แบบแผน ED THRESHOLD แบบปรับค่าได้สำหรับเครือข่ายเซ็นเซอร์ไร้สาย IEEE 802.15.4 เพื่อรองรับการทำงานร่วมกับเครือข่าย IEEE 802.11B/G

นายวันทวัฒน์ วงศ์มาโนชญ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า ภาควิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2555

ADAPTIVE ED THRESHOLD SCHEME FOR IEEE 802.15.4 WIRELESS SENSOR NETWORKS TO SUPPORT COEXISTENCE WITH IEEE 802.11B/G

Mr.Wantawat Wongmanoch

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering Program in Electrical Engineering

Department of Electrical Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2012

หัวข้อวิทยานิพนธ์	แบบแผน ED THRESHOLD แบบปรับค่าได้สำหรับเครือข่ายเซ็นเซอร์ไร้สาย IEEE 802.15.4 เพื่อรองรับการทำงานร่วมกับเครือข่าย IEEE 802.11B/G
โดย	นายวันทวัฒน์ วงศ์มาโนชญ์
สาขาวิชา	วิศวกรรมไฟฟ้า
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.วาทิต เบญจพลกุล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

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

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.ลัญฉกร วุฒิสิทธิกุลกิจ)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.วาทิต เบญจพลกุล)

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

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.ชัยพร เขมะภาตะพันธ์)

วันทวัฒน์ วงศ์มาโนชญ์ : แบบแผน ED THRESHOLD แบบปรับค่าได้สำหรับเครือข่ายเซ็นเซอร์ไร้สาย IEEE 802.15.4 เพื่อรองรับการทำงานร่วมกับเครือข่าย IEEE 802.11B/G. (ADAPTIVE ED THRESHOLD SCHEME FOR IEEE 802.15.4 WIRELESS SENSOR NETWORKS TO SUPPORT COEXISTENCE WITH IEEE 802.11B/G) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : รศ. ดร.วาทิต เบญจพลกุล, 108 หน้า.

ปัจจุบันเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เริ่มเป็นที่สนใจทั้งในการประยุกต์ใช้งานและการค้นคว้าวิจัย เนื่องจากมีความเรียบง่าย, มีราคาถูก, ใช้พลังงานต่ำ และมีความเชื่อถือได้สูง อย่างไรก็ตาม การที่เครือข่าย IEEE 802.15.4 ทำงานบนแถบความถี่ 2.4 GHz ซึ่งเป็นแถบความถี่สาธารณะ จึงมีเทคโนโลยีอื่นๆที่ทำงานบนแถบความถี่นี้เช่นกัน โดยเฉพาะเครือข่าย IEEE 802.11 b/g ซึ่งมีการใช้งานกันอย่างแพร่หลายถือเป็นเทคโนโลยีที่มีโอกาสส่งผลกระทบต่อเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 มากที่สุด ซึ่งด้วยลักษณะเฉพาะต่างๆของเครือข่าย IEEE 802.11 b/g มีโอกาสทำให้สมรรถนะของเครือข่าย IEEE 802.15.4 ลดลงอย่างมาก และทำให้การประยุกต์ใช้งานที่ใช้เครือข่ายเซ็นเซอร์ไร้สายมีโอกาสทำงานผิดพลาดได้

วิทยานิพนธ์ฉบับนี้เป็นการเสนอวิธีปรับปรุงสมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ในกรณีที่ใช้งานแถบความถี่ร่วมกับเครือข่าย IEEE 802.11b/g เพื่อบรรเทาปัญหาที่เครือข่ายเซ็นเซอร์ไร้สายอาจมีสมรรถนะลดลงหรือทำงานผิดพลาดอันเนื่องมาจากการแทรกสอดระหว่าง 2 มาตรฐานข้างต้น โดยการปรับปรุงรูปแบบการตรวจสอบเพื่อเข้าถึงช่องสัญญาณของโนดส่งในมาตรฐาน IEEE 802.15.4 เพื่อที่โนดส่งในมาตรฐาน IEEE 802.15.4 สามารถส่งแพ็กเกตข้อมูลได้หากระดับพลังงานของสัญญาณแทรกสอดไม่ส่งผลกระทบให้การส่งแพ็กเกตข้อมูลล้มเหลว แต่หากระดับพลังงานของสัญญาณแทรกสอดอาจส่งผลให้การส่งแพ็กเกตข้อมูลล้มเหลว โนดส่งก็จะยังไม่ส่งแพ็กเกตข้อมูลในขณะนั้น และจะรอเวลาเพื่อตรวจสอบสถานะของช่องสัญญาณอีกครั้งต่อไป ด้วยการทำงานในรูปแบบนี้จะทำให้เซ็นเซอร์โนดทุกตัวสามารถใช้งานช่องสัญญาณได้อย่างคุ้มค่าที่สุดในสภาวะที่เกิดการแทรกสอดขึ้น

ภาควิชา วิศวกรรมไฟฟ้า ลายมือชื่อนิสิต.....

สาขาวิชา วิศวกรรมไฟฟ้า ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก.....

ปีการศึกษา 2555

5270798221 : MAJOR ELECTRICAL ENGINEERING

KEYWORDS: WIRELESS SENSOR NETWORKS / IEEE 802.15.4 / IEEE 802.11 / COEXISTENCE / INTERFERENCE

WANTAWAT WONGMANOCH : ADAPTIVE ED THRESHOLD SCHEME FOR IEEE 802.15.4 WIRELESS SENSOR NETWORKS TO SUPPORT COEXISTENCE WITH IEEE 802.11B/G. ADVISOR : ASSOC. PROF. WATIT BENJAPOLAKUL. D. Eng., 108 pp.

IEEE 802.15.4 is becoming an attractive technology for Wireless Sensor Networks (WSNs) applications because of its simplicity, low cost, low power, and high reliability. However, IEEE 802.15.4 operates on unlicensed 2.4 GHz band, which shares among many wireless technologies. Especially, the widely-used IEEE 802.11b/g can be considered as the highest risk to IEEE 802.15.4 due to its characteristics that have more advantage than IEEE 802.15.4. Therefore, IEEE 802.15.4 networks may suffer from performance degradation in the presence of heavy IEEE 802.11b/g interference, which may impact Wireless Sensor Networks applications.

In this thesis, we propose an approach to improve IEEE 802.15.4 Wireless Sensor Networks performance in the coexistence with IEEE 802.11b/g in order to mitigate the performance degradation introduced by interference between these two standards by improving IEEE 802.15.4 channel access mechanism. In the proposed scheme, transmitter can transmit packet while there are interference from IEEE 802.11b/g if energy of the interference does not cause transmission failure but if energy of the interference may cause transmission failure, the transmitter will not transmit packet and will wait for next attempt. With this scheme, the sensor nodes can effectively utilize the channel in the presence of heavy interference.

Department : Electrical Engineering Student's Signature.....

Field of Study : Electrical Engineering Advisor's Signature.....

Academic Year : 2012

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดีด้วยความช่วยเหลืออย่างดียิ่งของอาจารย์ที่ปรึกษาวิทยานิพนธ์ คือ รศ. ดร.วาทิต เบญจพลกุล ซึ่งได้ให้ความรู้ คำแนะนำ และข้อคิดเห็นต่างๆ อันมีค่ายิ่ง อีกทั้งยังตรวจทานงานวิทยานิพนธ์ด้วยดีเสมอมา ตลอดจนอาจารย์ทุกๆ ท่านที่ได้กรุณาให้ความรู้ ข้อคิดเห็นและข้อเสนอแนะต่างๆ ซึ่งเป็นประโยชน์กับงานวิจัย ผู้วิจัยจึงขอกราบขอบพระคุณมา ณ ที่นี้

ขอขอบคุณท่านคณะกรรมการสอบวิทยานิพนธ์ทุกท่านที่ได้สละเวลาอันมีค่าตลอดจนให้คำแนะนำและแนวทางในการปรับปรุงงานวิจัยให้มีความสมบูรณ์มากยิ่งขึ้น ขอขอบคุณ พี่ๆ เพื่อนๆ และน้องๆ ในห้องปฏิบัติการวิจัยศูนย์เชี่ยวชาญพิเศษเฉพาะด้านเทคโนโลยีโทรคมนาคมทุกๆ คนที่ได้ให้ความช่วยเหลือและคำแนะนำที่ดีเสมอมา รวมถึงเพื่อนๆทุกคนที่คอยให้กำลังใจตลอดมา

สุดท้ายนี้ผู้วิจัยขอกราบขอบคุณ บิดา มารดา และครอบครัวที่ให้ความรัก ความเข้าใจและแรงสนับสนุนที่ดีตลอดมาซึ่งถือเป็นกำลังใจที่สำคัญจนผู้วิจัยสำเร็จการศึกษา

สารบัญ

หน้า

หน้า

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

รูปที่ **หน้า**

รูปที่ **หน้า**

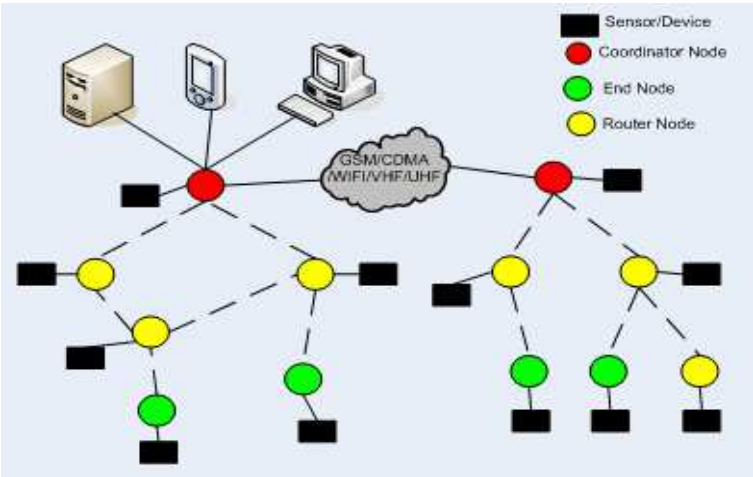
รูปที่ **หน้า**

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เครือข่ายเซ็นเซอร์ไร้สาย (Wireless Sensor Networks, WSNs) เป็นเครือข่ายของกลุ่มเซ็นเซอร์โนด (Sensor node) ซึ่งใช้สำหรับตรวจวัดคุณสมบัติต่างๆ ในพื้นที่ที่ต้องการ และสามารถส่งข้อมูลที่ตรวจวัดได้ไปยังปลายทางโดยอัตโนมัติ เพื่อนำข้อมูลเหล่านั้นไปใช้ประโยชน์ตามความต้องการต่อไป เซ็นเซอร์โนดแต่ละตัวสามารถควบคุมและบริหารจัดการงานของตนเองรวมทั้งสามารถติดต่อสื่อสารแบบไร้สายกับเซ็นเซอร์โนดข้างเคียงได้ ทุกๆเซ็นเซอร์โนดที่สามารถติดต่อสื่อสารถึงกันได้จะทำงานร่วมกันก่อให้เกิดเป็นเครือข่ายเซ็นเซอร์ไร้สายขึ้น ในเครือข่ายเซ็นเซอร์ไร้สาย แม้ว่าเซ็นเซอร์โนดต้นทางอาจไม่สามารถติดต่อกับเซ็นเซอร์โนดปลายทางได้โดยตรง เช่น อยู่ห่างกันเกินกว่าระยะสื่อสาร แต่ก็สามารถส่งต่อข้อมูลผ่านเซ็นเซอร์โนดระหว่างทางไปจนถึงเซ็นเซอร์โนดปลายทางได้ โดยวิธีการสื่อสารเช่นนี้เรียกว่าการสื่อสารแบบมัลติฮอป (Multi-hop) ดังนั้น เครือข่ายเซ็นเซอร์ไร้สายถือเป็นเครือข่ายแบบมัลติฮอป (Multi-hop network)



รูปที่ 1.1 สถาปัตยกรรมโดยทั่วไปของเครือข่ายเซ็นเซอร์ไร้สาย

สถาปัตยกรรมทั่วไปของเครือข่ายเซ็นเซอร์ไร้สาย แสดงดังรูปที่ 1.1 ซึ่งสามารถแบ่งชนิดของเซ็นเซอร์โนดซึ่งต่อแต่นี้ไปจะเรียกแทนว่า “โนด” ตามหน้าที่การทำงาน ได้ 3 ชนิด คือ

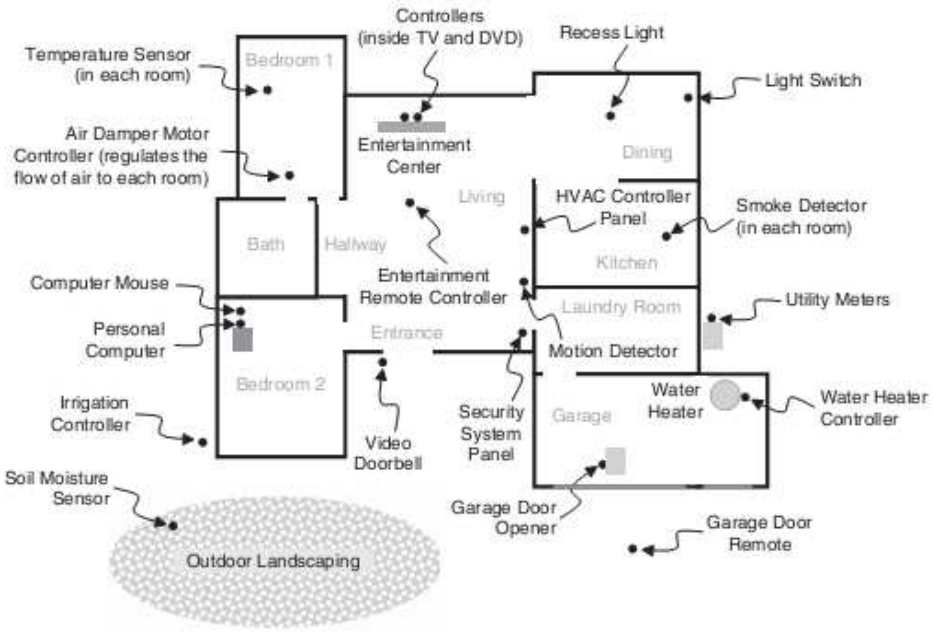
1. Coordinator node ทุกๆเครือข่ายเซ็นเซอร์ไร้สายจะต้องมี coordinator node อย่างน้อย 1 ตัว เพื่อทำหน้าที่เป็นศูนย์กลางในการควบคุมจัดการเครือข่าย

2. End node เป็นโนดที่สามารถส่งข้อมูลจากตนเองไปยังโนดอื่นได้เท่านั้น ไม่ได้ทำหน้าที่ส่งต่อข้อมูลจากโนดหนึ่งไปยังอีกโนดหนึ่ง มักจะเป็นโนดที่เชื่อมต่อกับเซ็นเซอร์หรืออุปกรณ์ปลายทาง

3. Router node เป็นโนดที่สามารถส่งข้อมูลจากตนเองไปยังโนดอื่น รวมทั้งสามารถส่งต่อข้อมูลจากโนดหนึ่งไปยังอีกโนดหนึ่งได้ด้วย โดย router node ถือเป็นปัจจัยสำคัญในเครือข่ายเซ็นเซอร์ไร้สายเนื่องจากเป็นโนดที่ทำให้เกิดการส่งมัลติฮอป

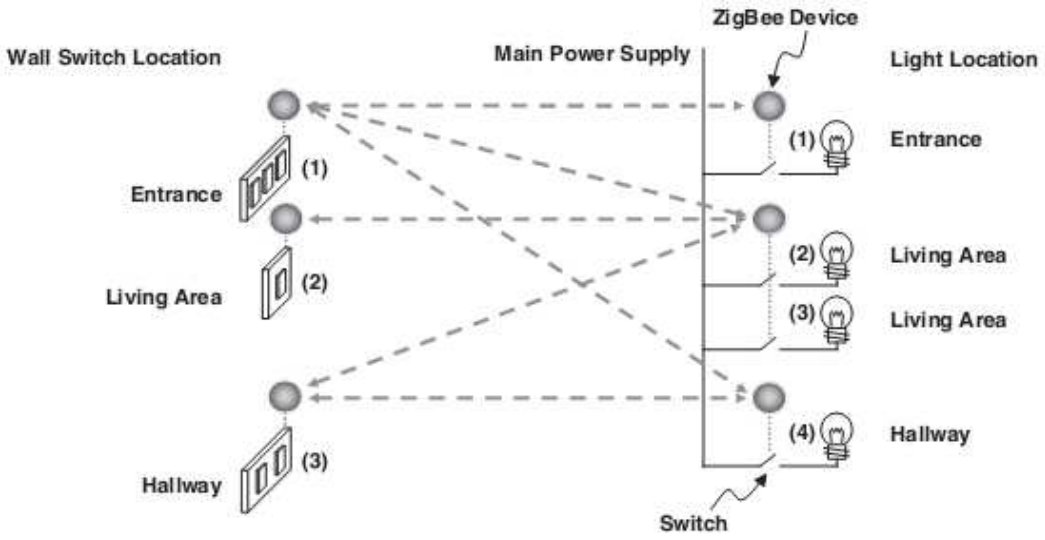
ปัจจุบันเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เริ่มเป็นที่สนใจทั้งในการใช้งานและการค้นคว้าวิจัย เนื่องจากมีความเรียบง่าย ราคาถูก ใช้พลังงานต่ำ และมีความเชื่อถือได้ (Reliability) สูง เนื่องจากรองรับทอพอโลยีแบบเมช ตัวอย่างเทคโนโลยีบนมาตรฐาน IEEE 802.15.4 ที่เป็นที่นิยม เช่น Zigbee, 6LoWPAN เป็นต้น โดย Zigbee ถือเป็นเทคโนโลยีที่ได้รับความสนใจเพิ่มขึ้นอย่างรวดเร็วในช่วงหลายปีมานี้ ตัวอย่างการประยุกต์ใช้งานที่ใช้เทคโนโลยี Zigbee ซึ่งเป็นที่นิยม [1] มี ดังนี้

1. ระบบอัตโนมัติภายในบ้าน (Home automation) ซึ่งถือเป็นหนึ่งในการประยุกต์ใช้งานหลักสำหรับระบบเครือข่ายเซ็นเซอร์ไร้สายของ Zigbee ในปัจจุบัน อัตราข้อมูลโดยทั่วไปสำหรับระบบอัตโนมัติภายในบ้านอยู่ที่ประมาณ 10 kbps เท่านั้น พิจารณารูปที่ 1.2 ซึ่งแสดงการประยุกต์ใช้งานของ Zigbee สำหรับระบบอัตโนมัติภายในบ้าน



