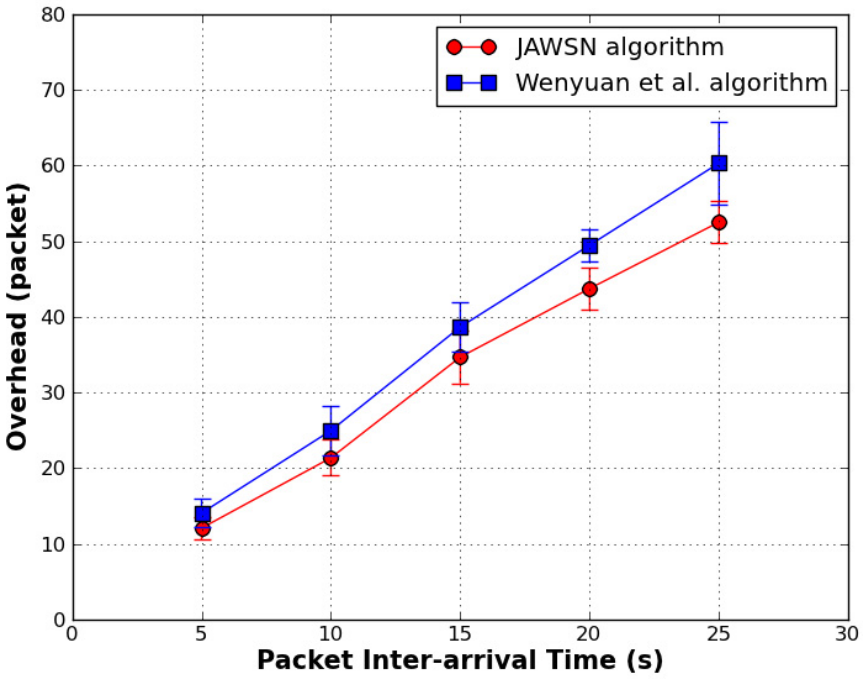
- ผลจากการโจมตีบริเวณขอบของเครือข่าย แสดงได้ตามภาพที่ 24



ภาพที่ 24 ความสัมพันธ์ระหว่างปริมาณโอเวอร์เฮดกับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล เมื่อพิจารณาผลจากการโจมตีบริเวณขอบของเครือข่าย

จากการโจมตีบริเวณขอบของเครือข่าย ปริมาณโอเวอร์เฮดที่เกิดขึ้นเมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN มีปริมาณโอเวอร์ในสัดส่วนโดยเฉลี่ยประมาณ 30.36 แพ็กเกต ส่วนวิธีการของ Wenyuan มีปริมาณโอเวอร์เฮดในสัดส่วนโดยเฉลี่ยประมาณ 34.74 แพ็กเกต

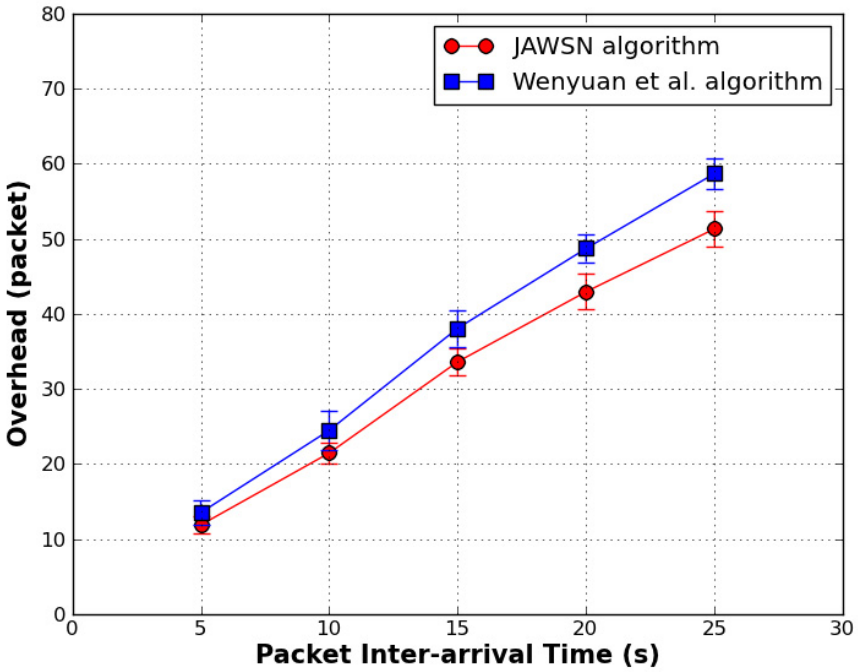
- ผลจากการโจมตีบริเวณใจกลางเครือข่าย แสดงได้ตามภาพที่ 25