รูปที่ 1.2 ตัวอย่างระบบอัตโนมัติภายในบ้านซึ่งใช้ Zigbee

- ระบบการอ่านหน่วยมิเตอร์อัตโนมัติ เป็นระบบที่มิเตอร์ไฟฟ้าสามารถส่งข้อมูลการอ่านหน่วยไปให้การไฟฟ้าโดยอัตโนมัติทุกๆช่วงเวลาที่กำหนด ซึ่งเป็นระบบที่มีแนวโน้มเติบโตอย่างรวดเร็วในต่างประเทศ รวมถึงประเทศไทยเองเช่นกัน ซึ่งระบบดังกล่าวเป็นที่รู้จักกันในชื่อ AMR (Automatic Meter Reading) หรือ AMI (Advanced Metering Infrastructure) การใช้ Zigbee สำหรับระบบการอ่านมิเตอร์อัตโนมัติจะเป็นการสร้างเครือข่ายไร้สายแบบเมชในพื้นที่ที่มีบ้านพักอาศัยหนาแน่น เพื่อเชื่อมต่อมิเตอร์ของบ้านแต่ละหลังกับระบบโครงข่ายสื่อสารของการไฟฟ้า นอกจากการอ่านหน่วยมิเตอร์ไฟฟ้าแล้ว ในบางประเทศยังรวมไปถึงการอ่านระบบมิเตอร์น้ำ มิเตอร์ก๊าซ เช่นกัน
- ระบบรดน้ำต้นไม้อัตโนมัติ ซึ่งมีการติดตั้งเซ็นเซอร์วัดความชื้นไว้ตามพื้นที่ต่างๆที่ต้องการ โดยจะติดต่อสื่อสารกับระบบควบคุมเพื่อกำหนดช่วงเวลาที่ระบบรดน้ำต้นไม้จะทำงาน โดยขึ้นอยู่กับระดับความชื้นของพื้นดิน ชนิดของต้นไม้ ช่วงเวลาของวันและฤดูกาล เป็นต้น ซึ่งการติดตั้งเซ็นเซอร์ไว้ใต้พื้นดินนั้นจะไม่เหมาะสมกับระบบสื่อสารแบบมีสาย
- ระบบควบคุมแสงสว่าง เป็นระบบแรกๆที่มีการนำ Zigbee เข้ามาใช้ในบ้านหรืออาคาร การประยุกต์ใช้งานของระบบควบคุมแสงสว่างจะเป็นการเปิดปิดหลอดไฟแสงสว่างต่างๆโดยอัตโนมัติตามเงื่อนไขต่างๆ เช่น เปิดไฟเมื่อตรวจพบว่ามีคนเดินเข้ามาในห้อง หรือเปิดไฟเมื่อแสงสว่างภายในบ้านต่ำกว่าระดับที่กำหนด เป็นต้น ซึ่งZigbee เป็นเทคโนโลยีที่ได้รับความนิยมอย่างมากสำหรับระบบควบคุมแสงสว่าง เนื่องจากการใช้เทคโนโลยีสื่อสารแบบมีสายจะมีความซับซ้อนในการเดินสายเคเบิลอย่างมาก
- ระบบ HVAC แบบแยกโซน ซึ่งทำให้ระบบ HVAC ภายในบ้านสามารถควบคุมอุณหภูมิภายในห้องต่างๆให้แตกต่างกันได้ตามความต้องการและควบคุมการใช้พลังงานให้ประหยัดที่สุด

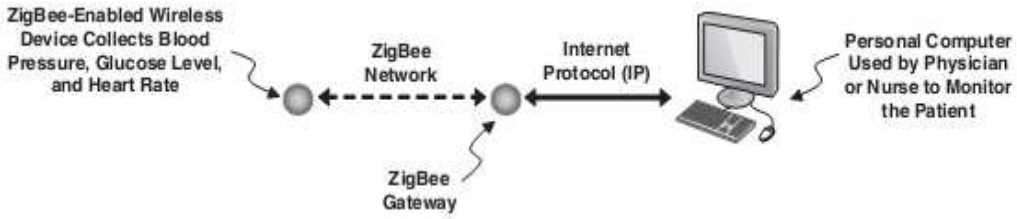


รูปที่ 1.3 ตัวอย่างระบบควบคุมแสงสว่างซึ่งใช้ Zigbee

2. ระบบควบคุมระยะไกล (Remote control) ของอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ซึ่งการใช้ Zigbee จะมีข้อได้เปรียบกว่าระบบควบคุมระยะไกลในปัจจุบันที่ใช้คลื่นอินฟราเรด เนื่องจาก Zigbee ซึ่งเป็นคลื่นความถี่วิทยุ (Radio Frequency, RF) สามารถส่งสัญญาณผ่านกำแพงหรือสิ่งกีดขวางได้ดีกว่า และไม่ต้องการเส้นทาง Line-of-sight ดังเช่น คลื่นอินฟราเรด ดังนั้น Zigbee หรือเทคโนโลยี IEEE 802.15.4 อื่นๆ น่าจะมีแนวโน้มมาแทนที่เทคโนโลยีอินฟราเรดมากขึ้น ซึ่งนอกจากข้อได้เปรียบข้างต้นแล้ว ยังมีข้อได้เปรียบด้านการประหยัดพลังงาน และรองรับการสื่อสารแบบสองทาง สำหรับการประยุกต์ใช้งานในอนาคตได้

3. ระบบอัตโนมัติภายในโรงงานอุตสาหกรรม (Industrial automation) ซึ่งระบบเครือข่ายแบบเมชของ Zigbee สามารถนำมาใช้ในระบบบริหารจัดการพลังงาน ระบบควบคุมแสงสว่าง ระบบบริหารจัดการสินทรัพย์ รวมไปถึงระบบควบคุมอัตโนมัติของกระบวนการผลิตด้วย

4. ระบบดูแลสุขภาพ (Healthcare) เป็นหนึ่งในการประยุกต์ใช้งาน Zigbee ที่เริ่มได้รับความสนใจ โดยบริษัทด้านการดูแลสุขภาพสามารถตรวจสอบข้อมูลสำคัญของคนไข้ที่กลับมาพักรักษาตัวที่บ้าน ตัวอย่างข้อมูลสำคัญดังกล่าว เช่น อัตราการเต้นของหัวใจ ความดันโลหิต เป็นต้น ซึ่งเซ็นเซอร์ที่ใช้วัดค่าดังกล่าวเป็นเซ็นเซอร์ Zigbee ซึ่งจะส่งข้อมูลที่วัดได้ต่อไปยัง Zigbee gateway เพื่อส่งข้อมูลต่อไปยังบริษัทด้านการดูแลสุขภาพต่อไป



รูปที่ 1.4 ตัวอย่างระบบดูแลสุขภาพผู้ป่วยตามบ้าน

5. การประยุกต์ใช้งานอื่นๆ เช่น ระบบควบคุมการเข้าออกห้องพักในโรงแรมซึ่งการใช้ Zigbee จะสะดวกกว่าการใช้เทคโนโลยีสื่อสารแบบมีสายซึ่งต้องเดินสายสำหรับประตูห้องพักทุกห้อง หรือระบบตรวจสอบอุปกรณ์ดับเพลิงอัตโนมัติ ซึ่งจะตรวจสอบค่าต่างๆของอุปกรณ์ดับเพลิงและส่งไปให้ผู้รับผิดชอบเป็นระยะ ช่วยให้สามารถดูแลอุปกรณ์ดับเพลิงทุกตัวให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ และประหยัดค่าจ้างบุคลากรไปตรวจสอบซึ่งอาจเกิดความผิดพลาดตกหล่นได้เช่นกัน

เนื่องจากเครือข่าย IEEE 802.15.4 ทำงานบนแถบความถี่ 2.4 GHz ซึ่งเป็นแถบความถี่สาธารณะสำหรับอุตสาหกรรม วิทยาศาสตร์ และการแพทย์ (The industrial, scientific and medical (ISM) band) ซึ่งเป็นแถบความถี่ที่ไม่ต้องขออนุญาตใช้งาน จึงมีเทคโนโลยีอื่นๆจำนวนมากที่ทำงานบนแถบความถี่นี้ เช่น เครือข่าย IEEE 802.11b/g, Bluetooth, โทรศัพท์แบบไร้สาย (Cordless phone) และเตาไมโครเวฟ เป็นต้น ซึ่งการใช้งานเทคโนโลยีดังกล่าวในพื้นที่เดียวกับบริเวณที่มีการใช้งานเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 จะทำเกิดการแทรกสอด (Interference) ระหว่างกัน และอาจทำให้สมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายลดลงได้ โดยเฉพาะ Wi-Fi (Wireless Fidelity) ซึ่งเป็นเทคโนโลยีบนเครือข่าย IEEE 802.11b/g ที่มีการใช้งานกันอย่างแพร่หลายโดยเฉพาะในบ้านพักอาศัย ทำให้มีโอกาสที่จะเกิดการแทรกสอดกับการประยุกต์ใช้งานต่างๆของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ภายในบ้านหรืออาคารดังที่ได้กล่าวข้างต้น ซึ่งด้วยลักษณะเฉพาะต่างๆของเครือข่าย IEEE 802.11b/g มีโอกาสทำให้สมรรถนะของเครือข่าย IEEE 802.15.4 ลดลงอย่างมากและทำให้ระบบต่างๆเหล่านี้ทำงานผิดพลาดได้ ซึ่งปัญหาดังกล่าวได้มีงานวิจัยจำนวนมากที่ได้พัฒนาแนวทางการลดผลกระทบจากการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b/g ดังที่จะนำเสนอในบทที่ 2

1.2 วัตถุประสงค์ของวิทยานิพนธ์

1. เสนอวิธีปรับปรุงการทำงานของเครือข่ายเซ็นเซอร์ไร้บนมาตรฐาน IEEE 802.15.4 ในกรณีที่ใช้งานแถบความถี่ร่วมกันกับเครือข่ายพื้นที่ท้องถิ่นไร้สาย (Wireless Local Area Networks, WLANs) ซึ่งอยู่บนมาตรฐาน IEEE 802.11b/g เพื่อบรรเทาปัญหาที่สมรรถนะการทำงานของเครือข่ายเซ็นเซอร์ไร้สายอาจลดลง อันเนื่องมาจากการแทรกสอดระหว่างสัญญาณของทั้ง 2 มาตรฐานข้างต้น โดยใช้การออกแบบวิธีตรวจสอบการเกิดการแทรกสอด และการปรับเปลี่ยนวิธีตรวจสอบเพื่อเข้าถึงช่องสัญญาณของโนดส่งในมาตรฐาน IEEE 802.15.4 ให้เหมาะสมกับสภาวะของการแทรกสอด
2. ศึกษาขั้นตอนการทำงานในการรับส่งแพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 และ IEEE 802.11b/g และวิเคราะห์สมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ในกรณีที่มีการแทรกสอดกับเครือข่าย IEEE 802.11b/g เปรียบเทียบระหว่างวิธีที่เสนอ กับวิธี ED และวิธี CS ซึ่งเป็นวิธีการตรวจสอบสถานะของช่องสัญญาณที่กำหนดอยู่ในมาตรฐาน IEEE 802.15.4

1.3 แนวทางวิทยานิพนธ์

วิทยานิพนธ์นี้เป็นการเสนอวิธีปรับปรุงสมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ในกรณีที่ใช้งานแถบความถี่ร่วมกันเครือข่าย IEEE 802.11b/g ซึ่งเป็นที่นิยมใช้กันอย่างแพร่หลายโดยเฉพาะตามบ้านพักอาศัยหรืออาคารสำนักงาน เพื่อบรรเทาปัญหาที่เครือข่ายเซ็นเซอร์ไร้สายอาจมีสมรรถนะลดลงหรือทำงานผิดพลาด อันเนื่องมาจากการแทรกสอดระหว่างสัญญาณทั้ง 2 มาตรฐานข้างต้น

แนวความคิดที่นำเสนอในวิทยานิพนธ์ คือ การปรับปรุงรูปแบบการตรวจสอบเพื่อเข้าถึงช่องสัญญาณของโนดส่งในมาตรฐาน IEEE 802.15.4 โดยการตรวจสอบว่าสัญญาณแทรกสอด (ในวิทยานิพนธ์นี้จะศึกษาเฉพาะสัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b/g เท่านั้น) ที่เกิดขึ้นในขณะนั้นจะส่งผลกระทบให้การส่งแพ็กเกตข้อมูลครั้งนี้ล้มเหลวหรือไม่ เพื่อที่โนดส่งของในมาตรฐาน IEEE 802.15.4 จะสามารถส่งแพ็กเกตข้อมูลได้ หากระดับพลังงานของสัญญาณแทรกสอดไม่ส่งผลกระทบให้การส่งแพ็กเกตข้อมูลล้มเหลว แต่หากระดับพลังงานของสัญญาณแทรกสอดอาจส่งผลให้การส่งแพ็กเกตข้อมูลล้มเหลวได้ โนดส่งก็จะยังไม่ส่งแพ็กเกตข้อมูลใน

ขณะนั้น และจะรอเวลาเพื่อตรวจสอบสถานะของช่องสัญญาณอีกครั้งต่อไป เพื่อลดโอกาสในการสูญเสียพลังงานและแพ็กเกตข้อมูลสูญเสีย ซึ่งอาจเกิดขึ้นจากการส่งแพ็กเกตข้อมูลล้มเหลว

1.4 ขอบเขตและเป้าหมายของวิทยานิพนธ์

1. เสนอแบบแผนการทำงานเพื่อควบคุมการเข้าถึงช่องสัญญาณของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เพื่อเพิ่มสมรรถนะโดยรวมของเครือข่ายเซ็นเซอร์ไร้สาย ในกรณีที่มีการแทรกสอดจากเครือข่าย IEEE 802.11b/g
2. สร้างแบบจำลองการทำงานของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เมื่อใช้วิธีวิธีที่เสนอ, วิธี ED และวิธี CS ในการควบคุมการเข้าถึงช่องสัญญาณ และสร้างแบบจำลองการทำงานของเครือข่าย IEEE 802.11b เพื่อใช้เป็นสัญญาณแทรกสอด
3. เปรียบเทียบสมรรถนะของวิธีที่เสนอ กับวิธี ED และวิธี CS

1.5 ขั้นตอนการดำเนินการ

1. ศึกษารายละเอียดและหลักการทำงานของเครือข่าย IEEE 802.15.4 และ IEEE 802.11b/g
2. ศึกษางานวิจัยและแนวทางต่างๆที่ช่วยบรรเทาปัญหาสมรรถนะการทำงานของเครือข่ายIEEE 802.15.4 ลดลงอันเนื่องมาจากการแทรกสอด ระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b/g
3. ศึกษาแบบจำลองในการวิเคราะห์การแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b/g
4. พัฒนาแบบแผนการควบคุมการเข้าถึงช่องสัญญาณของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เพื่อเพิ่มสมรรถนะการทำงานในกรณีที่มีการแทรกสอดจากเครือข่าย IEEE 802.11b/g
5. จำลองการทำงานของวิธีที่เสนอ, วิธี ED และวิธี CS
6. วิเคราะห์และเปรียบเทียบสมรรถนะการทำงานระหว่างวิธีที่เสนอ, วิธี ED และวิธี CS
7. สรุปผลและรวบรวมข้อมูลพร้อมทั้งจัดทำรูปเล่มวิทยานิพนธ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. แบบแผนที่เสนอในงานวิจัย สามารถเพิ่มสมรรถนะการทำงานโดยรวมให้กับเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เมื่อต้องทำงานร่วมกับการแทรกสอดจากเครือข่าย IEEE 802.11b/g
2. องค์ความรู้ในการประเมินสมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ในกรณีที่มีการแทรกสอดจากเครือข่าย IEEE 802.11b/g
3. องค์ความรู้เกี่ยวกับรายละเอียดและขั้นตอนการทำงานในการรับส่งแพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 และ IEEE 802.11b/g

บทที่ 2

การแทรกสอดกันระหว่างมาตรฐาน IEEE 802.15.4 กับ IEEE 802.11 และงานวิจัยที่เกี่ยวข้อง

ในช่วงระยะเวลาที่ผ่านมา การสื่อสารแบบไร้สายมีวิวัฒนาการและมีการเติบโตอย่างรวดเร็วจนเข้ามาทดแทนระบบสื่อสารแบบมีสายได้ในหลากหลายการใช้งาน ด้วยข้อได้เปรียบที่ไม่ต้องพึ่งพาสายสัญญาณในการสื่อสารทำให้ลดความยุ่งยากในการติดตั้งลงได้มาก นอกจากนี้ระบบสื่อสารไร้สายยังช่วยให้ผู้ใช้งานสามารถเชื่อมต่อเข้าสู่เครือข่ายได้โดยไม่จำกัดสถานที่ ตราบใดที่ยังอยู่ในเขตสัญญาณ ซึ่งเพิ่มความสะดวกสบายให้กับผู้ใช้งานเป็นอย่างมาก แม้ว่าที่ผ่านมาระบบสื่อสารไร้สายโดยทั่วไปยังมีอัตราข้อมูลต่ำกว่าระบบสื่อสารแบบมีสาย แต่ด้วยการพัฒนาที่รวดเร็วทำให้ระบบสื่อสารไร้สายในปัจจุบันมีความเร็วสูงขึ้นมาก จนสามารถทดแทนการใช้งานระบบสื่อสารแบบมีสายได้ ที่เห็นได้ชัดเจนคือ ระบบโทรศัพท์ ซึ่งปัจจุบันโทรศัพท์เคลื่อนที่ได้เข้ามาทดแทนโทรศัพท์พื้นฐานเกือบทั้งหมดแล้ว การเชื่อมต่ออินเทอร์เน็ตเองก็เริ่มเปลี่ยนมาเป็นการเชื่อมต่อผ่าน smart phone, tablet หรือ คอมพิวเตอร์ notebook ด้วยระบบสื่อสารไร้สายมากขึ้น

นอกจากระบบสื่อสารไร้สายสำหรับโทรศัพท์มือถือแล้ว หากมองเข้ามาภายในบ้าน อาคารสำนักงาน หรือแม้กระทั่งในโรงงานอุตสาหกรรม ระบบสื่อสารไร้สายก็เริ่มเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น อุปกรณ์ต่างๆซึ่งเคยต้องการสายสัญญาณก็เริ่มเปลี่ยนเป็นแบบไร้สายมากขึ้น เช่น เมาส์ไร้สาย หูฟังไร้สาย หรือการส่งรูปภาพจากโทรศัพท์เคลื่อนที่หรือกล้องถ่ายรูปเข้าสู่คอมพิวเตอร์หรือเครื่องรับโทรทัศน์ก็มีเทคโนโลยีไร้สายเข้ามามากขึ้น ยิ่งไปกว่านั้น ระบบไร้สายยังเข้าไปมีบทบาทในระบบควบคุมอัตโนมัติต่างๆ ทั้งในบ้าน อาคารสำนักงาน หรือโรงงานอุตสาหกรรม ซึ่งเริ่มมีให้เห็นมากขึ้นเรื่อยๆในต่างประเทศ โดยระบบสื่อสารไร้สายสำหรับอุปกรณ์ต่างๆหรือในระบบควบคุมจะเป็นระบบสื่อสารไร้สายระยะสั้น แตกต่างจากระบบโทรศัพท์เคลื่อนที่ที่จะใช้เทคโนโลยีสื่อสารไร้สายที่มีระยะไกล

ระบบสื่อสารไร้สายระยะสั้นที่เป็นนิยมใช้งานในปัจจุบัน แบ่งได้เป็น 2 ประเภทหลักๆ คือ

1. เครือข่ายพื้นที่ท้องถิ่นไร้สาย (Wireless Local Area networks, WLANs) ซึ่งเป็นระบบเครือข่ายไร้สายที่นำมาใช้ทดแทนหรือเป็นส่วนขยายกับระบบเครือข่ายพื้นที่ท้องถิ่น (Local Area Networks, LANs) แบบมีสาย เช่น Ethernet (IEEE 802.3) โดยอุปกรณ์ WLAN สามารถนำมาเชื่อมต่อเข้ากับระบบ LAN แบบมีสายได้ทันที และเมื่ออุปกรณ์ WLAN ได้เข้ามาเป็นส่วนหนึ่ง

ระบบ LAN แล้ว ระบบ LAN จะมองอุปกรณ์ WLAN ดังกล่าว เสมือนเป็นอุปกรณ์แบบมีสายอื่นๆ ในเครือข่ายนั้น แนวทางการพัฒนา WLAN จะเน้นไปที่การเพิ่มอัตราข้อมูล (Data rate) และระยะทางสื่อสาร ระบบ WLAN ที่เป็นที่นิยมใช้กันทั่วโลกในปัจจุบันจะมีพื้นฐานมาจากชุดมาตรฐาน IEEE 802.11

2. เครือข่ายพื้นที่บุคคลไร้สาย (Wireless Personal Area Networks, WPANs) ซึ่งเป็นระบบที่ไม่ได้ถูกพัฒนาให้มาทดแทนระบบ LAN แบบมีสาย โดยวัตถุประสงค์หลักของ WPAN คือการสร้างระบบเครือข่ายที่มุ่งเน้นด้านการใช้พลังงานอย่างมีประสิทธิภาพภายในพื้นที่ใช้งานส่วนบุคคล (Personal Operating Space, POS) ซึ่งเป็นพื้นที่รูปทรงกลมรัศมีประมาณ 10 เมตร หรือ 33 ฟุต รอบๆอุปกรณ์สื่อสารไร้สาย โดยไม่จำเป็นต้องมีโครงสร้างพื้นฐานใดๆ ระบบ WPAN ที่เป็นที่นิยมใช้กันทั่วโลกในปัจจุบันจะมีพื้นฐานมาจากชุดมาตรฐาน IEEE 802.15

WPAN ยังสามารถแบ่งย่อยได้อีกเป็น 3 ระดับ ตามอัตราข้อมูล ดังนี้

2.1 เครือข่ายพื้นที่บุคคลไร้สายอัตราข้อมูลสูง (High-rate Wireless Personal Area Networks, HR-WPANs) ตัวอย่างเช่น มาตรฐาน IEEE 802.15.3 ซึ่งมีอัตราข้อมูล 11 Mbps ถึง 55 Mbps ด้วยอัตราข้อมูลที่สูงเช่นนี้ HR-WPAN จึงสามารถรองรับการประยุกต์ใช้งานที่ต้องการอัตราข้อมูลสูง เช่น การส่งสัญญาณภาพจากกล้องถ่ายรูปไปยังเครื่องรับโทรทัศน์ เป็นต้น

2.2 เครือข่ายพื้นที่บุคคลไร้สายอัตราข้อมูลปานกลาง (Medium-rate Wireless Personal Area Networks, MR-WPANs) มีอัตราข้อมูลประมาณ 1 ถึง 3 Mbps ตัวอย่าง เช่น เทคโนโลยี Bluetooth ซึ่งมีพื้นฐานมาจากมาตรฐาน IEEE 802.15.1 การประยุกต์ใช้งานของ MR-WPAN มักจะนิยมใช้ในการส่งสัญญาณเสียงคุณภาพสูง เช่น หูฟังแบบไร้สาย เป็นต้น

2.3 เครือข่ายพื้นที่บุคคลไร้สายอัตราข้อมูลต่ำ (Low-rate Wireless Personal Area Networks, LR-WPANs) ตัวอย่างเช่น Zigbee และ 6LoWPAN ซึ่งมีพื้นฐานมาจากมาตรฐาน IEEE 802.15.4 โดย LR-WPAN มีอัตราข้อมูลสูงสุดที่ 250 kbps

ระบบสื่อสารไร้สายระยะสั้นที่ใช้งานกันโดยทั่วไป มักจะเป็นเทคโนโลยีที่ทำงานบนแถบความถี่ 2.4 GHz ซึ่งเป็นแถบความถี่สาธารณะสำหรับอุตสาหกรรม วิทยาศาสตร์ และการแพทย์ (The industrial, scientific and medical (ISM) band) ซึ่งสามารถใช้งานได้ทันทีโดยที่ไม่ต้องขออนุญาต เทคโนโลยีที่ใช้งานแถบความถี่ 2.4 GHz ซึ่งเป็นที่นิยมใช้งานอย่างแพร่หลาย ตัวอย่าง เช่น Wi-Fi (IEEE 802.11b/g), Bluetooth (IEEE 802.15.1) และ Zigbee (IEEE 802.15.4) แม้ว่ามาตรฐาน IEEE 802.15.4 จะมีอัตราข้อมูลต่ำที่สุด เมื่อเปรียบเทียบกับเทคโนโลยีอื่นๆ แต่การ

ประยุกต์ใช้งานสำหรับเครือข่ายเซ็นเซอร์ไร้สาย ซึ่งต้องการเพียงแค่การรับส่งสัญญาณคำสั่ง เช่น การสั่งเปิดปิดสวิทช์หลอดไฟ หรือ การรวบรวมข้อมูลจากเซ็นเซอร์ต่างๆ ตัวอย่างเช่น อุณหภูมิ และค่าความชื้นเท่านั้น ดังนั้น เครือข่ายเซ็นเซอร์ไร้สายโดยทั่วไปจึงต้องการอัตราข้อมูลที่ไม่สูงนัก ซึ่งเครือข่าย IEEE 802.15.4 ถือเป็นตัวเลือกที่เหมาะสมที่สุด เนื่องจากเป็นระบบเครือข่ายที่มีความเรียบง่าย, ประหยัดพลังงาน และมีความเชื่อถือได้สูง ทำให้อายุการใช้งานของแบตเตอรี่สำหรับอุปกรณ์ปลายทางหรือเซ็นเซอร์ยาวนานกว่าการใช้เทคโนโลยีอื่นๆ

สำหรับเครือข่าย IEEE 802.11b/g ซึ่งมีอัตราข้อมูลสูงสุด 11 Mbps (สำหรับ IEEE 802.11b) และ 54 Mbps (สำหรับ IEEE 802.11g) มีระยะทางสื่อสารประมาณ 30-100 เมตร มักนิยมใช้งานกับการเชื่อมต่อระบบอินเทอร์เน็ตแบบไร้สาย ในขณะที่ Bluetooth ซึ่งมีอัตราข้อมูลไม่เกิน 3 Mbps มีระยะสื่อสารเพียงประมาณ 2-10 เมตร จึงเหมาะสมสำหรับการประยุกต์ใช้งานระหว่างโทรศัพท์เคลื่อนที่กับอุปกรณ์เสริมอื่นๆ เช่น หูฟังไร้สาย หรืออุปกรณ์ Hands-free เป็นต้น

ตารางที่ 2.1 เปรียบเทียบเทคโนโลยีสื่อสารไร้สายบนแถบความถี่ 2.4 GHz

เทคโนโลยี	อัตราข้อมูล	ระยะทางสื่อสาร	การประยุกต์ใช้งาน
Zigbee (IEEE 802.15.4)	20 ถึง 250 kbps	10-100 เมตร	เครือข่ายเซ็นเซอร์ไร้สาย
Bluetooth (IEEE 802.15.1)	1 ถึง 3 Mbps	2-10 เมตร	หูฟังไร้สาย เมาส์ไร้สาย
Wi-Fi (IEEE 802.11b)	1 ถึง 11 Mbps	30-100 เมตร	การเชื่อมต่ออินเทอร์เน็ตแบบไร้สาย

ด้วยเหตุนี้ มาตรฐาน IEEE 802.15.4 ได้รับความสนใจเพิ่มขึ้นอย่างรวดเร็วในช่วงระยะเวลาที่ผ่านมา โดยเฉพาะกับการประยุกต์ใช้งานเป็นเครือข่ายเซ็นเซอร์ไร้สายแบบเมช เช่น ระบบอัตโนมัติภายในบ้าน ระบบการอ่านหน่วยมิเตอร์อัตโนมัติ ระบบดูแลสุขภาพ (Healthcare) หรือแม้แต่ระบบควบคุมอัตโนมัติภายในโรงงานอุตสาหกรรม โดยระบบสื่อสารแบบไร้สายจะมีข้อได้เปรียบกว่าระบบสื่อสารแบบมีสายสำหรับการประยุกต์ใช้งานดังกล่าว เนื่องจากในกรณีที่ใช้ระบบสื่อสารแบบมีสาย การติดตั้งเซ็นเซอร์จำนวนมากจะค่อนข้างยุ่งยากในการเดินสำหรับ

บ้านพักอาศัยหรือโรงงานอุตสาหกรรมที่มีการวางผังการเดินสายระบบไฟฟ้าไว้เรียบร้อยแล้ว ในขณะที่การใช้ระบบสื่อสารแบบไร้สายจะลดความยุ่งยากในการเดินสายสื่อสารลงได้มาก เพียงแค่ติดตั้งเซ็นเซอร์ไร้สายตามจุดที่ต้องการก็สามารถสร้างระบบอัตโนมัติภายในบ้าน อาคาร หรือโรงงานอุตสาหกรรมได้อย่างรวดเร็ว

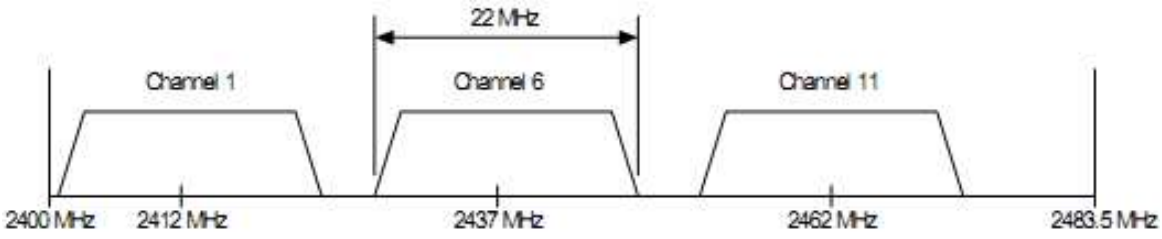
อย่างไรก็ตาม การที่เครือข่าย IEEE 802.15.4 ทำงานบนแถบความถี่ 2.4 GHz ซึ่งเป็นแถบความถี่สาธารณะ จึงมีเทคโนโลยีอื่นๆจำนวนมากที่ทำงานบนแถบความถี่นี้ เช่น เครือข่าย IEEE 802.11b/g, Bluetooth ดังที่ได้กล่าวไปแล้ว และยังรวมไปถึงโทรศัพท์แบบไร้สาย (Cordless phone) และเตาไมโครเวฟ เป็นต้น หากมีการใช้งานเทคโนโลยีดังกล่าวในพื้นที่เดียวกับบริเวณที่มีการใช้งานเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 จะทำเกิดการแทรกสอด (Interference) ระหว่างกัน และอาจทำให้สมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายลดลงได้ เครือข่าย IEEE 802.11b/g ซึ่งมีการใช้งานกันอย่างแพร่หลายที่สุด โดยเฉพาะการเชื่อมต่ออินเทอร์เน็ตในบ้านพักอาศัย ถือเป็นเทคโนโลยีที่มีโอกาสเกิดการแทรกสอดเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 มากที่สุด ซึ่งด้วยลักษณะเฉพาะต่างๆของเครือข่าย IEEE 802.11b/g มีโอกาสทำให้สมรรถนะของเครือข่าย IEEE 802.15.4 ลดลงอย่างมาก และทำให้การประยุกต์ใช้งานที่ใช้เครือข่ายเซ็นเซอร์ไร้สายมีโอกาสทำงานผิดพลาดได้ ดังนั้น งานวิจัยนี้จะเน้นศึกษาผลกระทบของเครือข่าย IEEE 802.15.4 จากการแทรกสอดโดยเครือข่าย IEEE 802.11b/g เป็นหลัก

2.1 การซ้อนทับกันระหว่างเครือข่าย IEEE 802.15.4 กับ IEEE 802.11b/g - [2], [3]

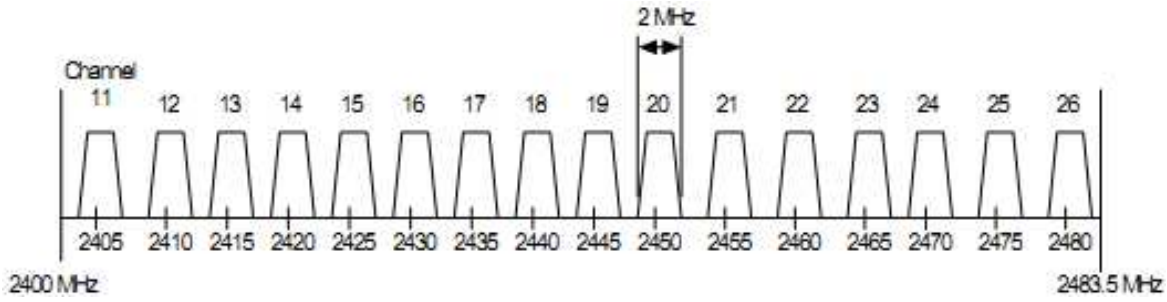
มาตรฐาน IEEE 802.15.4 เป็นมาตรฐานที่กำหนดโดย IEEE (Institute of Electrical and Electronics Engineers) ซึ่งออกแบบมาเพื่อกำหนดการทำงานในชั้นกายภาพ (Physical layer, PHY) และชั้นย่อยควบคุมการเข้าถึงตัวกลาง (Media Access Control sublayer, MAC) สำหรับเครือข่ายพื้นที่บุคคลไร้สายอัตราข้อมูลต่ำ (Low-Rate Wireless Personal Area Networks, LR-WPANs) ซึ่งเป็นระบบเครือข่ายที่มีความเรียบง่าย, ประหยัดพลังงาน, มีความเชื่อถือได้ และเหมาะสมสำหรับการสื่อสารแบบไร้สายสำหรับการประยุกต์ใช้งานที่มีพลังงานจำกัดและมีปริมาณข้อมูลไม่มากนัก

มาตรฐาน IEEE 802.15.4 กำหนดการใช้งานเป็น 3 แถบความถี่ (Frequency band) คือ 868 MHz, 915 MHz และ 2450 MHz ซึ่งแถบความถี่ 2450 MHz เป็นแถบความถี่ที่นิยมใช้มากที่สุด เนื่องจากเป็นแถบความถี่ที่ไม่ต้องขออนุญาตใช้งานและมีอัตราข้อมูลสูงที่สุด ในแถบความถี่

2450 MHz มีช่องสัญญาณทั้งหมด 16 ช่อง คือ ช่องสัญญาณที่ 11-26 แต่ละช่องสัญญาณมีแบนด์วิดท์ 2 MHz และมีอัตราข้อมูล 250 kbps อย่างไรก็ตาม เนื่องจากเป็นแถบความถี่ที่สามารถใช้งานได้ทั่วไปโดยไม่ต้องขออนุญาต ทำให้มีหลายเทคโนโลยีที่ใช้งานแถบความถี่นี้เช่นกัน โดยเฉพาะเทคโนโลยี Wi-Fi บนมาตรฐาน IEEE 802.11b/g ถือเป็นเทคโนโลยีที่มีการใช้งานกันมากมายในหลายๆพื้นที่ ทั้งนี้ กำลังส่ง (Transmit power) ของเครือข่าย IEEE 802.11b/g สูงกว่ากำลังส่งของ เครือข่าย IEEE 802.15.4 อยู่มาก จึงอาจส่งผลให้สมรรถนะในการรับส่งข้อมูลของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ลดลง โดยเฉพาะเมื่อใช้งานในพื้นที่ที่มีทราฟฟิกของเครือข่าย IEEE 802.11b/g หนาแน่น และเซ็นเซอร์โนดอยู่ห่างจากโนดส่งของเครือข่าย IEEE 802.11b/g ไม่มากพอ



a) ช่องสัญญาณของ IEEE 802.11b/g ที่นิยมใช้งาน



b) ช่องสัญญาณของ IEEE 802.15.4

รูปที่ 2.1 ช่องสัญญาณของ IEEE 802.15.4 และ IEEE 802.11b/g ในแถบความถี่ 2.4 GHz

พิจารณารูปที่ 2.1 ซึ่งแสดงสเปกตรัมช่องสัญญาณของมาตรฐาน IEEE 802.15.4 และ IEEE 802.11b/g โดยในแถบความถี่ 2.4 GHz มาตรฐาน IEEE 802.15.4 จะมี 16 ช่องสัญญาณ แต่ละช่องสัญญาณมีแบนด์วิดท์ 2 MHz และไม่ซ้อนทับกับช่องสัญญาณข้างเคียง ในขณะที่มาตรฐาน IEEE 802.11b/g จะมี 14 ช่องสัญญาณ ซึ่งจะซ้อนทับกับช่องสัญญาณข้างเคียง โดยความถี่กลาง (Center frequency) ระหว่างช่องสัญญาณข้างเคียงจะห่างกัน 5 MHz ในขณะที่

แต่ละช่องสัญญาณมีแบนด์วิดท์ 22 MHz และเนื่องจากช่องสัญญาณของ IEEE 802.11b/g มีแบนด์วิดท์กว้างกว่าช่องสัญญาณของ IEEE 802.15.4 มาก ดังนั้น หนึ่งช่องสัญญาณของ IEEE 802.11b/g จะซ้อนทับกับช่องสัญญาณของ IEEE 802.15.4 อยู่ 4 หรือ 5 ช่องสัญญาณด้วยกัน ทั้งนี้ในพื้นที่หนึ่งๆ อาจมีการใช้งาน Wi-Fi พร้อมๆกันหลายเครือข่าย ซึ่งโดยทั่วไปการใช้งาน Wi-Fi หลายเครือข่ายในพื้นที่เดียวกันนั้นจะเลือกใช้ช่องสัญญาณต่างกัน ซึ่งช่องสัญญาณที่มักใช้กันทั่วไปคือ ช่องสัญญาณที่ 1, 6 และ 11 เนื่องจากเป็นช่องสัญญาณที่ไม่ซ้อนทับกัน ดังนั้นในพื้นที่ที่มีการใช้งาน Wi-Fi หลายเครือข่ายก็ยิ่งทำให้โอกาสที่ช่องสัญญาณของ IEEE 802.11b จะซ้อนทับกับช่องสัญญาณของ IEEE 802.15.4 มากขึ้น และจากการที่กำลังส่งของเครือข่าย IEEE 802.11b/g สูงกว่ามาก ดังนั้นจึงมีโอกาสสูงที่แพ็กเกตข้อมูลของเซ็นเซอร์โนดบนมาตรฐาน IEEE 802.15.4 จะสูญเสีย งานวิจัย [4] และ [5] ศึกษาสมรรถนะการทำงานของเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b/g เมื่อใช้งานในพื้นที่เดียวกัน ซึ่งผลการศึกษาของงานวิจัยดังกล่าว แสดงให้เห็นว่าสมรรถนะของเครือข่าย IEEE 802.15.4 ลดลงอย่างเห็นได้ชัดเมื่อมีการแทรกสอดจากเครือข่าย IEEE 802.11b/g ในขณะที่สมรรถนะของเครือข่าย IEEE 802.11b/g แทบไม่ได้รับผลกระทบมากนักจากการแทรกสอดจากเครือข่าย IEEE 802.15.4

2.2 หลักการทำงานของเครือข่าย IEEE 802.15.4 - [2]

ในหัวข้อนี้จะอธิบายถึงหลักการทำงานในการรับส่งข้อมูลของเครือข่าย IEEE 802.15.4 โดยจะเน้นไปที่ความรู้พื้นฐานและรายละเอียดที่เกี่ยวข้องกับการรับส่งข้อมูลของเครือข่าย IEEE 802.15.4 เท่านั้น เนื่องจากรายละเอียดในส่วนอื่นๆจะไม่อยู่ในขอบเขตของงานวิจัยนี้

2.2.1 ส่วนประกอบของเครือข่าย IEEE 802.15.4

อุปกรณ์ในเครือข่าย IEEE 802.5.4 สามารถแบ่งได้เป็น 2 ชนิด คือ Full-function device (FFD) และ Reduced-function device (RFD) โดย FFD คืออุปกรณ์ที่สามารถทำงานได้ทั้ง 3 หน้าที่การทำงาน คือ สามารถเป็น coordinator node, router node และ end node ได้ทั้งหมด (รายละเอียดหน้าที่การทำงานทั้ง 3 แบบ อยู่ในหัวข้อที่ 1.1) ขณะที่ FFD สามารถทำงานเป็น end node ได้เท่านั้น เช่น สวิทช์ไฟแสงสว่าง เป็นต้น