ภาพที่ 25 ความสัมพันธ์ระหว่างปริมาณโอเวอร์เฮดกับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล เมื่อพิจารณาผลจากการโจมตีบริเวณใจกลางเครือข่าย

จากการโจมตีบริเวณใจกลางเครือข่าย ปริมาณโอเวอร์เฮดที่เกิดขึ้นเมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN มีปริมาณโอเวอร์ในสัดส่วนโดยเฉลี่ยประมาณ 32.86 แพ็กเกต ส่วนวิธีการของ Wenyuan มีปริมาณโอเวอร์เฮดในสัดส่วนโดยเฉลี่ยประมาณ 37.48 แพ็กเกต

- ผลรวมจากการโจมตีทั้งหมด แสดงได้ตามภาพที่ 26



ภาพที่ 26 ความสัมพันธ์ระหว่างปริมาณโอเวอร์เฮดกับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล เมื่อพิจารณาผลรวมจากการโจมตีทั้งหมด

จากผลรวมของการโจมตีทั้งหมด ปริมาณโอเวอร์เฮดที่เกิดขึ้นเมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูล วิธีการ JAWSN มีปริมาณโอเวอร์ในสัดส่วนโดยเฉลี่ยประมาณ 32.23 แพ็กเกต ส่วนวิธีการของ Wenyuan มีปริมาณโอเวอร์เฮดในสัดส่วนโดยเฉลี่ยประมาณ 36.68 แพ็กเกต

วิจารณ์

ขั้นตอนวิธี JAWSN สามารถเพิ่มปริมาณข้อมูลที่รับส่งได้จากวิธีการแบบเดิม ซึ่งจากการทดลองระบบแบบย่อย ทั้ง 2 วิธีมีความแตกต่างกันอย่างเห็นได้ชัด โดยปริมาณข้อมูลที่รับส่งได้เพิ่มขึ้นจากวิธีการแบบเดิมเฉลี่ยถึง 25.84% และในส่วนของการทดลองแบบเต็มระบบ ปริมาณข้อมูลที่รับส่งได้เพิ่มขึ้นจากวิธีการแบบเดิมเฉลี่ย 12.97%

ในส่วนของปริมาณแพ็กเกตควบคุมที่ส่งทั้งหมด วิธีการ JAWSN มีปริมาณที่มากกว่าเมื่อเทียบกับวิธีการแบบเดิม เนื่องจากในกระบวนการทำงานมีการใช้แพ็กเกตควบคุมที่มากกว่าวิธีการแบบเดิม จึงทำให้เมื่อสิ้นสุดระยะเวลาของการเก็บข้อมูลแพ็กเกตควบคุมทั้งหมดจึงมีจำนวนที่มากกว่า แต่หากนำไปพิจารณาเป็นปริมาณโอเวอร์เฮดที่เกิดขึ้นบนเครือข่าย วีธีการ JAWSN มีสัดส่วนที่น้อยกว่า โดยหากเป็นการทดลองระบบเครือข่ายย่อย ทั้ง 2 วิธีมีความแตกต่างกันมาก โดยวิธีการ JAWSN มีค่าที่ลดลงจากวิธีการแบบเดิมในสัดส่วนถึง 24.65 แพ็กเกต แต่ในส่วนของการทดลองเครือข่ายแบบเต็มระบบ ทั้ง 2 วิธีมีค่าที่ไม่แตกต่างกัน โดยวิธีการ JAWSN มีค่าที่ลดลงจากวิธีการแบบเดิมในสัดส่วนเพียง 4.45 แพ็กเกต ซึ่งข้อสังเกตปลีกย่อยอื่นจะแยกวิเคราะห์ตามตัวชี้วัดดังหัวข้อต่อไปนี้

1. เปรียบเทียบปริมาณข้อมูลที่รับส่งได้ (PDR)