การที่จะสร้างเครือข่าย WPAN ได้นั้น จะต้องมีอุปกรณ์อย่างน้อย 2 ตัวขึ้นไปที่อยู่ในระยะ POS และทำงานอยู่บนช่องสัญญาณเดียวกัน โดยต้องมี FFD อย่างน้อย 1 ตัว เพื่อทำงานเป็น coordinator node ซึ่งเครือข่าย IEEE 802.15.4 ก็ถือเป็น WPAN เช่นกัน แต่ระยะสื่อสารของ

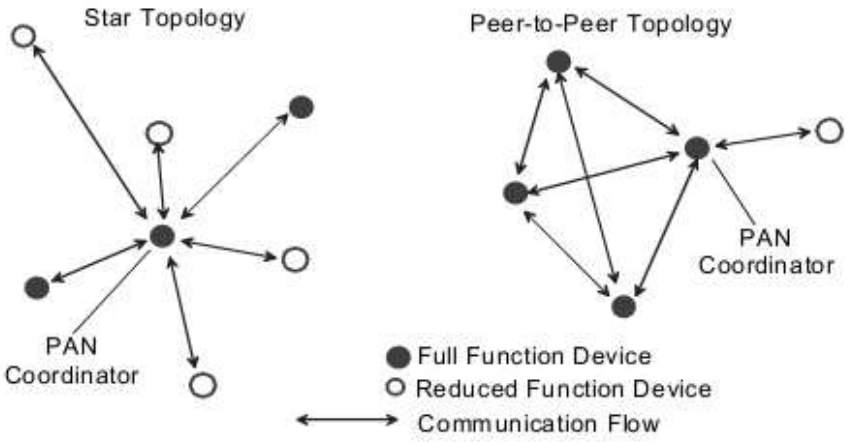
เครือข่าย IEEE 802.15.4 สามารถขยายได้มากกว่าระยะ POS อย่างไรก็ตาม ระยะสื่อสารของเครือข่าย IEEE 802.15.4 ไม่อาจระบุให้แน่ชัดได้ เนื่องจากการใช้ตัวกลางแบบไร้สาย จะมีหลายปัจจัยมาเกี่ยวข้อง เช่น ลักษณะการกระจาย (Propagation characteristic) ของคลื่นความถี่วิทยุที่มีความไม่แน่นอนขึ้นอยู่กับสภาพพื้นที่ที่ใช้งาน

2.2.2 ทอพอโลยีเครือข่าย

เครือข่าย IEEE 802.15.4 สามารถรองรับทอพอโลยีเครือข่ายได้ 2 แบบ ขึ้นอยู่กับความต้องการของการประยุกต์ใช้งาน คือ

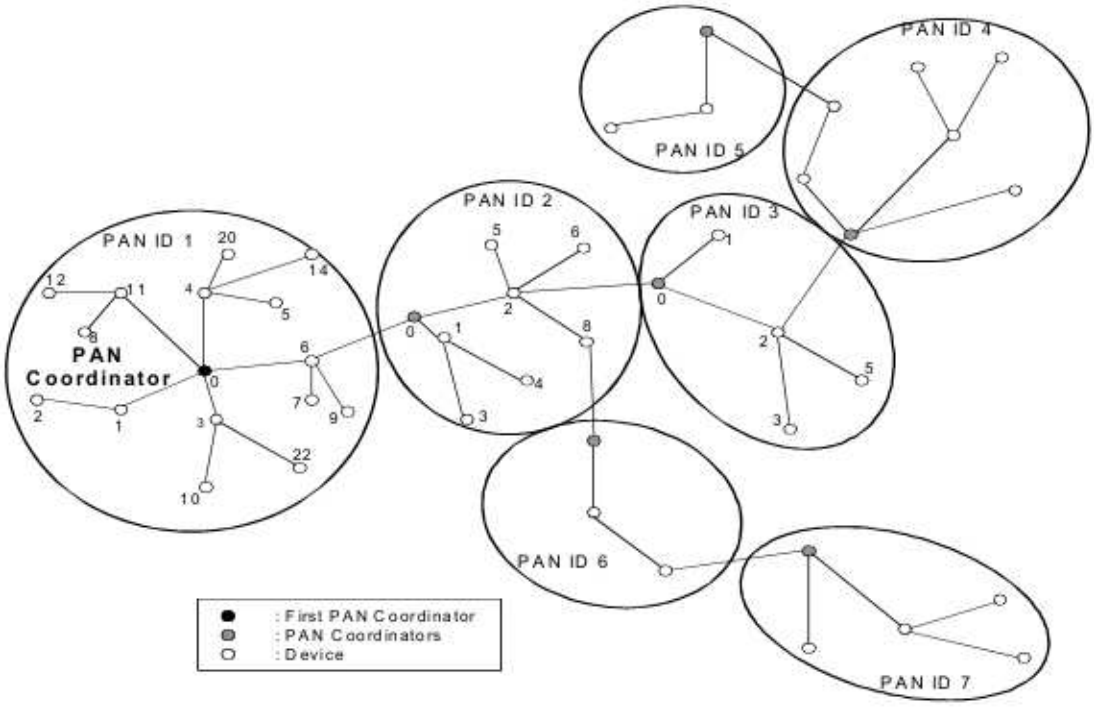
1. ทอพอโลยีแบบดาว (Star) คือ เครือข่ายที่อุปกรณ์ในเครือข่ายจะสื่อสารกันได้ผ่านอุปกรณ์ศูนย์กลางหนึ่งตัว ซึ่งอุปกรณ์ศูนย์กลางดังกล่าวก็คือ coordinator นั่นเอง ซึ่งในเครือข่ายแบบดาว coordinator node มักจะใช้ไฟฟ้าจากระบบไฟฟ้า เนื่องจากจะต้องเป็นศูนย์กลางในการรับและส่งต่อข้อมูลจากทุกโนดในเครือข่าย จึงใช้พลังงานมาก ในขณะที่อุปกรณ์ที่เหลือมักจะใช้พลังงานจากแบตเตอรี่ ตัวอย่างการประยุกต์ใช้งานของทอพอโลยีแบบดาว เช่น ระบบอัตโนมัติภายในบ้าน ซึ่งจะมีแผงควบคุมกลางหนึ่งชุดคอยทำหน้าที่ควบคุมอุปกรณ์ไฟฟ้าทุกเครื่องภายในบ้าน, ระบบดูแลสุขภาพส่วนบุคคล และอุปกรณ์ต่อพ่วงคอมพิวเตอร์ เช่น เมาส์ คีย์บอร์ด เป็นต้น

2. ทอพอโลยีแบบเพียร์ทูเพียร์ (Peer-to-Peer) จะแตกต่างจากทอพอโลยีแบบดาวตรงที่อุปกรณ์ภายในเครือข่ายสามารถสื่อสารกันได้โดยตรงโดยไม่ต้องผ่าน coordinator ตราบที่อยู่ในระยะสื่อสารของกันละกัน หรือในกรณีที่โนดปลายทางไม่อยู่ในระยะสื่อสารของโนดส่ง ก็สามารถสื่อสารแบบมัลติฮอปผ่านโนดอื่นๆไปยังโนดปลายทางได้ ทอพอโลยีแบบเพียร์ทูเพียร์ถือเป็นพื้นฐานของการสร้างทอพอโลยีแบบเมชของเครือข่าย IEEE 802.15.4 ซึ่งเป็นที่นิยมสำหรับการประยุกต์ใช้งานในเครือข่ายเซ็นเซอร์ไร้สาย, ระบบมอนิเตอร์และควบคุมในอุตสาหกรรม, ระบบรดน้ำต้นไม้อัตโนมัติ และระบบรักษาความปลอดภัย เป็นต้น เนื่องจากทอพอโลยีแบบเมชมีความเชื่อถือได้สูง มีความทนทานเนื่องจากสามารถรักษาตัวเอง (Self-healing) ได้โดยการเลือกเส้นทางการส่งข้อมูลใหม่ (Reroute) อย่างไรก็ตาม ฟังก์ชันเกี่ยวกับการเลือกเส้นทางจะอยู่ในระดับชั้น (Layer) ที่สูงกว่าข้อกำหนดในมาตรฐาน IEEE 802.15.4



รูปที่ 2.2 ทอพอโลยีพื้นฐานของเครือข่าย IEEE 802.15.4

นอกจากนี้ เครือข่าย IEEE 802.15.4 มากกว่าหนึ่งเครือข่ายยังสามารถเชื่อมต่อกันเป็นเครือข่ายพื้นที่ส่วนบุคคลไร้สายขนาดใหญ่เครือข่ายเดียวได้ โดยจะมี coordinator เพียงตัวเดียวจาก coordinator ของเครือข่ายย่อยทั้งหมดทำหน้าที่เป็น PAN coordinator ของเครือข่ายใหญ่เพื่อควบคุมการทำงานของเครือข่ายใหญ่ทั้งหมด ในขณะที่การสื่อสารกันระหว่างเครือข่ายย่อยจะต้องทำผ่าน coordinator ของแต่ละเครือข่ายย่อย เรียกสถาปัตยกรรมเช่นนี้ว่าเครือข่ายแบบ Cluster-tree



รูปที่ 2.3 เครือข่ายพื้นที่ส่วนบุคคลไร้สายแบบ Cluster-tree

2.2.3 กระบวนการรับส่งข้อมูล

ในหัวข้อนี้จะกล่าวถึงกระบวนการรับส่งข้อมูลของเครือข่าย IEEE 802.15.4 โดยจะอธิบายกลไกหลักๆที่ใช้ในกระบวนการรับส่งข้อมูล คือ กลไก CSMA-CA, การใช้ Frame Acknowledgement และการส่งซ้ำ (Retransmission) จากนั้นจะสรุปกระบวนการรับส่งข้อมูลทั้งหมดในภาพรวม

2.2.3.1 กลไก CSMA-CA

มาตรฐาน IEEE 802.15.4 ใช้กลไก Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) ในการควบคุมการเข้าถึงตัวกลางเพื่อหลีกเลี่ยงการเข้าถึงตัวกลางพร้อมกันของแต่ละโนด โดยกลไก CSMA-CA ในมาตรฐาน IEEE 802.15.4 จะมีอยู่ 2 แบบ ขึ้นอยู่กับรูปแบบการทำงานของเครือข่ายซึ่งเป็น 2 รูปแบบ คือ

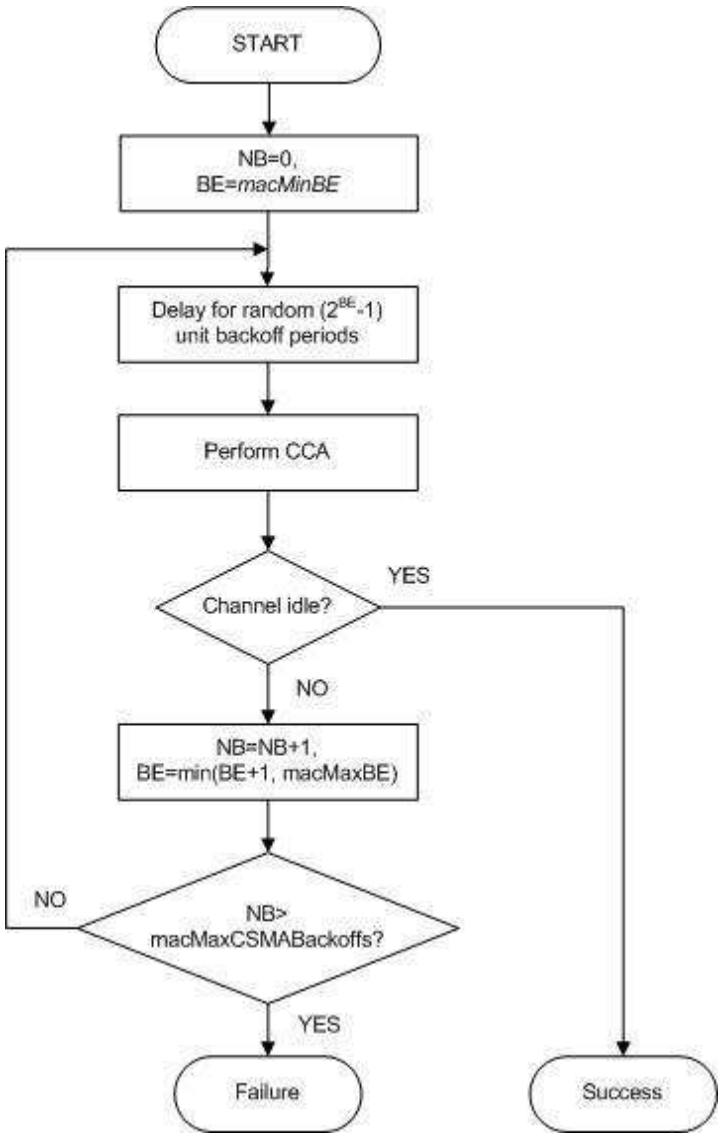
1) Beacon-enabled PAN เป็นรูปแบบเครือข่ายที่ coordinator จะส่งสัญญาณ regular beacon เพื่อควบคุมการทำงานของโนดอื่นๆ มักจะใช้สำหรับเครือข่ายที่ต้องการการประสานเวลา (Synchronization) นอกจากนี้ ในระหว่างช่วงของสัญญาณ regular beacon สามารถกำหนดให้โนดอื่นๆเข้าสู่ภาวะ sleep เพื่อประหยัดพลังงานได้ กลไก CSMA-CA สำหรับ beacon-enabled PAN เรียกว่า slotted CSMA-CA

2) Nonbeacon-enabled PAN เป็นรูปแบบเครือข่ายที่ coordinator จะไม่มีการส่งสัญญาณ regular beacon ทำให้แต่ละโนดสามารถรับส่งข้อมูลได้อย่างอิสระ โดยใน nonbeacon-enabled PAN ทุกโนดจะพร้อมรับส่งข้อมูลตลอดเวลาโดยไม่มีการเข้าสู่ภาวะ sleep จึงสิ้นเปลืองพลังงานมากกว่ารูปแบบเครือข่าย beacon-enabled PAN อย่างไรก็ตาม nonbeacon-enabled PAN เหมาะสมสำหรับการใช้งานในเครือข่ายเซ็นเซอร์ไร้สายมากกว่า เนื่องจากในเครือข่ายเซ็นเซอร์ไร้สายส่วนใหญ่ เซ็นเซอร์โนดจะต้องตรวจวัดคุณสมบัติต่างๆ ตลอดเวลาเพื่อส่งข้อมูลไปยังปลายทาง หรืออีกกรณีหนึ่งคือเซ็นเซอร์โนดจะรายงานไปยังปลายทางเมื่อตรวจพบสถานะตามที่กำหนดไว้ เช่น อุณหภูมิสูงกว่าค่าที่กำหนด เป็นต้น ซึ่งการทำงานทั้งสองลักษณะนี้เซ็นเซอร์โนดจะต้องพร้อมรับส่งข้อมูลตลอดเวลา และการประยุกต์ใช้งานของเครือข่ายเซ็นเซอร์ไร้สายส่วนใหญ่ไม่จำเป็นต้องมีการประสานเวลา ดังนั้นงานวิจัยนี้จะเลือกศึกษา nonbeacon-enabled PAN โดยกลไก CSMA-CA สำหรับ nonbeacon-enabled PAN เรียกว่า unslotted CSMA-CA

กลไก unslotted CSMA-CA ของมาตรฐาน IEEE 802.15.4 มีขั้นตอนวิธี (Algorithm) ในการทำงานดังแสดงดังผังงานของ unslotted CSMA-CA ในรูปที่ 2.4 ซึ่งอธิบายโดยสรุปได้คือ โนดใดๆที่ต้องการส่งแพ็กเกตข้อมูล จะต้องประวิงเป็นช่วงเวลาหนึ่งก่อน โดยเรียกช่วงเวลานี้ว่า backoff period ซึ่งจะถูกกำหนดโดยค่า backoff unit ซึ่งโนดส่งจะสุ่มค่า backoff unit เป็นตัวเลขจำนวนเต็มค่าหนึ่งจากช่วง [0, 2^{BE}-1] (โดย BE คือ Backoff Exponent และ 1 backoff unit มีระยะเวลา 20 symbol หรือ 320 μs) เมื่อประวิงจนครบ backoff period แล้ว โนดส่งจะตรวจสอบสถานะของช่องสัญญาณว่าในขณะนั้นช่องสัญญาณว่าง (Idle) หรือไม่ว่าง (Busy) ซึ่งการตรวจสอบสถานะของช่องสัญญาณจะทำโดยกระบวนงาน CCA (Clear Channel Assessment) หากพบว่าช่องสัญญาณว่าง โนดก็จะส่งแพ็กเกตข้อมูลทันที แต่หากพบว่าช่องสัญญาณไม่ว่าง ค่า BE ถูกเพิ่มขึ้นอีก 1 และเริ่มดำเนินการส่งข้อมูลใหม่อีกครั้ง ดังนั้น จะเห็นว่าทุกๆครั้งที่การเข้าถึงช่องสัญญาณไม่สำเร็จ ช่วงเวลา backoff period จะมีโอกาสยาวนานขึ้น เนื่องจากพิสัยของการสุ่มค่า backoff unit จะกว้างขึ้นนั่นเอง และหากโนดส่งไม่สามารถเข้าถึงช่องสัญญาณได้เลยจากการพยายามมากกว่าจำนวนครั้งที่กำหนดโดยค่า *macMaxCSMABackoffs* จะถือว่าการเข้าถึงช่องสัญญาณครั้งนั้นล้มเหลว (Channel access failure)

ตารางที่ 2.2 พารามิเตอร์สำคัญในกลไก Unslotted CSMA-CA

พารามิเตอร์	คำอธิบาย	พิสัย	ค่าปริยาย
macMaxBE	ค่าสูงสุดของ Backoff Exponent (BE) ในขั้นตอนวิธีของ CSMA-CA	3-8	5
macMinBE	ค่าต่ำสุดของ Backoff Exponent (BE) ในขั้นตอนวิธีของ CSMA-CA	0-*macMaxBE*	3
macMaxCSMABackoffs	จำนวนครั้งสูงสุดสำหรับการ Backoff ของ CSMA-CA ในการพยายามเข้าถึงช่องสัญญาณก่อนที่จะประกาศสถานะการเข้าถึงช่องสัญญาณล้มเหลว	0-5	4



รูปที่ 2.4 ผังงานกลไก unslotted CSMA-CA สำหรับ nonbeacon-enabled PAN

การตรวจสอบสถานะช่องสัญญาณของเครือข่าย IEEE 802.15.4 จะใช้กระบวนงาน CCA (Clear Channel Assessment) ดังที่กล่าวไปแล้วข้างต้น ซึ่งในกระบวนงาน CCA โนดส่งจะตรวจสอบระดับพลังงานของสัญญาณทั้งหมดภายในช่องสัญญาณที่โนดส่งใช้งานอยู่เป็นระยะเวลา 8 symbol period ซึ่ง 1 symbol period เท่ากับ 16 μs (1 symbol เท่ากับ 4 bit ซึ่งรายละเอียดจะกล่าวถึงในหัวข้อที่ 2.2.4) โดยเงื่อนไขที่ CCA ใช้ตรวจสอบว่าช่องสัญญาณไม่ว่างจะขึ้นอยู่กับวิธี (Mode) ของ CCA ที่เลือกใช้ งาน โดยวิธีของ CCA แบ่งออกเป็น 3 วิธี ดังนี้

วิธีที่ 1: Energy above Threshold - CCA จะรายงานว่าช่องสัญญาณไม่ว่างเมื่อตรวจสอบพบระดับพลังงานที่สูงกว่าค่าที่กำหนดซึ่งเรียกค่านี้ว่า ED threshold ดังนั้น CCA จะถือ

ว่าช่องสัญญาณว่าง หากตรวจพบสัญญาณที่มีระดับพลังงานต่ำกว่าค่า ED threshold โดยไม่สนใจว่าสัญญาณนั้นจะเป็นสัญญาณที่มีรูปแบบการมอดูเลตและมีลักษณะการแผ่สเปกตรัมแบบใด โดยทั่วไปจะเรียกวิธีนี้แบบสั้นๆว่า วิธี ED

วิธีที่ 2: Carrier Sense only - CCA จะรายงานว่าช่องสัญญาณไม่ว่างก็ต่อเมื่อตรวจพบสัญญาณที่มีรูปแบบการมอดูเลตและมีลักษณะการแผ่สเปกตรัม (Spreading Characteristic) เช่นเดียวกับที่กำหนดในชั้นกายภาพ (PHY) ของอุปกรณ์นั้นๆ โดยสัญญาณที่ตรวจพบนี้จะมีพลังงานสูงกว่าหรือต่ำกว่าค่า ED threshold ก็ได้ นั่นคือในวิธีนี้ CCA จะรายงานว่าช่องสัญญาณไม่ว่างเมื่อตรวจสอบพบสัญญาณในมาตรฐาน IEEE 802.15.4 ด้วยกันเท่านั้น โดยไม่สนใจว่าสัญญาณที่ตรวจพบนี้จะมีระดับพลังงานเท่าใด โดยทั่วไปจะเรียกวิธีนี้แบบสั้นๆว่า วิธี CS

วิธีที่ 3: Carrier sense with energy above energy threshold - CCA จะรายงานว่าช่องสัญญาณไม่ว่างโดยมีเงื่อนไขดังนี้

- ตรวจพบสัญญาณที่มีรูปแบบการมอดูเลตและมีลักษณะการแผ่สเปกตรัมเช่นเดียวกับที่กำหนดในมาตรฐาน IEEE 802.15.4 และ/หรือ
- ตรวจพบระดับพลังงานที่สูงกว่าค่า ED threshold

จะเห็นว่าวิธีที่ 3 จะเป็นการรวมรูปแบบการตรวจสอบช่องสัญญาณของวิธี ED และวิธี CS เข้าด้วยกัน โดยใช้ตัวดำเนินการทางตรรกศาสตร์ AND หรือ OR

2.2.3.2 **การใช้** Frame Acknowledgement

การส่งแพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 สามารถเลือกได้ว่าจะใช้การส่งแบบต้องการสัญญาณยืนยันการได้รับข้อมูลอย่างถูกต้อง (Acknowledgement หรือ ACK) หรือไม่ โดยจะระบุอยู่ใน Acknowledgement Request subfield ของเฟรมแพ็กเกตข้อมูลที่ส่งไป ซึ่งในงานวิจัยนี้จะถือว่าการส่งแพ็กเกตข้อมูลทุกครั้งจะต้องการสัญญาณ ACK ยืนยันการได้รับข้อมูลตอบกลับมาด้วย

แพ็กเกตข้อมูลที่ต้องการสัญญาณ ACK ตอบกลับจากโนดรับจะถูกส่งโดยตั้งค่า Acknowledgement Request subfield เป็น 1 เมื่อโนดรับได้รับเฟรมแพ็กเกตข้อมูลถูกต้องสมบูรณ์แล้วก็จะสร้างเฟรม ACK ซึ่งมีค่า DSN (Data Sequence Number) เดียวกับที่ระบุอยู่ในเฟรมแพ็กเกตข้อมูล

การส่งสัญญาณ ACK โดยโนดรับจะเกิดขึ้นหลังจากได้รับ symbol สุดท้ายของเฟรมแพ็กเกตข้อมูลไปแล้วเป็นระยะเวลาเท่ากับจำนวน symbol ที่ถูกกำหนดโดยค่าพารามิเตอร์ *aTurnaroundTime* และเมื่อโนดส่งได้รับสัญญาณ ACK ภายในระยะเวลาที่กำหนดโดยพารามิเตอร์ *macAckWaitDuration* ก็จะถือว่าการส่งแพ็กเกตข้อมูลครั้งนั้นเสร็จสิ้นสมบูรณ์ แต่หากโนดส่งไม่ได้รับสัญญาณ ACK ภายในระยะเวลาที่กำหนดก็จะถือว่าการส่งแพ็กเกตข้อมูลครั้งนั้นล้มเหลว และจะดำเนินการส่งซ้ำ (Retransmission) ต่อไป

สำหรับกรณีที่การส่งแพ็กเกตข้อมูลไม่ต้องการสัญญาณ ACK ตอบกลับจากโนดรับ โนดส่งจะถือว่าการส่งแพ็กเกตข้อมูลทุกครั้งสำเร็จทั้งหมด

ตารางที่ 2.3 พารามิเตอร์สำคัญในกรณีที่ใช้ Frame Acknowledgement

พารามิเตอร์	**คำอธิบาย**	**ค่าปริยาย**
aTurnaroundTime	จำนวน symbol period สูงสุดสำหรับการเปลี่ยนโมดจากการรับเป็นการส่ง (RX-to-TX) หรือ การส่งเป็นการรับ (TX-to-RX)	12
macAckWaitDuration	จำนวน symbol period สูงสุดที่โนดส่งจะรอเฟรม Acknowledgement ภายหลังจากการส่งแพ็กเกตข้อมูลแล้วเสร็จ	ค่านี้ขึ้นอยู่กับช่องสัญญาณที่ใช้งาน ซึ่งจะส่งผลต่อพารามิเตอร์อื่นๆที่นำมาใช้ในการคำนวณค่า macAckWaitDuration ซึ่งเมื่อคำนวณแล้วจะได้ค่า macAckWaitDuration สำหรับช่องสัญญาณที่แถบความถี่ 2.4 GHZ เท่ากับ 54 (รายละเอียดการคำนวณจะไม่ขอกล่าวถึง)

2.2.3.3 **การส่งซ้ำ** (Retransmission)

การส่งซ้ำจะเกิดขึ้นเฉพาะกรณีที่การส่งแพ็กเกตข้อมูลต้องการสัญญาณ ACK ตอบกลับจากโนดรับเท่านั้น เนื่องจากการส่งแพ็กเกตข้อมูลที่ไม่ต้องการสัญญาณ ACK ตอบกลับจะถือว่า

การส่งแพ็กเกตข้อมูลสำเร็จทุกครั้ง โดยโนดส่งจะดำเนินการส่งซ้ำเมื่อโนดส่งไม่ได้รับสัญญาณ ACK หลังจากส่งแพ็กเกตข้อมูลแล้วเสร็จเป็นระยะเวลาเท่ากับจำนวน symbol period ที่กำหนดโดยพารามิเตอร์ *macAckWaitDuration* หรือเมื่อได้รับสัญญาณ ACK ที่มีค่า DSN ไม่ตรงกับค่า DSN ของแพ็กเกตข้อมูลที่ส่งไป

การส่งซ้ำจะใช้ค่า DSN เดียวกับที่ระบุในการส่งครั้งแรก และจะใช้ค่าต่างๆในกลไก CSMA-CA เสมือนเป็นการส่งแพ็กเกตข้อมูลครั้งใหม่ นั่นคือค่าพารามิเตอร์ต่างๆที่เกี่ยวข้องกับการ backoff จะเป็นค่าเริ่มแรกทั้งหมด หากการส่งซ้ำครั้งแรกยังไม่สำเร็จ หรือยังไม่ได้รับสัญญาณ ACK ตอบกลับมาภายในระยะเวลาที่กำหนด โนดส่งก็จะทำการส่งซ้ำอีกครั้งต่อไปเรื่อยๆจนกว่าจะถึงจำนวนครั้งที่กำหนดในพารามิเตอร์ *macMacFrameRetries* และเมื่อทำการส่งซ้ำจนครบจำนวนครั้งที่กำหนดใน *macMacFrameRetries* แล้ว โนดส่งก็ยังไม่ได้รับสัญญาณ ACK ตอบกลับมาก็จะถือว่าการส่งแพ็กเกตข้อมูลครั้งนั้นล้มเหลว

ตารางที่ 2.4 พารามิเตอร์สำคัญที่เกี่ยวข้องการส่งซ้ำ

พารามิเตอร์	คำอธิบาย	พิสัย	ค่าปริยาย
macMacFrameRetries	จำนวนครั้งสูงสุดของการส่งซ้ำก่อนที่จะถือว่าการส่งแพ็กเกตข้อมูลครั้งนั้นล้มเหลว	0-7	3

2.2.3.4 กระบวนการรับส่งข้อมูลในภาพรวม

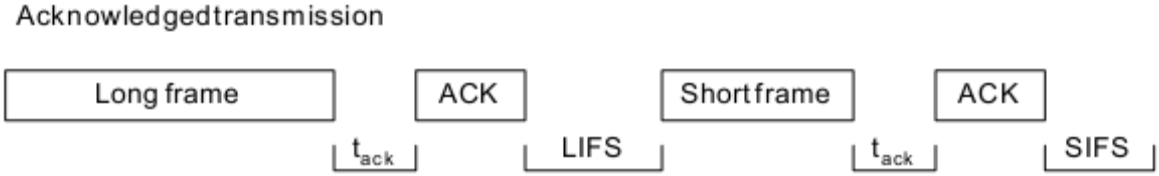
ในหัวข้อนี้จะสรุปกระบวนการการรับส่งข้อมูลในภาพรวม โดยจะอธิบายเฉพาะในส่วนที่เกี่ยวข้องกับขอบเขตของงานวิจัยนี้เท่านั้น คือจะไม่กล่าวถึงกระบวนการในการสร้างเฟรมข้อมูลหรือรูปแบบของเฟรมข้อมูล โดยจะกล่าวถึงเฉพาะกระบวนการของเครือข่าย IEEE 802.15.4 ในการรับส่งข้อมูลเมื่อโดนส่งมีแพ็กเกตข้อมูลที่พร้อมจะส่งอยู่แล้วเท่านั้น

หลักการทำงานของการรับส่งข้อมูลสำหรับเครือข่าย IEEE 802.15.4 คือ เมื่อโนดส่งมีแพ็กเกตข้อมูลที่ต้องการส่งไปยังโนดรับ โนดส่งจะต้องตรวจสอบสถานะของช่องสัญญาณโดยใช้กลไก CSMA-CA และมีเงื่อนไขการตรวจสอบว่าช่องสัญญาณว่างหรือไม่ตามวิธี CCA ที่เลือกใช้ (รายละเอียดอยู่ในหัวข้อ 2.2.3.1) หากพบว่าช่องสัญญาณว่างอยู่ โนดส่งจะทำการส่งแพ็กเกตข้อมูลนั้นทันที เมื่อโนดรับได้รับเฟรมแพ็กเกตข้อมูลครบถ้วนสมบูรณ์แล้วก็จะส่งเฟรม

Acknowledgement หรือ ACK กลับคืนไปให้โนดส่งเพื่อยืนยันการได้รับข้อมูล หากโนดส่งได้รับเฟรม ACK ดังกล่าวแล้ว ก็จะถือว่าการส่งแพ็กเกตข้อมูลนี้สำเร็จ แต่หากโนดส่งไม่ได้รับเฟรม ACK กลับมาหลังจากส่งแพ็กเกตข้อมูลเสร็จสิ้นไปแล้วเป็นระยะเวลาหนึ่ง ไม่ว่าสาเหตุที่โดนส่งไม่ได้รับสัญญาณ ACK นั้นจะมาจากการส่งเฟรมแพ็กเกตข้อมูลไม่สำเร็จตั้งแต่แรก หรือเกิดจากการส่งสัญญาณ ACK ไม่สำเร็จก็ตาม จะถือว่าการส่งครั้งนั้นไม่สำเร็จและโนดส่งจะทำการส่งซ้ำใหม่โดยเริ่มต้นใหม่ตั้งแต่การตรวจสอบสถานะของช่องสัญญาณโดยใช้กลไก CSMA-CA และหากการส่งยังไม่สำเร็จอีก โนดส่งก็จะส่งซ้ำไปเรื่อยๆจนกว่าจำนวนครั้งของการส่งซ้ำจะสูงกว่าค่าที่กำหนด โนดส่งจะหยุดการส่งซ้ำและรายงานไปยังชั้น (Layer) ที่สูงกว่าว่าการส่งแพ็กเกตข้อมูลครั้งนั้นล้มเหลว

จากกระบวนการรับส่งข้อมูลข้างต้น ยังมีอีกพารามิเตอร์หนึ่งที่สำคัญและเกี่ยวข้องอย่างยิ่งกับงานวิจัยนี้คือ Interframe spacing (IFS) โดย IFS คือ ช่วงระยะเวลาที่ MAC จำเป็นต้องใช้ในการประมวลผลข้อมูลที่ได้รับมา ดังนั้น การส่งแพ็กเกตข้อมูลติดๆกันจำเป็นต้องเว้นช่วงเวลาในการส่งแพ็กเกตข้อมูลถัดไปอย่างน้อยเท่ากับระยะเวลา IFS เช่น หากการส่งแพ็กเกตข้อมูลเป็นแบบต้องการสัญญาณ ACK โนดส่งจะสามารถส่งแพ็กเกตข้อมูลถัดไปได้ก็ต่อเมื่อได้รับสัญญาณ ACK เสร็จสิ้นเป็นระยะเวลาอย่างน้อยเท่ากับ IFS

ระยะเวลา IFS จะขึ้นอยู่กับขนาดของเฟรมข้อมูลที่เพิ่งส่งไปก่อนหน้า คือ หากเฟรมข้อมูลมีขนาดไม่เกิน *aMaxSIFSFrameSize* octet ระยะเวลา IFS จะถือเป็น SIFS (Short-interframe space) ซึ่งจะระยะเวลาเป็นจำนวน symbol ตามค่าที่กำหนดในพารามิเตอร์ *macMinSIFSPeriod* แต่หากเฟรมข้อมูลมีขนาดเกินกว่า *aMaxSIFSFrameSize* octet ระยะเวลา IFS จะถือเป็น LIFS (Long-interframe space) ซึ่งจะระยะเวลาเป็นจำนวน symbol ตามค่าที่กำหนดในพารามิเตอร์ *macMinLIFSPeriod*



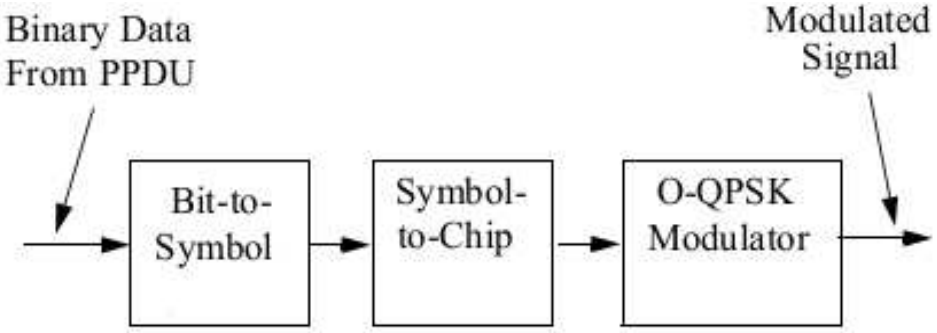
รูปที่ 2.5 รูปแบบ IFS สำหรับการส่งแพ็กเกตข้อมูลที่ต้องการ ACK

ตารางที่ 2.5 พารามิเตอร์ที่เกี่ยวข้องกับ IFS

พารามิเตอร์	คำอธิบาย	ค่าปริยาย
aMaxSIFSFrameSize	ขนาดสูงสุดของ MPDU (MAC Protocol Data Unit) เป็น octet ที่สามารถเว้นช่วงการส่งต่อเนื่องด้วยระยะเวลา SIFS	18
macMinSIFSPeriod	จำนวน symbol ที่น้อยที่สุดในการสร้างระยะเวลา SIFS	12
macMinLIFSPeriod	จำนวน symbol ที่น้อยที่สุดในการสร้างระยะเวลา LIFS	40

2.2.4 การมอดูเลตและการแผ่สเปกตรัม

เครือข่าย IEEE 802.15.4 ที่แถบความถี่ 2450 MHz จะใช้เทคนิคการมอดูเลตแบบ 16-ary quasi-orthogonal โดยใน 1 symbol จะเป็นการ map เฟรมแพ็กเกตข้อมูลมา 4 bit เพื่อนำมาเลือกว่ารูปแบบของ 4 bit นั้นๆ (ซึ่งมีได้ 16 รูปแบบ) ตรงกับ orthogonal pseudo-random noise (PN) sequence ใด และจะทำเช่นนี้สำหรับทุกๆ symbol ของเฟรมแพ็กเกตข้อมูล จากนั้น PN sequence หรือ chip sequence ดังกล่าวจะถูกมอดูเลตลงบนคลื่นพาห์โดยใช้การมอดูเลตแบบ Offset Quadrature Phase-Shift Keying (O-QPSK)



รูปที่ 2.6 แผนภาพบล็อกการมอดูเลตและการแผ่สเปกตรัม

จากขั้นตอนการมอดูเลตที่ได้อธิบายไปข้างต้น สามารถสรุปได้เป็น 3 ขั้นตอนดั งแสดงในรูปที่ 2.6 ซึ่งอธิบายได้ ดังนี้

1. Bit-to-Symbol เป็นขั้นตอนการแปลงข้อมูลไบนารีในเฟรมแพ็กเกตข้อมูลให้เป็น symbol โดยใน 1 octet จะถูก map เป็น 2 symbol คือ 4 LSBs (b_0, b_1, b_2, b_3) เป็น 1 symbol และ 4 MSBs (b_4, b_5, b_6, b_7) เป็นอีก 1 symbol

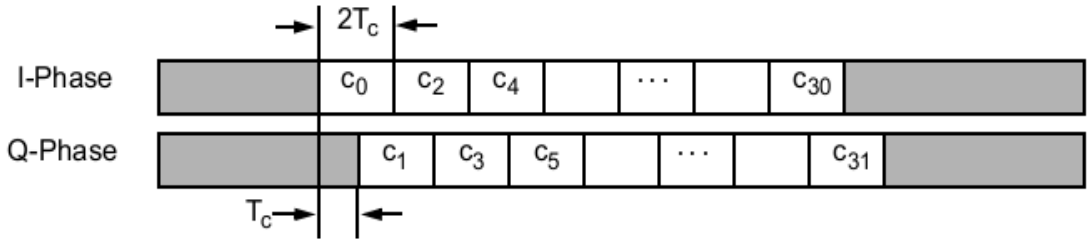
2. Symbol-to-Chip ขั้นตอนนี้จะเป็นการ map symbol ที่มีขนาด 4 bit ให้เป็น 32-chip PN sequence ตามที่กำหนด ดังแสดงในตารางที่ 2.6

ตารางที่ 2.6 Symbol-to-chip mapping

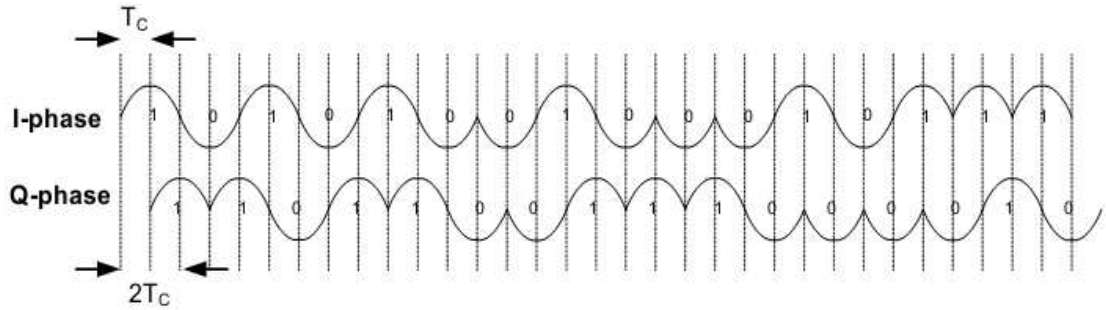
Data symbol (ฐานสิบ)	Data symbol (ไบนารี) (b_0 b_1 b_2 b_3)	Chip values (c_0 c_1 … c_{30} c_{31})
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