จากกราฟความสัมพันธ์ระหว่างค่า PDR กับระยะเวลาการทำงานของเครือข่ายตามภาพที่ 20 จะเห็นได้ว่าหากเกิดการโจมตีขึ้น วิธีการ JAWSN ที่มีกระบวนการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณของ Boundary node สามารถที่จะทำให้ระบบเครือข่ายสร้างการสื่อสารขึ้นมาใหม่โดยมีปริมาณข้อมูลที่รับส่งได้ถึงประมาณ 50% จาก 100% เนื่องจากการทำงานที่ให้ระยะเวลาในการอยู่บนช่องสัญญาณใหม่และช่องสัญญาณเดิมมีค่าที่เท่ากัน และ Boundary node สามารถเปลี่ยนช่องสัญญาณมารับส่งข้อมูลได้ในเวลาที่ตรงกัน จึงทำให้ข้อมูลที่รับได้มีถึง 50% และสูญเสียไป 50% จากข้อมูลที่มีการส่งทั้งหมด แต่ในส่วนของวิธีการเดิมนั้นมีปริมาณข้อมูลที่รับได้นั้นน้อยมากแต่สูญเสียไปเยอะกว่า เนื่องจากไม่มีกระบวนการประสานจังหวะเวลาในการเปลี่ยนช่องสัญญาณของ Boundary node ทำให้การเปลี่ยนช่องสัญญาณมารับส่งข้อมูลของ Boundary node มีเวลาที่ไม่ตรงกัน ยิ่งโหนดลูกของ Boundary node ที่อยู่หลังพื้นที่การโจมตีมีจำนวนมากข้อมูลที่รับส่งได้จะมีน้อยลง แต่การสูญเสียข้อมูลจะยิ่งมีมากขึ้น

ในส่วนของกราฟความสัมพันธ์ระหว่างค่า PDR กับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล หากมีการเพิ่มช่วงเวลาของการส่งแพ็กเกตข้อมูลขึ้น ค่า PDR ของวิธีการ JAWSN มีปริมาณเฉลี่ยที่มากกว่าวิธีการของ Wenyuan ในทุกๆ ช่วงเวลา แต่หากพิจารณาตามภาพที่ 21 ในส่วนของ Confident interval จะมีบางช่วงเวลาที่ไม่แตกต่างกัน แต่ในภาพที่ 22 และ 23 เมื่อพิจารณาในส่วนของ Confident interval ในทุกๆ ช่วงเวลา ค่า PDR มีความแตกต่างกันอย่างมีนัยสำคัญ

จากกระบวนการทำงานที่มีการประสานจังหวะเวลาของการอยู่บนแต่ละช่องสัญญาณของ Boundary node ทำให้สามารถรับส่งข้อมูลได้ในปริมาณมากและข้อมูลเกิดการสูญเสียน้อย จึงทำให้ค่า PDR ที่ได้มีค่าสูง แต่หากไม่มีกระบวนการทำงานที่มีการประสานจังหวะเวลาของการอยู่บนแต่ละช่องสัญญาณของ Boundary node ตามวิธีการของ Wenyuan จะทำให้จังหวะในการเปลี่ยนช่องสัญญาณเพื่อมารับข้อมูลมีช่วงเวลาที่ไม่ตรงกัน เนื่องจากในส่วนของกระบวนการตรวจสอบการโจมตีเพื่อให้โหนดสามารถเปลี่ยนไปใช้งานช่องสัญญาณใหม่นั้น มีจังหวะของการตรวจรู้ที่ไม่เท่า กันในแต่ละโหนด ดังนั้นช่วงเวลาของการอยู่บนแต่ละช่องสัญญาณจึงไม่เท่ากัน ยิ่งหากช่วงเวลาดังกล่าวแตกต่างกันมากระหว่างตัวรับและตัวส่ง การสูญเสียข้อมูลจะยิ่งมีมาก ส่งผลให้ปริมาณข้อมูลที่ได้มีค่าน้อย

2. เปรียบเทียบปริมาณโอเวอร์เฮด

ในส่วนของการพิจารณาผลของปริมาณโอเวอร์เฮดของการทดลองระบบเครือข่ายแบบย่อย ทั้งในส่วนของวิธีการที่นำเสนอและวิธีการแบบเดิม จะพิจารณาในประเด็นลักษณะเดียวกันกับการพิจารณาผลในส่วนของค่า PDR ดังที่กล่าวมาแล้วก่อนหน้านี้

จากกราฟความสัมพันธ์ระหว่างปริมาณโอเวอร์เฮดกับการเปลี่ยนแปลงช่วงเวลาของการส่งแพ็กเกตข้อมูล ปริมาณโอเวอร์เฮดของทั้ง 2 วิธี มีปริมาณที่ไม่แตกต่างกันนัก และมีสัดส่วนที่เพิ่มขึ้นเรื่อยๆ เหมือนกัน หากช่วงเวลาของการส่งแพ็กเกตข้อมูลเพิ่มขึ้น เนื่องจากช่วงเวลาระหว่างแพ็กเกตยิ่งนานการรับส่งแพ็กเกตข้อมูลจะยิ่งมีจำนวนน้อย แต่ปริมาณของแพ็กเกตควบคุมนั้นยังคงมีค่าเท่าเดิม ทำให้สัดส่วนของแพ็กเกตที่ส่งออกไปมีค่ามากเมื่อเทียบกับแพ็กเกตข้อมูลที่รับได้ แต่อย่างไรก็ตามวิธีการ JAWSN ที่นำเสนอก็ยังคงมีปริมาณเฉลี่ยที่น้อยกว่าวิธีการของ Wenyuan ในทุกๆ ช่วงเวลา