3. การมอดูเลตแบบ O-QPSK เป็นขั้นตอนการนำ chip sequence มามอดูเลตลงบนคลื่นพาห์โดยใช้การมอดูเลตแบบ O-QPSK ด้วยรูปร่างครึ่งหนึ่งของคลื่นไซน์ โดย chip ที่มี index เป็นเลขคู่จะถูกมอดูเลตลงบนคลื่นพาห์ in-phase (I) ขณะที่ chip ที่มี index เป็นเลขคี่จะถูกมอดูเลตลงบนคลื่นพาห์ quadrature-phase (Q) และเนื่องจากข้อมูล 1 symbol ถูกแทนด้วย 32-chip sequence ดังนั้น chip rate จะมีอัตราสูงกว่า symbol rate อยู่ 32 เท่า (symbol rate 62.5 ksymbol/s, chip rate 2.0 Mchip/s) คลื่นพาห์ I-phase และ Q-phase จะมีมุมที่ offset กันอยู่ โดย Q-phase จะช้ากว่า I-Phase อยู่เป็นเวลา T_c โดย T_c จะเป็นส่วนกลับของ chip rate หรือก็คือคาบของ 1 chip นั่นเอง

หลังจากนั้น สัญญาณพาห์ I-phase และ Q-phase จะถูกนำมารวมเป็นสัญญาณเดียวกันและส่งออกไปตามลำดับ chip sequence คือ c_0 จะถูกส่งก่อนเป็นลำดับแรก และ c_{31} จะถูกส่งเป็นลำดับสุดท้าย



รูปที่ 2.7 Chip offset ของ O-QPSK



รูปที่ 2.8 ตัวอย่างรูปคลื่น baseband chip sequence

2.2.5 การตรวจสอบความผิดพลาดของแพ็กเกตข้อมูล

การตรวจสอบความผิดพลาดสำหรับเครือข่าย IEEE 802.15.4 จะใช้กลไก 16-bit Frame Check Sequence (FCS) Cyclic Redundancy Check (CRC) ของ ITU-T ในการตรวจสอบความผิดพลาดของทุกเฟรมข้อมูล ซึ่งในแต่ละเฟรมข้อมูลจะมี FCS field ขนาด 2 octet อยู่ใน MAC payload

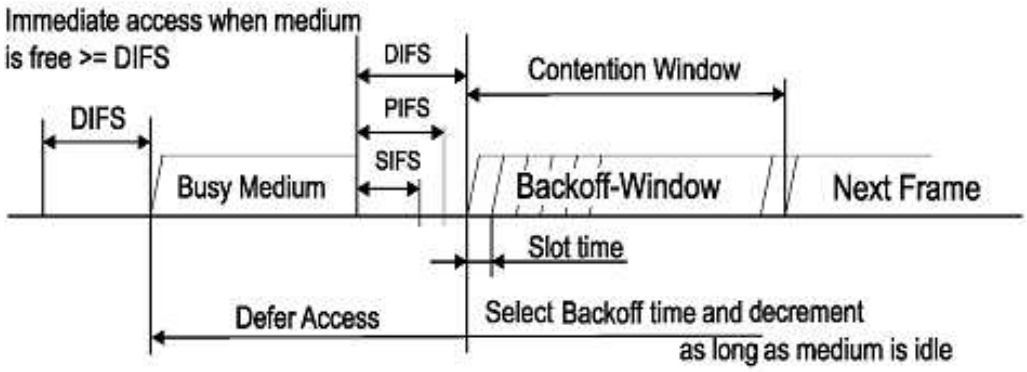
สำหรับการกู้คืนข้อมูลจากความผิดพลาดนั้น มาตรฐาน IEEE 802.15.4 ไม่ได้ระบุถึงความสามารถดังกล่าวไว้ ดังนั้น ในงานวิจัยนี้จึงถือว่าเครือข่าย IEEE 802.15.4 ไม่มีความสามารถในการกู้คืนข้อมูลที่ผิดพลาดหรือเสียหาย

2.3 หลักการทำงานของเครือข่าย IEEE 802.11b/g - [3]

มาตรฐาน IEEE 802.11 เป็นชุดของมาตรฐานสำหรับเครือข่ายพื้นที่ท้องถิ่นไร้สาย ซึ่งยังแบ่งได้อีกเป็นหลายโพรโทคอลย่อยตามเทคนิคการแผ่สเปกตรัมและแถบความถี่ที่ใช้งาน โดยโพรโทคอลที่เป็นที่นิยมใช้งานกันมากที่สุดคือ IEEE 802.11b และ IEEE 802.11g ซึ่งทำงานบนแถบความถี่ 2.4 GHz ซึ่งทั้งเครือข่าย IEEE 802.11b และ IEEE 802.11g จะมีการแบ่งช่องสัญญาณที่เหมือนกัน (ดังรูปที่ 2.1) และมีการใช้กลไก CSMA-CA ในการควบคุมการเข้าถึงช่องสัญญาณที่มีขั้นตอนวิธีเหมือนกัน แต่จะแตกต่างกันที่พารามิเตอร์ในกลไก CSMA-CA ของมาตรฐาน IEEE 802.11g จะมีช่วงเวลา backoff สั้นกว่า

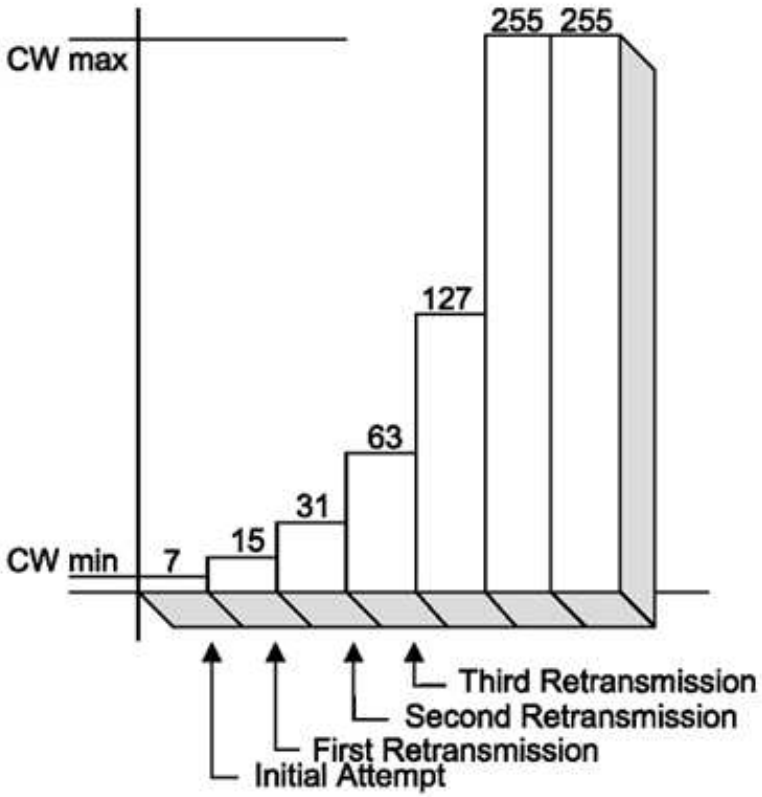
กล่าวโดยสรุปแล้ว มาตรฐาน IEEE 802.11g เป็นส่วนขยายที่พัฒนาเพิ่มเติมจากมาตรฐาน IEEE 802.11b เพื่อรองรับอัตราข้อมูลที่สูงขึ้น ในขณะที่กระบวนการรับส่งข้อมูลยังคงเป็นรูปแบบเดียวกัน เพียงแต่ค่าของพารามิเตอร์ต่างๆของทั้งสองโพรโทคอลนี้อาจจะแตกต่างกันอยู่บ้าง ซึ่งงานวิจัยนี้จะเลือกใช้ค่าพารามิเตอร์จากมาตรฐาน IEEE 802.11b เป็นหลัก

ดังนั้น การอธิบายหลักการทำงานในการรับส่งข้อมูลของเครือข่าย IEEE 802.11b/g ในหัวข้อนี้จะอ้างอิงค่าพารามิเตอร์จากมาตรฐาน IEEE 802.11b แต่กระบวนการรับส่งข้อมูลก็ยังถือว่าเป็นรูปแบบเดียวกัน ซึ่งในงานวิจัยนี้จะเลือกศึกษารูปแบบ Basic access เท่านั้น เนื่องจากวัตถุประสงค์ของงานวิจัยนี้จะเน้นไปที่การปรับปรุงการทำงานของ IEEE 802.15.4 เป็นหลัก จึงจะไม่ลงรายละเอียดในการทำงานของเครือข่าย IEEE 802.11b/g มากนัก รูปแบบการทำงานของ Basic access สำหรับเครือข่าย IEEE 802.11b/g แสดงดังรูปที่ 2.9



รูปที่ 2.9 รูปแบบ Basic Access เครือข่าย ของ IEEE 802.11b/g

จากรูปที่ 2.9 สามารถสรุปการทำงานได้ดังนี้ โนดส่งที่ต้องการส่งแพ็กเกตข้อมูล จะเริ่มต้นโดยการตรวจสอบสถานะของช่องสัญญาณก่อน โดยช่องสัญญาณจะต้องว่าง (idle) ติดต่อกันเป็นระยะเวลาหนึ่ง เรียกระยะเวลานี้ว่า DIFS (DCF Interframe Space) ซึ่งเท่ากับ 50 μs หากช่องสัญญาณว่างเป็นระยะเวลามากกว่าหรือเท่ากับระยะเวลา DIFS แล้ว โนดส่งจะตั้งค่า backoff time ซึ่งกำหนดโดยการสุ่มค่า backoff unit หรือจำนวน slot ของการ backoff จากช่วง [0, CW] โดย CW คือ *Contention Window* และ 1 backoff unit จะเท่ากับระยะเวลา 20 μs ค่า backoff time นี้จะลดลงเรื่อยๆตราบที่ช่องสัญญาณยังคงว่างอยู่ และจะหยุดการลดลงเมื่อช่องสัญญาณถูกพบว่าไม่ว่าง โดยจะเริ่มลดลงใหม่ต่อจากค่าเดิมเมื่อช่องสัญญาณว่างเป็นระยะเวลา DIFS อีกครั้ง เมื่อ backoff time ลดลงเหลือ 0 โนดส่งจึงจะเริ่มต้นส่งแพ็กเกตข้อมูล ซึ่งหากส่งสำเร็จโนดปลายทางจะส่งเฟรม Acknowledgement (ACK) กลับมา แต่หากโนดต้นทางไม่ได้รับสัญญาณ ACK กลับมาภายในระยะเวลาที่กำหนด (ประมาณ 222 μs) จะถือว่าการส่งไม่สำเร็จ และโนดส่งจะทำการส่งซ้ำ โดยเริ่มต้นกลไก CSMA-CA ใหม่ ซึ่งในการส่งซ้ำนั้น *Contention Window* จะมีขนาดเพิ่มขึ้นอีกประมาณเท่าตัว ดังแสดงในรูปที่ 2.10



รูปที่ 2.10 การเพิ่มขึ้นของ Contention Window ตามจำนวนครั้งของการส่งซ้ำ

สำหรับการตรวจสอบสถานะของช่องสัญญาณ เครือข่าย IEEE 802.11b/g ก็ยังคงใช้กระบวนงาน CCA เช่นเดียวกับเครือข่าย IEEE 802.15.4 โดยมาตรฐาน IEEE 802.11b กำหนดวิธี CCA ไว้ 3 วิธี ซึ่งมีรูปแบบเดียวกับเครือข่าย IEEE 802.15..4 (รายละเอียดอยู่ในหัวข้อที่ 2.2.3.1) ในขณะที่มาตรฐาน IEEE 802.11g ก็กำหนดวิธี CCA ไว้ 3 วิธีเช่นกัน โดยวิธี CCA สำหรับมาตรฐาน IEEE 802.11g จะมีข้อแตกต่างจากมาตรฐาน IEEE 802.11b เล็กน้อย ตรงที่วิธี CS ในมาตรฐาน IEEE 802.11g จะมีการกำหนดตัวจับเวลา (Timer) มาเกี่ยวข้องด้วย

2.4 ผลกระทบจากการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับ IEEE 802.11b/g

จากรายละเอียดข้างต้นทั้งหมด สามารถสรุปได้ว่า หากเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ใช้งานช่องสัญญาณที่มีความถี่ซ้อนทับกับช่องสัญญาณของ IEEE 802.11b/g จะเกิดการแทรกสอดกันระหว่างสัญญาณของทั้ง 2 ระบบ โดยการแทรกสอดดังกล่าวอาจส่งผลให้สมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายลดลง ทั้งนี้อาจประเมินสมรรถนะที่ลดลงเป็นการสูญเสีย (Loss) ซึ่งงานวิจัย [6] ได้แบ่งประเภทของการสูญเสียดังกล่าวเป็น 2 ประเภท คือ

1. การสูญเสียจากการไม่สามารถเข้าถึงตัวกลาง (Inhibition Loss) เป็นการสูญเสียที่เกิดจากโนดที่ต้องการส่งแพ็กเกตข้อมูลไม่สามารถเข้าถึงช่องสัญญาณได้ เนื่องจากมีทราฟฟิก IEEE 802.11b/g ใช้งานช่องสัญญาณอยู่ การสูญเสียประเภทนี้จะเกิดขึ้นเมื่อเลือกใช้ CCA วิธีที่ 1 (ED) โดยหากทราฟฟิก IEEE802.11b/g มีความหนาแน่นสูงมาก การสูญเสียจะยิ่งมากขึ้น เนื่องจากกลไก CSMA-CA ของ IEEE 802.15.4 กำหนดให้ backoff period มีโอกาสยาวนานขึ้น ทุกๆครั้งที่ตรวจพบว่าช่องสัญญาณไม่ว่าง การสูญเสียประเภทนี้ถือว่าเป็นการสูญเสียในชั้น MAC

2. การสูญเสียจากการชนกันของแพ็กเกตข้อมูล (Collision Loss) เป็นการสูญเสียที่มักจะเกิดขึ้นเมื่อเลือกใช้ CCA วิธีที่ 2 (CS) หรือวิธีที่ 3 เนื่องจากโนดใดๆที่ต้องการส่งข้อมูล จะตรวจสอบเพียงทราฟฟิก IEEE 802.15.4 เท่านั้น จึงมีโอกาสที่แพ็กเกตข้อมูลจากโนดส่งหรือเซ็นเซอร์โนดจะชนกับแพ็กเกตข้อมูลจากเครือข่าย IEEE 802.11b/g ทำให้แพ็กเกตข้อมูลของเซ็นเซอร์โนดเสียหายหรือเกิดความผิดพลาด (Packet Error) ขึ้น ส่งผลให้ต้องทำการส่งซ้ำ (Retransmission) ซึ่งนอกจากจะทำให้เสียเวลาแล้วยังทำให้สิ้นเปลืองพลังงานและอาจทำให้ข้อมูลบางส่วนสูญหายได้ การสูญเสียประเภทนี้ถือว่าเป็นการสูญเสียในชั้น PHY

2.5 งานวิจัยที่เกี่ยวข้อง

ดังที่ได้กล่าวไปแล้วข้างต้นแล้วว่าเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ซึ่งทำงานบนแถบความถี่ 2.4 GHz มีโอกาสเกิดการแทรกสอดกับเทคโนโลยีอื่นๆที่ทำงานบนแถบความถี่ 2.4 GHz เช่นกัน โดยเฉพาะเทคโนโลยีบนมาตรฐาน IEEE 802.11b/g เช่น Wi-Fi ซึ่งเป็นที่นิยมใช้งานกันอย่างแพร่หลาย ซึ่งการแทรกสอดดังกล่าวมีโอกาสส่งผลให้สมรรถนะของเครือข่ายเซ็นเซอร์ไร้สายลดลงอย่างมาก ทำให้การประยุกต์ใช้งานต่างๆของเครือข่ายเซ็นเซอร์ไร้สายอาจทำงานผิดพลาดได้ จากการศึกษางานวิจัยอื่นๆที่เกี่ยวข้อง จึงพอสรุปได้ว่าแนวทางในการปรับปรุงการทำงานของเครือข่าย IEEE 802.15.4 เพื่อแก้ปัญหาการแทรกสอดกับเครือข่าย IEEE 802.11b/g สามารถแบ่งได้เป็น 2 แนวทาง คือ การแก้ปัญหาบนพื้นฐานของการย้ายช่องสัญญาณของเครือข่าย IEEE 802.15.4 และการแก้ปัญหาบนพื้นฐานของการปรับเปลี่ยน ED threshold ในการทำ CCA

2.5.1 แนวทางการแก้ปัญหาการแทรกสอดระหว่าง IEEE 802.15.4 กับ IEEE 802.11b/g บนพื้นฐานของการย้ายช่องสัญญาณของเครือข่าย IEEE 802.15.4

2.5.1.1 Frequency Agility - [7], [8]

Zigbee specification [7] เสนอแนวทางการแก้ปัญหาการแทรกสอดระหว่าง IEEE 802.15.4 กับ IEEE 802.11b/g โดยใช้วิธีที่เรียกว่า Frequency Agility โดยในเครือข่าย Zigbee หนึ่ง จะมีอุปกรณ์ตัวหนึ่งทำหน้าที่เป็น Network Channel Manager ซึ่งโดยปกติ Network Channel Manager จะเป็น coordinator เว้นแต่จะมีการกำหนดอุปกรณ์ตัวอื่นให้เป็น Network Channel Manager แทน

ในวิธี Frequency Agility ของ Zigbee อุปกรณ์ที่เป็น router หรือ coordinator จะมีการติดตามการส่งข้อมูลล้มเหลว โดยจะมีการเก็บค่าจำนวนครั้งของการส่งข้อมูลล้มเหลวและจำนวนครั้งของการส่งข้อมูลทั้งหมดไว้ใน neighbor table เมื่อใดที่จำนวนครั้งของการส่งข้อมูลทั้งหมดมากกว่า 20 ครั้ง และการส่งข้อมูลล้มเหลวสูงกว่า 25% จะถือว่าตรวจพบการแทรกสอดที่อุปกรณ์นั้น และอุปกรณ์ดังกล่าวจะต้องทำตามขั้นตอน ดังนี้

1. ทำ energy scan ในทุกๆช่องสัญญาณ หากพบว่าพลังงานในช่องสัญญาณที่ใช้งานอยู่ไม่สูงกว่าพลังงานในช่องสัญญาณอื่นๆ จะไม่มีการดำเนินการอะไรต่อ

2. หากพบว่าพลังงานในช่องสัญญาณที่ใช้งานอยู่สูงกว่าช่องสัญญาณอื่นๆ อุปกรณ์นั้นจะส่งข่าวสารว่าตรวจพบการแทรกสอดแจ้งไปยัง Network Channel Manager และเมื่อได้รับสัญญาณ ACK กลับมาจาก Network Channel Manager อุปกรณ์นั้นจะตั้งค่าจำนวนครั้งของการส่งข้อมูลล้มเหลวและจำนวนครั้งของการส่งข้อมูลทั้งหมดกลับไปเป็นศูนย์ใหม่

3. เพื่อหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นต่อเครือข่ายทั้งหมด อุปกรณ์ที่ตรวจพบการแทรกสอดจะแจ้งข่าวสารการตรวจพบการแทรกสอดไปยัง Network Channel Manager ได้ไม่เกิน 4 ครั้งต่อชั่วโมง