จากการทดลองที่ผ่านมาการจะวัดประสิทธิภาพการทำงานในส่วนของการเลือกใช้งานช่องสัญญาณได้ทั้ง 16 ช่องสัญญาณของวิธีการที่นำเสนอนั้น ไม่สามารถที่จะเปรียบเทียบผลการทดลองให้เห็นได้ชัดเจนนัก เนื่องจากอุปกรณ์รบกวนสัญญาณมีเพียงตัวเดียว โจมตีได้เพียงช่องสัญญาณเดียวในหนึ่งช่วงเวลา จึงทำให้ทั้งวิธีการที่นำเสนอและวิธีการเดิมมีการใช้งานช่องสัญญาณเพียง 2 ช่องสัญญาณเท่านั้นในแต่ละครั้งของการโจมตี แต่ในส่วนของวิธีการที่นำเสนอจะมีทางเลือกในการเลือกใช้ช่องสัญญาณใหม่ที่มากกว่า โดยสามารถเลือกได้ถึง 15 ช่องสัญญาณ แต่วิธีการเดิมสามารถเลือกได้เพียงช่องเดียวเท่านั้น หากจะวัดประสิทธิภาพการทำงานในส่วนนี้จำเป็นต้องมีการใช้อุปกรณ์รบกวนสัญญาณมากกว่า 2 ตัว เพื่อให้สามารถทำการโจมตี 2 ช่องสัญญาณพร้อมกันได้ แต่อย่างไรก็ตามหากเกิดการโจมตีพร้อมกัน 2 ช่องสัญญาณ วิธีการเดิมย่อมไม่สามารถที่จะทำงานได้ เพราะไม่มีทางเลือกในการเลือกใช้ช่องสัญญาณใหม่ที่ไม่ถูกโจมตี ทั้งนี้การที่วิธีการที่นำเสนอจะสามารถทำงานได้ก็จะต้องไม่เกิดการโจมตีพร้อมกันทั้ง 16 ช่องสัญญาณด้วย เพราะจะทำให้ไม่มีทางเลือกในการเปลี่ยนช่องสัญญาณเช่นเดียวกัน โดยหากจะต้องทำการทดลองในลักษณะดังกล่าวจำเป็นจะต้องใช้งบประมาณที่เพิ่มขึ้น รวมทั้งต้องการระยะเวลาในการทำวิจัยที่มากขึ้นตาม ซึ่งไม่เหมาะกับการทดลองกับระบบเครือข่ายจริง อย่างไรก็ตามของงานวิจัยนี้ไม่ได้มุ่งเน้นในประเด็นเรื่องจำนวนช่องสัญญาณ แต่การที่ทำให้วิธีการ JAWSN สามารถใช้งานช่องสัญญาณได้อย่างเต็มประสิทธิภาพไม่ได้จำกัดการใช้งานไว้เพียง 2 ช่องสัญญาณจะทำให้มีแนวโน้มสูงกว่าในการที่จะหลบหลีกการรบกวนได้หากการโจมตีเกิดขึ้นพร้อมกันมากกว่า 2 ช่อง สัญญาณ เพราะมีจำนวนช่องสัญญาณให้เลือกใช้มากกว่า เมื่อเทียบกับวิธีการในแบบเดิม