เมื่อ Network Channel Manager ได้รับข่าวสารแจ้งการตรวจพบการแทรกสอดจากอุปกรณ์ใดๆในเครือข่ายแล้ว Network Channel Manager จะต้องประเมินว่าจำเป็นต้องย้ายช่องสัญญาณของเครือข่ายหรือไม่ โดยกลไกที่ Network Channel Manager จะใช้ในการตัดสินใจว่าควรย้ายช่องสัญญาณหรือไม่นั้น ผู้นำไปใช้งาน (Implementer) จะเป็นผู้กำหนด

งานวิจัย [8] เสนอการปรับปรุงแบบแผน Frequency Agility สำหรับ Zigbee เพื่อตรวจจับการเกิดการแทรกสอดและย้ายช่องสัญญาณไปยังช่องสัญญาณที่ไม่มีการแทรกสอดให้มีเหมาะสมยิ่งขึ้น โดยจะแบ่งการทำงานเป็น 2 ขั้นตอน คือ การตรวจจับการแทรกสอด (Interference Detection) และการหลีกเลี่ยงการแทรกสอด (Interference Avoidance)

- แบบแผนการตรวจจับการแทรกสอด

วิธีนี้ตรวจจับการเกิดการแทรกสอดโดยใช้แบบแผนการตรวจจับการแทรกสอดแบบ NACK (NACK-based Interference Detection scheme) นั่นคือโนดใดที่ส่งแพ็กเกตข้อมูลไปแล้ว จะตรวจสอบสัญญาณตอบรับ (Acknowledgement, ACK) หากไม่ได้รับสัญญาณ ACK ภายในระยะเวลาที่กำหนด ตัวนับ NACK (NACK counter) จะนับขึ้นทีละ 1 และโนดจะดำเนินการส่งข้อมูลใหม่อีกครั้ง หาก NACK counter มีค่าเกินกว่าค่า threshold ที่กำหนด โนดจะหยุดการส่งใหม่และเรียกใช้งานฟังก์ชั่น Energy Detection (ED) scan เพื่อตรวจสอบระดับพลังงานในขณะนั้น เพื่อให้มั่นใจว่าการแทรกสอดจากสัญญาณจากมาตรฐานอื่นเป็นสาเหตุที่ทำให้การส่งข้อมูลล้มเหลวจริงๆ โดยหากค่า Receive Signal Strength Indicator (RSSI) ที่ได้จากการทำ ED scan มีค่าสูงกว่าค่า threshold ที่กำหนด จะถือว่าเกิดการแทรกสอดขึ้น และโนดนั้นๆ จะรายงานไปยัง coordinator จากนั้น coordinator จะเรียกใช้แบบแผนการหลีกเลี่ยงการแทรกสอด (Interference Avoidance scheme) เพื่อย้ายช่องสัญญาณไปยังช่องสัญญาณที่ปลอดภัยจากการแทรกสอดต่อไป ซึ่งแบบแผนการตรวจจับการแทรกสอดนี้สามารถดำเนินการได้พร้อมๆกับการส่งแพ็กเกตข้อมูลปกติ จึงมีความเรียบง่ายและไม่เพิ่ม overhead ให้กับระบบ ผังงานของแบบแผนการตรวจจับการแทรกสอดแสดงในรูปที่ 2.11

- แบบแผนการหลีกเลี่ยงการแทรกสอด

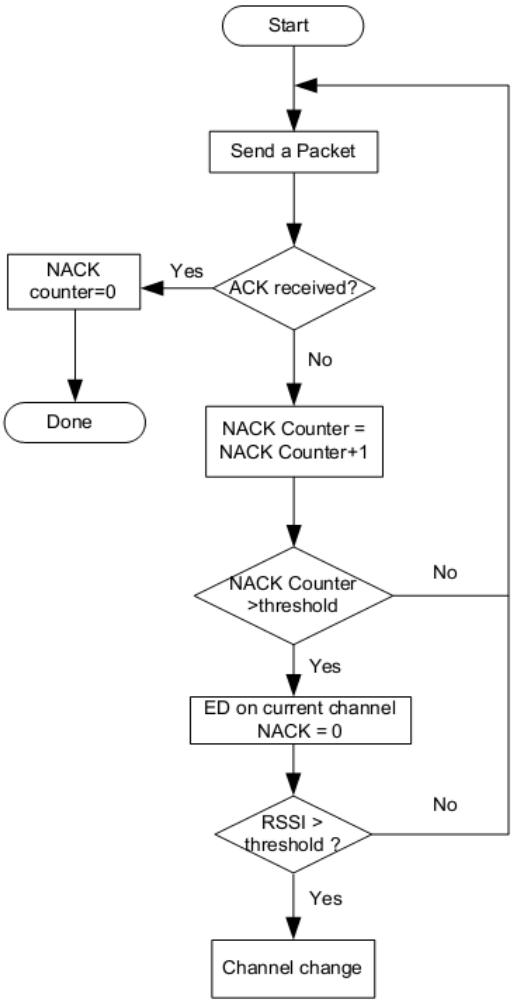
หลังจาก coordinator ได้รับรายงานตรวจพบการแทรกสอด ก็จะเรียกใช้แบบแผนการหลีกเลี่ยงการแทรกสอดทันที ซึ่งแบบแผนนี้ใช้สำหรับย้ายช่องสัญญาณไปยังช่องสัญญาณอื่นที่ไม่มีการแทรกสอด ในการเลือกช่องสัญญาณใหม่นั้น งานวิจัย [8] เสนอให้แบ่งช่องสัญญาณทั้ง 16 ช่องออกเป็น 3 คลาส โดยแบ่งตามค่า offset frequency ซึ่งก็คือระยะห่างระหว่าง center frequency ของช่องสัญญาณของเครือข่าย IEEE 802.15.4 กับ center frequency ของช่องสัญญาณที่ 1, 6 และ11 ของเครือข่าย IEEE 802.11b ดังนี้

คลาส 1 ประกอบด้วยช่องสัญญาณที่ 15, 20, 25, 26 ซึ่งเป็นช่องสัญญาณที่มี offset frequency มากกว่า 12 MHz

คลาส 2 ประกอบด้วยช่องสัญญาณที่ 11, 14, 16, 19, 21, 24 ซึ่งเป็นช่องสัญญาณที่มี offset frequency อยู่ระหว่าง 7-12 MHz

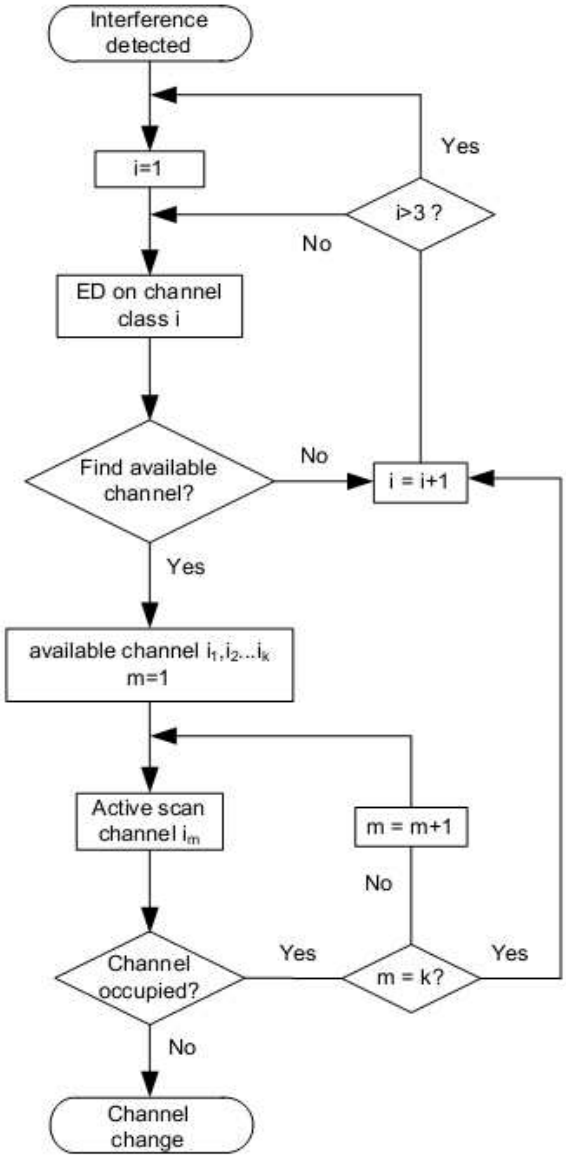
คลาส 3 ประกอบด้วยช่องสัญญาณที่ 12, 13, 17, 18, 22, 23 ซึ่งเป็นช่องสัญญาณที่มี offset frequency น้อยกว่า 3 MHz

ช่องสัญญาณในคลาส 1 จะได้รับผลกระทบจากการแทรกสอดของ IEEE 802.11b น้อยที่สุดเนื่องจากเป็นช่องสัญญาณที่อยู่ห่างจาก center frequency ของช่องสัญญาณที่ 1, 6 และ 11 ของ IEEE 802.11b มากที่สุด ในทางตรงกันข้าม ช่องสัญญาณในคลาส 3 จะได้รับผลกระทบจากการแทรกสอดของ IEEE 802.11b มากที่สุด เนื่องจากอยู่ใกล้กับ center frequency ของช่องสัญญาณที่ 1, 6 และ 11 ของ IEEE 802.11b มากที่สุดนั่นเอง (พิจารณารูปที่ 2.1 ประกอบ)



รูปที่ 2.11 ผังงานแสดงขั้นตอนการตรวจจับการแทรกสอดของงานวิจัย [8]

เมื่อ coordinator ได้รับแจ้งการเกิดการแทรกสอด coordinator จะส่งคำร้องขอ (request) ให้ router ทุกตัวในเครือข่ายเรียกใช้งานฟังก์ชั่น ED scan โดยเริ่มทำ ED scan จากช่องสัญญาณในคลาส 1 ไปจนถึงคลาส 3 ตามลำดับ จนกว่าจะเจอช่องสัญญาณที่ว่าง จากนั้น router ทุกตัวจะทำ Active scan ในช่องสัญญาณที่ coordinator เสนอมาเพื่อตรวจสอบว่ามีเครือข่าย PAN อื่นๆ ใช้งานช่องสัญญาณนั้นอยู่หรือไม่ หากพบว่ามี PAN Identifier (PAN ID) อื่นใช้ช่องสัญญาณนั้นอยู่ coordinator จะเลือกช่องสัญญาณอื่นต่อไป ผังงานของแบบแผนการหลีกเลี่ยงการแทรกสอดแสดงในรูปที่ 2.12



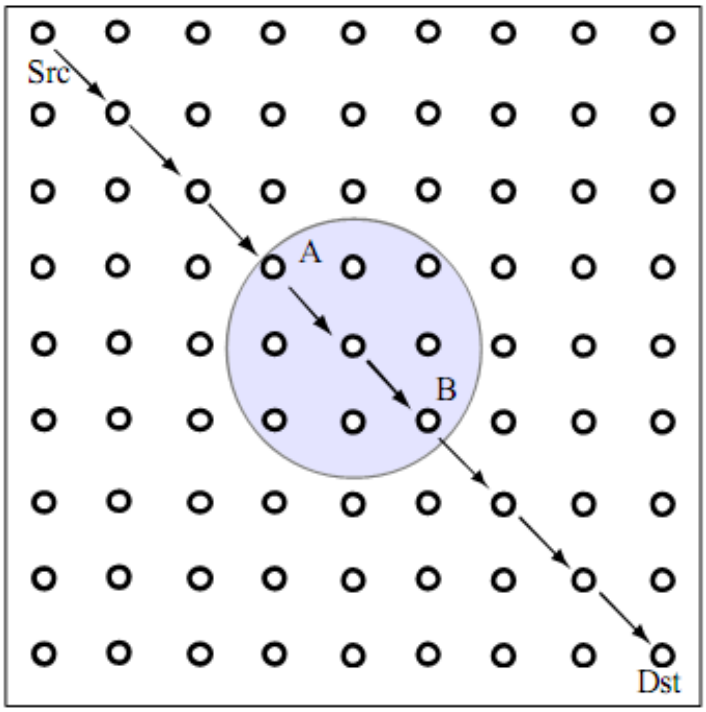
รูปที่ 2.12 ผังงานแสดงขั้นตอนการหลีกเลี่ยงการแทรกสอดของงานวิจัย [8]

2.5.1.2 Adaptive Radio Channel Allocation – [9]

งานวิจัย [9] ใช้วิธีย้ายช่องสัญญาณเพื่อหลีกเลี่ยงการแทรกสอดเช่นเดียวกัน แต่มีรูปแบบและวิธีในการตรวจจับการแทรกสอดและการหลีกเลี่ยงการแทรกสอดต่างจากวิธี Frequency Agility โดยการหลีกเลี่ยงการแทรกสอดในงานวิจัย [9] จะเลือกย้ายช่องสัญญาณเฉพาะโนดที่ได้รับผลกระทบจากการแทรกสอดเท่านั้น ในการตรวจจับการแทรกสอด งานวิจัย [9] เสนอให้ใช้การทำ ED scan หรือใช้ CCA (Clear Channel Assessment) ซึ่งเป็น service ในชั้น PHY ของ IEEE 802.15.4 เพื่อวัดค่า RSSI โดยอาจเรียกใช้การตรวจสอบค่า RSSI นี้ตามกำหนดเวลาหรือเรียกใช้ตามความต้องการ เช่น เมื่อแอปพลิเคชันที่ใช้งานอยู่ตรวจสอบพบว่า throughput ของระบบลดลงมากอย่างทันทีทันใด เป็นต้น ซึ่งหากค่า RSSI ที่วัดได้มีค่าสูงกว่าค่า threshold ก็จะถือว่าเกิดการแทรกสอดที่ช่องสัญญาณนั้น

ทุกโนดที่ตรวจพบการแทรกสอดจะสร้าง Group Formation (GF) ขึ้นมาโดย GF เป็นกลุ่มของโนดที่ตรวจพบการแทรกสอด จากนั้นทุกโนดใน GF จะย้ายช่องสัญญาณไปยังช่องสัญญาณอื่นโดยใช้ข้อมูลจาก Switching Table (SWTB) เพื่อให้มั่นใจว่าทุกโนดใน GF จะย้ายไปยังช่องสัญญาณเดียวกัน หลังจากนั้นทุกโนดใน GF จะส่ง GF message เพื่อแจ้งให้ neighbor ของตนทราบว่าได้ย้ายช่องสัญญาณไปยังช่องสัญญาณใหม่แล้ว โนดใดๆที่ได้รับ GF Message ก็จะตัดสินว่าตนเองเป็น Border node หรือไม่ ซึ่งโนดที่จะเป็น Border Node ได้นั้นจะต้องไม่ตรวจพบการแทรกสอด โนดใดที่ตัดสินว่าตนเองเป็น Border Node ก็จะส่ง GF Reply message กลับไปยังโนดที่ส่ง GF message มาให้ โดยส่งผ่านทางช่องสัญญาณใหม่ เพื่อยืนยันการสร้าง Border node

Border Node (โนด A และ B ในรูปที่ 2.13) จะเป็นโนดที่คอยสลับช่องสัญญาณเพื่อรับส่งข้อมูลระหว่างโนดที่อยู่ภายใน GF (พื้นที่วงกลมสีฟ้าในรูปที่ 2.13) กับโนดที่อยู่ภายนอก GF ดังนั้น Border Node จะต้องสร้างตารางเวลา (Schedule) สำหรับจัดสรรการใช้งานของช่องสัญญาณ ซึ่ง Border Node จะเก็บข้อมูลช่องสัญญาณที่ neighbor ของตนใช้อยู่ไว้ใน Neighbor Table (NTAB) เพื่อให้ทราบว่าจะต้อง “ฟัง” และ “พูด” กับ neighbor โนดใดที่ช่องสัญญาณใด

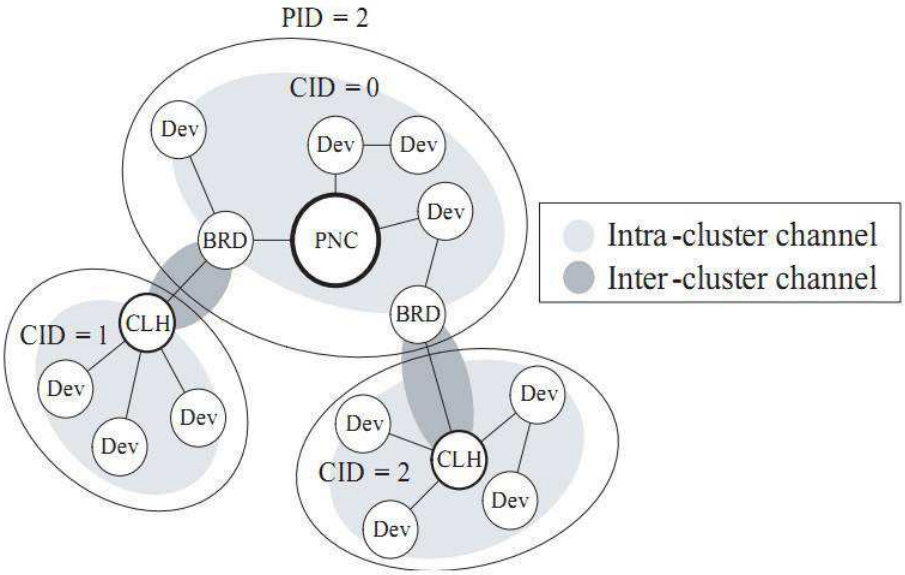


รูปที่ 2.13 แผนภาพแสดงการส่งข้อมูลผ่านกลุ่มโนดที่ตรวจพบการแทรกสอด

ทุกโนดใน GF จะคอยตรวจสอบการแทรกสอดที่ช่องสัญญาณเดิมเป็นระยะ โดยจะทราบช่องสัญญาณเดิมจากข้อมูลใน SWTB หากโนดใดไม่พบการแทรกสอดในช่องสัญญาณเดิมและมี neighbor เป็น Border Node โนดนั้นๆจะส่ง TD (Tear-down) message ไปยัง neighbor ทุกตัว รวมทั้งที่เป็น Border Node ด้วย โดย Border Node ใดๆที่ได้รับ TD message จะออกจากการเป็น Border Node ทันที ส่วนโนดอื่นๆที่ได้รับ TD Message จะพิจารณาสภาวะการแทรกสอดที่ช่องสัญญาณเดิมของตน เพื่อตัดสินใจว่าจะส่ง TD message ให้กับ neighbor ต่อไป หรือจะส่ง TD Reply message กลับไปให้กับโนดที่ส่ง TD message มาให้กับตน โดยการส่ง TD Reply message กลับไปให้โนดต้นทางนั้นเพื่อเป็นการแจ้งว่าช่องสัญญาณเดิมยังพบการแทรกสอดอยู่ และร้องขอให้โนดต้นทางเป็น Border Node ต่อไป ด้วยกลไก Tear-down เช่นนี้ หากการแทรกสอดลดลงหรือหายไปจนโนดทุกโนดไม่ตรวจพบการแทรกสอดอีก ทุกโนดใน GF จะกลับไปใช้ช่องสัญญาณเดิมทั้งหมด และ GF จะสลายไป

2.5.1.3 Adaptive Interference-Aware Multi-Channel Clustering Algorithm – [10]

งานวิจัย [10] นำเสนอแบบแผนการหลีกเลี่ยงการแทรกสอดสำหรับเครือข่าย Zigbee ที่ใช้ทอพอโลยีแบบ cluster-tree ดังตัวอย่างในรูปที่ 2.14