ในการทดลองงานวิจัยนี้ ไม่ได้ทำการทดลองกับโทโปโลยีหลายๆ ลักษณะ เนื่องจากข้อจำกัดหลายประการในการทดลองด้วยระบบเครือข่ายจริง และด้วยลักษณะการหาเส้นทางที่เป็นแบบ Static route ทำให้โทโปโลยีถูกกำหนดไว้แบบตายตัว โดยหากโทโปโลยีมีการเปลี่ยนไปเป็นแบบอื่นก็อาจมีผลต่อกระบวนการทำงานของระบบ เนื่องจากกระบวนการตรวจสอบการโจมตีมีการพิจารณาจากโหนดเพื่อนบ้านเป็นหลัก ซึ่งอาจยังไม่มีประสิทธิภาพมากนัก ดังนั้นลักษณะของโทโปโลยีจึงมีผลต่อกระบวนการตรวจสอบการโจมตี ซึ่งอาจทำให้เกิดความผิดพลาดได้ อย่างไรก็ตามในงานวิจัยนี้ก็ไม่ได้มุ่งเน้นศึกษาในส่วนของกระบวนการตรวจสอบการโจมตีจากอุปกรณ์รบกวนสัญญาณ แต่เพื่อให้ระบบเครือข่ายสามารถทำงานได้จึงจำเป็นต้องมีการนำกระบวนการดังกล่าวมาใช้ร่วมกับส่วนอื่นที่ได้นำเสนอ

สรุปและข้อเสนอแนะ

สรุป

ในงานวิจัยฉบับนี้ เป็นการนำเสนอวิธีการปรับปรุงการเปลี่ยนช่องสัญญาณแบบ spectral multiplexing เดิม ให้สามารถทำงานได้ดีขึ้นหากเกิดการโจมตีจาก reactive jammer ที่มีการตรวจสอบการใช้งานช่องสัญญาณและสามารถเปลี่ยนช่องสัญญาณในการโจมตีได้ ด้วยการเพิ่มกระบวนการเลือกช่องสัญญาณแบบสุ่มให้สามารถใช้งานช่องสัญญาณได้ครบทั้ง 16 ช่องสัญญาณ และเมื่อเกิดการโจมตีขึ้น โหนดที่อยู่บริเวณขอบของเครือข่ายสามารถประสานจังหวะเวลาของการเปลี่ยนช่องสัญญาณให้มีระยะเวลาที่เท่ากันได้ ทำให้สามารถเพิ่มปริมาณข้อมูลที่รับส่งได้ (PDR) และยังช่วยลดปริมาณโอเวอร์เฮดที่เกิดขึ้น ส่งผลให้เครือข่ายมีความน่าเชื่อถือและยังรับประกันได้ว่าข้อมูลจะส่งไปถึงยังปลายทาง

ข้อเสนอแนะ

ในการทดลองงานวิจัยด้วยระบบเครือข่ายจริงนั้น มีข้อจำกัดอยู่หลายประการ ทั้งในเรื่องของสถานที่ในการทดสอบระบบที่ต้องการพื้นที่ขนาดใหญ่หากเครือข่ายมีโหนดจำนวนมาก และเมื่อโหนดมีจำนวนมากย่อมต้องการแหล่งพลังงานที่มาก และงบประมาณในการทำวิจัยก็ต้องมากขึ้นตาม อีกทั้งในการเปลี่ยนค่าตัวแปรต่างๆ ในแต่ละครั้งของการทดลองก็ต้องการระยะเวลาที่มากขึ้นด้วยเช่นเดียวกัน ทำให้การที่จะทำการทดลองในหลายๆ เหตุการณ์ หรือต้องการทดลองซ้ำให้ได้จำนวนผลลัพธ์หลายๆ ครั้งนั้น จำเป็นต้องใช้ระยะเวลาที่นานมาก ดังนั้นจึงต้องมีระยะเวลาในการทำวิจัยที่นานพอสมควร นอกจากนี้ในขั้นตอนการทำงานของทั้ง 2 วิธี ก็ยังคงต้องการกระบวนการในการตรวจจับการโจมตีที่มีประสิทธิภาพและรวดเร็ว เพื่อช่วยเพิ่มโอกาสในการส่งข้อมูลที่มากขึ้นโดยไม่เสียเวลาในการตรวจสอบการโจมตีมากนัก

ท้ายสุดสำหรับงานในอนาคต หากเครือข่ายมีขนาดใหญ่ โหนดมีจำนวนมาก มีลักษณะการเชื่อมต่อด้วยโทโปโลยีหลายๆ แบบ แล้วเกิดการโจมตีจากอุปกรณ์รบกวนสัญญาณมากกว่า 2 ตัว หรือเกิดขึ้นมากกว่า 2 ช่องสัญญาณพร้อมกัน การที่จะทำให้โหนดสามารถหลบหลีกการรบกวนที่เกิดขึ้นได้นั้นยังต้องมีการค้นคว้าขั้นตอนวิธีที่มีประสิทธิภาพต่อไป

เอกสารและสิ่งอ้างอิง

Aritides, M., D. Gavalas., Ch. Konstantopoulos. and G. Pantziou. 2009. A Survey on Jamming Attacks and Countermeasures in WSNs. **Pourth Quarter.** 11: 42-50.

Kristopher, W.R. and A. Salem. 2009. A Survey on Jamming Avoidance in Ad-Hoc Sensory networks, pp. 93-98. *In* **CCSC.** USA.

Loukas, L., S. Liu. and M. Krunz. 2009. Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks, pp. 169-180. *In* **WiSec'09**. Switzerland.

Sudip, M., S.K. Dhurandher., A. Rayankula. and D. Agrawal. 2009. Using honeynodes for defense against jamming attacks in wireless infrastructure-based networks. **Computers and Electrical Engineering.** in press.

Wenyuan, X., W. Trappe. and Y. Zhang. 2007. Channel Surfing : Defending Wireless Sensor Network from Interence, pp. 499-508. *In* **IPSN'07**. Cambridge, Massachusetts, USA.

Wenyuan, X., W. Trappe. and Y. Zhang. 2006. Poster Abstract: Channel Surfing: Defending Wireless Sensor Networks from Jamming and Interference, pp. 403-404. *In* **SenSys'06**. Boulder, Colorado, USA.

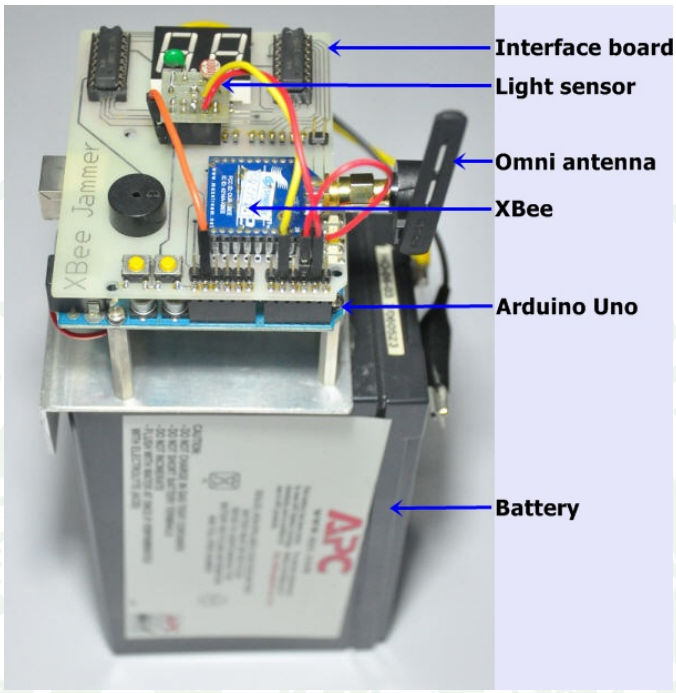
Wenyuan, X., W. Trappe., Y. Zhang. and T.Wood. 2005. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, *In* **MobiHoc'05**. Urbana-Champaign, Illinois, USA.

Wenyuan, X., W. Trappe. and Y. Zhang. 2004. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service, pp. 80-89. *In* **WiSe'04**. Philadelphia, Pennsylvania, USA.

ภาคผนวก

ส่วนประกอบอุปกรณ์รบกวนสัญญาณ

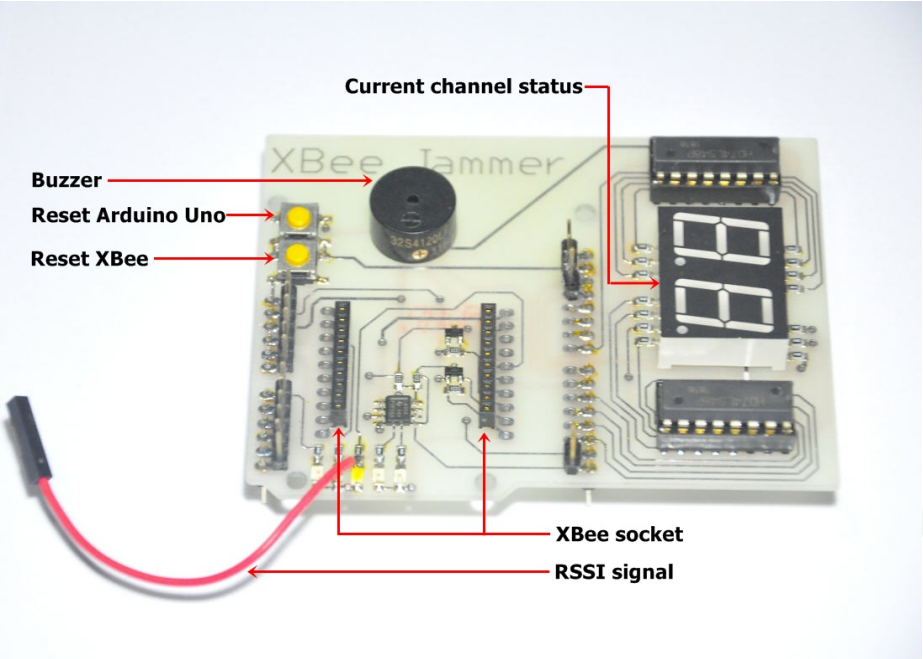
อุปกรณ์รบกวนสัญญาณแบบ reactive ที่ใช้ในงานวิจัย มีส่วนประกอบหลักๆ อยู่ด้วยกัน 6 ส่วน ดังแสดงตามภาพผนวกที่ 1



ภาพผนวกที่ 1 ส่วนประกอบอุปกรณ์รบกวนสัญญาณ

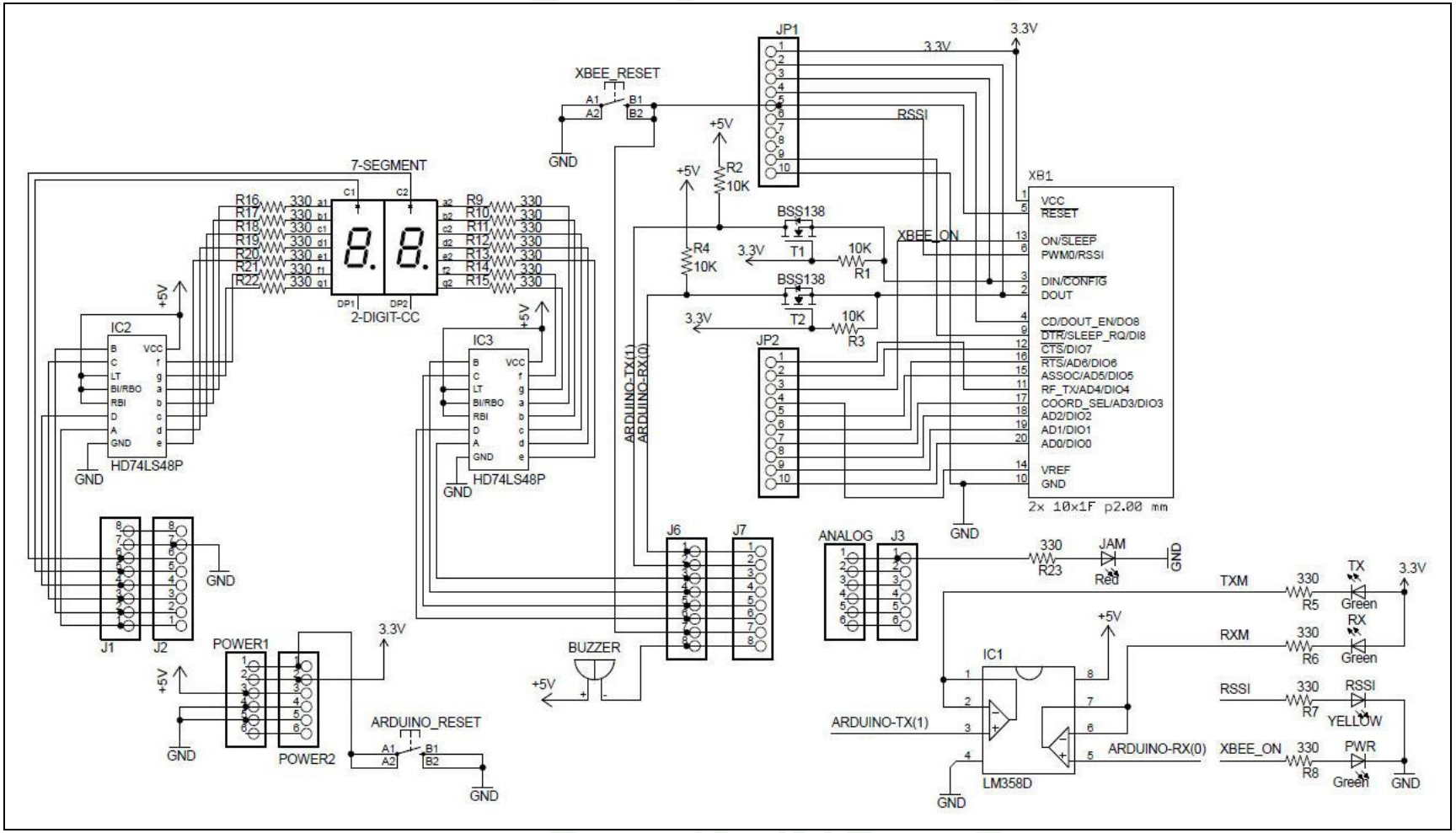
จากภาพผนวกที่ 1 บอร์ดสำหรับเชื่อมต่อ (Interface board) จะเป็นส่วนประกอบหลักที่ใช้สำหรับเชื่อมต่ออุปกรณ์อื่นเข้าด้วยกัน คือ ตัวตรวจวัดแสง (Light sensor) และโมดูล XBee กับ Arduino Uno เพื่อที่ทำให้สามารถทำงานเป็น reactive jammer ได้ โดยจากส่วนประกอบจะเห็นว่ามีการใช้ตัวตรวจวัดแสงร่วมด้วย ซึ่งตัวตรวจวัดแสงนี้จะมีส่วนสำคัญในขั้นตอนการสุ่มช่องสัญญาณของ reactive jammer ในงานวิจัย โดยกระบวนการสุ่มช่องสัญญาณใหม่ด้วย PRG แต่ละครั้ง ช่องสัญญาณเริ่มต้นที่ป้อนให้กับ PRG จะได้มาจากตัวตรวจวัดแสงนี้ จึงทำให้รูปแบบของช่องสัญญาณที่สุ่มได้มีการเปลี่ยนใหม่ในทุกครั้งของการสุ่ม

สำหรับรายละเอียดทางด้านฮาร์ดแวร์ของ Arduino Uno และ XBee จะไม่นำมาอธิบาย เนื่องจากเป็นอุปกรณ์ที่มีขายทั่วไปตามท้องตลาด และรายละเอียดต่างๆ สามารถหาได้ไม่ยาก แต่จะอธิบายเฉพาะส่วนฮาร์ดแวร์ที่ได้ออกแบบขึ้นมาใหม่เพื่อใช้สำหรับงานวิจัยนี้ คือ บอร์ดสำหรับเชื่อมต่อ ซึ่งมีส่วนประกอบหลักต่างๆ ดังแสดงตามภาพผนวกที่ 2



ภาพผนวกที่ 2 ส่วนประกอบของบอร์ดสำหรับเชื่อมต่อ Arduino Uno กับ XBee

บอร์ดสำหรับเชื่อมต่อ Arduino Uno กับ XBee นอกจากจะเป็นบอร์ดที่ใช้ในการเชื่อมต่อในการควบคุม XBee แล้ว ยังสามารถแสดงสถานะต่างๆ ระหว่างการทำงานได้ ทั้งในส่วนของสถานะช่องสัญญาณปัจจุบันที่กำลังใช้งานอยู่ ซึ่งจะแสดงผ่านตัว 7-segment การแสดงสภาวะการณ์ต่างๆ ที่จะแสดงผ่านทางหลอด LED ได้แก่ การรับส่งข้อมูลทางพอร์ตอนุกรม การแสดงสถานะค่า RSSI และสถานะที่มีการโจมตีช่องสัญญาณ นอกจากนี้ยังสามารถที่จะแจ้งเตือนการทำงานต่างๆ ผ่านทางลำโพงขนาดเล็ก (Buzzer) ไม่ว่าจะเป็นการเริ่มกระบวนการสุ่มช่องสัญญาณใหม่ การเปลี่ยนช่องสัญญาณ และเมื่อจะเริ่มทำการโจมตี ซึ่งรายละเอียดต่างๆ ดังที่กล่าวมาสามารถที่จะพิจารณาส่วนประกอบต่างๆ อย่างละเอียดตามวงจรในภาพผนวกที่ 3



ภาพผนวกที่ 3 วงจร Interface board

ประวัติการศึกษาและการทำงาน

ชื่อ	ประธาน สมบูรณ์
เกิดวันที่	25 กรกฎาคม 2528
สถานที่เกิด	อำเภอโซ่พิสัย จังหวัดบึงกาฬ
ประวัติการศึกษา	วศ.บ. (วิศวกรรมอิเล็กทรอนิกส์และโทรคมนาคม) มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
ตำแหน่งปัจจุบัน	วิศวกร
สถานที่ทำงานปัจจุบัน	บริษัท ที-เน็ต จำกัด
ผลงานดีเด่น/หรือรางวัลทางวิชาการ	-
ทุนการศึกษาที่ได้รับ	ได้รับทุนสนับสนุนจาก “สถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย (TGIST) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) สัญญารับทุนเลขที่ TG-44-11-52-061M”