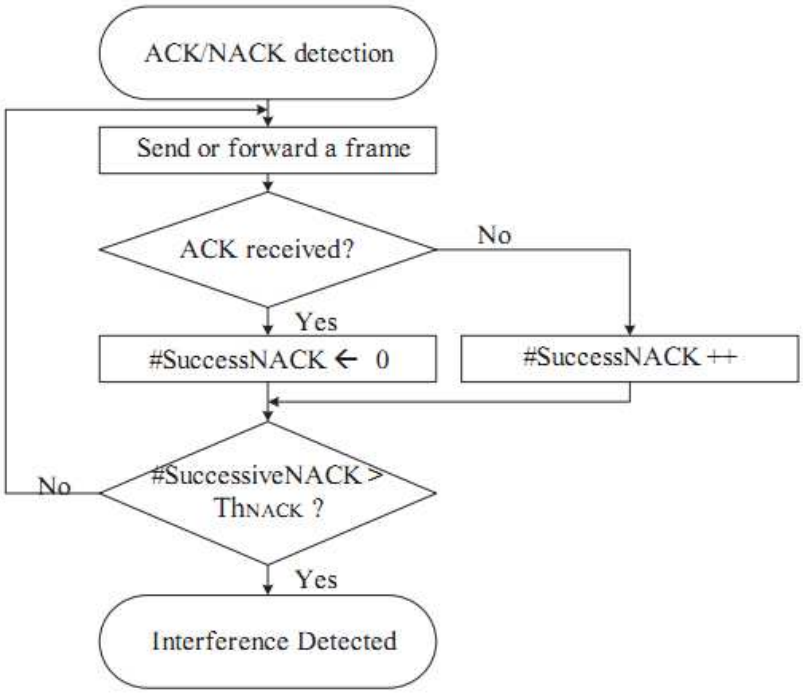


รูปที่ 2.14 ตัวอย่างเครือข่าย cluster-tree ของ Zigbee

จากรูปที่ 2.14 PAN Coordinator (PNC) เป็น coordinator ของเครือข่ายใหญ่ทั้งหมด โดยในเครือข่าย PAN ใดๆจะมี PAN Identifier (PID) ที่ไม่ซ้ำกันกับเครือข่าย PAN อื่นๆ สำหรับทอพอโลยีแบบ cluster-tree นั้น อุปกรณ์หรือโนด (Device, DEV) ในเครือข่ายจะอยู่ด้วยกันเป็นกลุ่มๆ เรียกว่า cluster โดยมี Cluster Head (CLH) ทำหน้าที่ควบคุม cluster หรืออาจเรียกได้ว่า CLH เป็น coordinator ท้องถิ่นของ cluster นั้นๆ โดยมี Cluster Identifier (CID) สำหรับระบุว่า DEV นั้นๆอยู่ใน cluster ใด และกำหนดให้ Bridge Device (BRD) คือโนดใน cluster ที่สามารถสื่อสารโดยตรงกับ CLH ของ cluster ใกล้เคียง งานวิจัย [10] กำหนดให้แบ่งช่องสัญญาณของ cluster-tree Zigbee เป็น 2 ชนิด คือ intra-cluster channel (พื้นที่สีอ่อนในรูปที่ 2.14) และ inter-cluster channel (พื้นที่สีเข้มในรูปที่ 2.14) นอกจากนี้ยังกำหนดให้กลุ่มช่องสัญญาณ (Channel Group) คือ กลุ่มของโนดที่ใช้ช่องสัญญาณเดียวกัน เช่น โนดทั้งหมดใน cluster เดียวกันหรือคู่ของ CLH กับ BRD จะถือว่าอยู่ใน Channel Group เดียวกัน ดังนั้น BRD และ CLH ใดๆ อาจจะเป็นสมาชิกของหลาย Channel Group ได้

- แบบแผนการตรวจจับการแทรกสอด

งานวิจัย [10] เลือกใช้แบบแผนการตรวจจับแบบ NACK (NACK-based Interference Detection scheme) เช่นเดียวกับงานวิจัย [8] แต่จะแตกต่างกันที่งานวิจัย [10] ไม่ได้กำหนดให้ใช้งาน ED scan เพื่อตรวจสอบระดับพลังงานในช่องสัญญาณซ้ำอีกครั้งเมื่อ NACK มีค่ามากกว่า threshold แบบแผนการตรวจจับการแทรกสอดของงานวิจัย [10] สรุปเป็นผังงานได้ดังรูปที่ 2.15



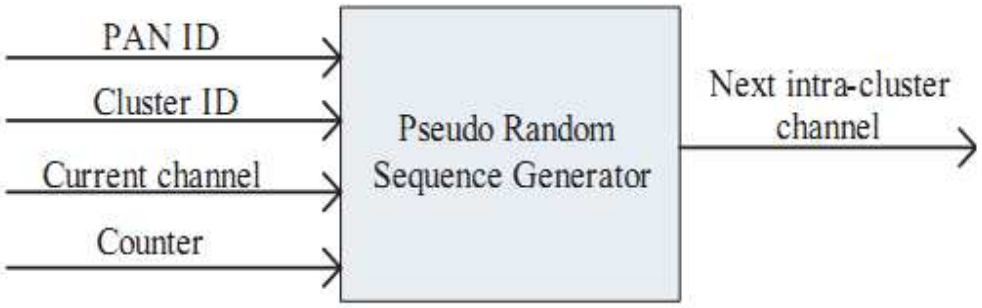
รูปที่ 2.15 ผังงานการตรวจจับการแทรกสอดของงานวิจัย [10]

สำหรับการสื่อสารระหว่าง CLH กับ BRD ซึ่งถือเป็นการสื่อสารที่สำคัญ งานวิจัย [10] เสนอให้ตรวจสอบการแทรกสอดโดยการส่งและรับ test frame เป็นระยะ หากโนดใดไม่สามารถรับ test frame ได้ก็จะถือว่ามีการแทรกสอดเกิดขึ้น

เนื่องจากทุกโนดใน Channel Group เดียวกันจะใช้งานช่องสัญญาณเดียวกัน ดังนั้นเมื่อโนดใดๆใน Channel Group ตรวจพบการแทรกสอด ทุกโนดใน Channel Group จะต้องย้ายช่องสัญญาณทั้งหมด โดยโนดที่เป็นผู้ตรวจพบการแทรกสอดจะส่ง Channel Change Broadcast Message (CCBM) ไปยังโนดใกล้เคียงเพื่อให้โนดใกล้เคียงเสมือนว่าตรวจพบการแทรกสอดด้วยเช่นกัน ดังนั้นหากโนดใดๆใน Channel Group ตรวจพบการแทรกสอดแล้วจะทำให้โนดทุกตัวใน Channel Group นั้นถือว่าตรวจพบการแทรกสอดด้วย

- แบบแผนการหลีกเลี่ยงการแทรกสอด

โนดใดๆที่ตรวจพบการแทรกสอดจะย้ายช่องสัญญาณไปยังช่องสัญญาณใหม่โดยใช้แบบแผนการหลีกเลี่ยงการแทรกสอดแบบ pseudorandom-based โดยจะใช้ Pseudo Random Sequence Generator (PRSG) (รูปที่ 2.16) ในการกำหนดช่องสัญญาณใหม่ โดย PRSG จะใช้ PAN ID, Cluster ID และตัวเลขช่องสัญญาณปัจจุบันเพื่อกำหนดช่องสัญญาณใหม่ ดังนั้นทุกโนดใน Channel Group เดียวกัน จะได้ค่าช่องสัญญาณใหม่ที่เหมือนกัน เนื่องจากมีพารามิเตอร์เหล่านี้เหมือนกัน ด้วยวิธีนี้แต่ละโนดไม่จำเป็นต้องมีการแลกเปลี่ยนข่าวสารระหว่างกันก็สามารถย้ายไปยังช่องสัญญาณเดียวกันได้



รูปที่ 2.16 แผนภาพบล็อกของ PRSG

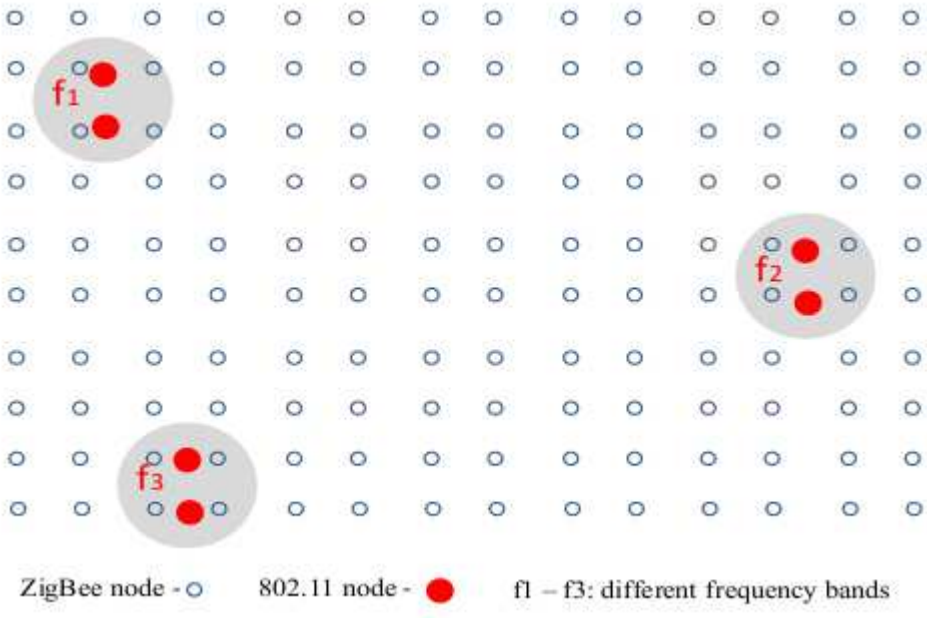
อย่างไรก็ตามช่องสัญญาณใหม่ที่ได้จาก PRSG ก็อาจพบสัญญาณแทรกสอดเช่นเดียวกัน ดังนั้นก่อนที่แต่ละโนดจะย้ายช่องสัญญาณควรตรวจสอบว่าช่องสัญญาณใหม่นั้นว่างอยู่หรือไม่ โดยใช้งาน ED scan ในช่องสัญญาณใหม่นี้ หากตรวจพบว่าช่องสัญญาณใหม่ไม่ว่าง แต่ละโนดจะเพิ่ม Counter ขึ้นอีก 1 และใช้ PRSG ในการกำหนดช่องสัญญาณใหม่อีกครั้ง อย่างไรก็ตามการใช้งาน ED scan อาจส่งผลให้แต่ละโนดใน Channel Group ย้ายไปยังช่องสัญญาณที่แตกต่างกันได้ ดังนั้นงานวิจัย [10] จึงแนะนำให้ใช้แบบแผนการหลีกเลี่ยงการแทรกสอดแบบ pseudorandom-based โดยไม่ใช้งาน ED Scan

หลังจากย้ายไปยังช่องสัญญาณใหม่แล้ว แต่ละโนดจะต้องรอเป็นระยะเวลา reconfiguration period (t_{reconf}) เพื่อให้โนดอื่นๆย้ายช่องสัญญาณได้เสร็จสิ้นครบทั้งหมด ดังนั้นโนดใดๆที่ไม่พบ neighbor เลย ภายหลังรอเป็นระยะเวลา t_{reconf} แสดงว่าโนดนั้นล้มเหลวในการย้ายช่องสัญญาณ ซึ่งหากโนดที่ย้ายช่องสัญญาณล้มเหลวไม่ใช่ CLH หรือ PNC โนดนั้นจะต้อง Disassociate เพื่อ Associate เข้าสู่เครือข่ายอีกครั้ง ในการ Associate ใหม่นี้ จะเริ่มจากการทำ Passive scan ซึ่งจะช่วยค้นหาช่องสัญญาณที่ควรจะใช้ในการสื่อสารกับเครือข่ายได้ แต่หากโนด

ที่ย้ายช่องสัญญาณล้มเหลวเป็น CLH หรือ PNC โนดนั้นจะต้องเรียกใช้แบบแผนการตรวจจับการแทรกสอดและแบบแผนการหลีกเลี่ยงการแทรกสอดใหม่อีกครั้งเพื่อให้สามารถย้ายช่องสัญญาณไปยังช่องสัญญาณใหม่ได้

2.5.1.4 Distributed Adaptive Interference-Avoidance Multi-channel MAC Protocol – [11]

งานวิจัย [11] เสนอให้ย้ายช่องสัญญาณเฉพาะโนดที่ได้รับผลกระทบจากการแทรกสอดเท่านั้นเช่นเดียวกับงานวิจัย [9] เนื่องจากพิจารณาว่าในเครือข่าย Zigbee ขนาดใหญ่ การแทรกสอดจากเครือข่าย IEEE 802.11 หนึ่งๆจะส่งผลกระทบต่อเครือข่าย Zigbee เพียงบางโนดเท่านั้น แต่ก็มีความเป็นไปได้ที่จะมีการแทรกสอดจากเครือข่าย IEEE 802.11 มากกว่าหนึ่งเครือข่ายที่มีความถี่แตกต่างกัน แนวคิดดังกล่าวแสดงดังรูปที่ 2.17 โดยงานวิจัย [11] ได้แบ่งการทำงานเป็นแบบแผนการตรวจจับการแทรกสอดและแบบแผนการหลีกเลี่ยงการแทรกสอดเช่นเดียวกัน



รูปที่ 2.17 แนวคิด Local interference ของเครือข่าย Zigbee ขนาดใหญ่

- แบบแผนการตรวจจับการแทรกสอด

งานวิจัย [11] เสนอว่าแบบแผนการตรวจจับการแทรกสอดแบบ NACK ที่มีพื้นฐานจากงานวิจัย [12] ซึ่งหลายๆงานวิจัยนำไปพัฒนาต่อนั้น อาจทำให้การตรวจจับการแทรกสอดมีการแปลความหมายผิดพลาดได้ เนื่องจากการที่โนดส่งไม่ได้รับสัญญาณ ACK นั้นไม่ได้หมายความว่าการแทรกสอดจะเกิดขึ้นที่โนดส่งเพียงกรณีเดียวแต่การแทรกสอดอาจเกิดขึ้นที่โนดรับก็ได้ ดังนั้น

งานวิจัย [11] จึงเสนอแบบแผนการตรวจจับการแทรกสอดที่ทำงานโดยโนดส่งเพียงอย่างเดียวและไม่ต้องพึ่งพาการแลกเปลี่ยนข้อมูลกับโนดอื่นๆ โดยโนดส่งจะทำหน้าที่ตรวจสอบการแทรกสอดในลักษณะใกล้เคียงกับวิธี Frequency Agility ของ Zigbee [7] แต่จะแตกต่างกันที่ในงานวิจัย [11] จะเลือกติดตามการจำนวนครั้งของการเข้าถึงช่องสัญญาณล้มเหลว ในขณะที่ Zigbee จะติดตามจำนวนครั้งของการส่งข้อมูลล้มเหลว ซึ่งเมื่อสัดส่วนระหว่างจำนวนครั้งของการเข้าถึงช่องสัญญาณล้มเหลวต่อจำนวนครั้งของความพยายามเข้าถึงช่องสัญญาณทั้งหมดสูงกว่าค่า threshold ที่กำหนด โนดส่งจะทำ energy scan บนช่องสัญญาณที่ใช้งานอยู่ และระดับพลังงานที่วัดได้สูงกว่าค่า threshold ที่กำหนด ก็จะถือว่าโนดส่งนั้นได้รับผลกระทบจากการแทรกสอด

- แบบแผนการหลีกเลี่ยงการแทรกสอด

เมื่อโนดส่งตรวจพบการแทรกสอดก็จะเรียกใช้แบบแผนการหลีกเลี่ยงการแทรกสอดทันที โดยโนดส่งจะทำ energy scan บนช่องสัญญาณต่างๆตามลำดับที่กำหนดในขั้นตอนวิธีการเลือกช่องสัญญาณ (รูปที่ 2.18) จนกว่าจะพบช่องสัญญาณที่มีระดับพลังงานต่ำกว่าค่า threshold ที่กำหนด และหากไม่พบช่องสัญญาณใดที่มีระดับพลังงานต่ำกว่าค่า threshold โนดส่งก็จะใช้ช่องสัญญาณเดิมต่อไป

Algorithm 1 Pseudo-code for Channel Selection Algorithm

```
OriginalChannel = CurrentChannel
StartingChannel = CurrentChannel
while Energy level in the current channel > TH_energy do
  channel = CurrentChannel + 4
  if channel > 26 then
    channel = channel − 26 + 10
  end if
  if channel == StartingChannel then
    channel = channel + 1
    if channel > 26 then
      channel = channel − 26 + 10
    end if
  end if
  CurrentChannel = channel
  Do energy scan in the current channel
end while
```

รูปที่ 2.18 ขั้นตอนวิธีการเลือกช่องสัญญาณของงานวิจัย [11]

เมื่อโนดส่งเลือกช่องสัญญาณใหม่ได้แล้วก็จะทำการแพร่สัญญาณไปยัง neighbor ในรัศมีหนึ่งฮอปเพื่อแจ้งให้ทราบถึงช่องสัญญาณใหม่ของตน โดยการแพร่สัญญาณดังกล่าวจะทำอย่างต่อเนื่องจนกว่าจะส่งสัญญาณได้สำเร็จ เช่น ไม่หยุดการแพร่สัญญาณไม่ว่าจะพยายามเข้าถึงช่องสัญญาณมากกว่าจำนวนครั้งที่กำหนด เป็นต้น เมื่อแพร่สัญญาณดังกล่าวสำเร็จแล้ว โนดส่งก็จะย้ายช่องสัญญาณของตนไปยังช่องสัญญาณใหม่ทันที ด้วยวิธีเช่นนี้จะเกิดกลุ่มของโนดที่ย้ายไปยังช่องสัญญาณอื่น และกลุ่มของโนดที่ยังทำงานอยู่บนช่องสัญญาณเดิม ทำให้เกิดโนดที่เรียกว่า Edge ในลักษณะเดียวกับ Border node ของงานวิจัย [9] ซึ่ง Edge node นี้จะต้องติดตามสัดส่วนการถึงช่องสัญญาณล้มเหลวต่อไปและแจ้งสถานะไปยัง neighbor ที่ยังคงใช้ช่องสัญญาณเดิมอยู่เป็นระยะ หาก Edge node พบว่าสัดส่วนการถึงช่องสัญญาณล้มเหลวต่ำกว่าค่า threshold ที่กำหนด Edge node นั้นก็จะย้ายกลับไปใช้ช่องสัญญาณเดิม ซึ่งอาจทำให้โนดข้างเคียงกลายเป็น Edge node แทนต่อไป ซึ่งหากการแทรกสอดหายไปทั้งหมด บรรดาโนดที่ได้ย้ายช่องสัญญาณไปแล้วก็จะทยอยย้ายช่องสัญญาณกลับมายังช่องสัญญาณเดิม

2.5.2 แนวทางการแก้ปัญหาการแทรกสอดระหว่าง IEEE 802.15.4 กับ IEEE 802.11b/g บนพื้นฐานของการปรับเปลี่ยน ED threshold ในการทำ CCA

จากการศึกษางานวิจัยที่เกี่ยวข้อง พบว่างานวิจัยที่แก้ปัญหาการแทรกสอดระหว่าง IEEE 802.15.4 กับ IEEE 802.11b/g บนพื้นฐานของการปรับเปลี่ยน ED threshold ในการทำ CCA นั้นยังมีเพียงแบบแผน Adaptive CCA [13] เพียงงานวิจัยเดียวเท่านั้น

แบบแผน Adaptive CCA – [13]

งานวิจัย [13] เสนอลักษณะการทำงานเป็นแบบกระจายตัว (Distribute) คือแต่ละโนดจะจัดการงานด้วยตนเอง ทั้งนี้เนื่องจากการใช้วิธีย้ายช่องสัญญาณนั้นจำเป็นต้องมีการติดต่อสื่อสารระหว่างโนด เพื่อให้ทุกโนดย้ายไปยังช่องสัญญาณเดียวกันหรือเพื่อแจ้งโนดข้างเคียงให้ทราบถึงการย้ายช่องสัญญาณของตนเอง ซึ่งการสื่อสารดังกล่าวอาจผิดพลาดได้ในสภาวะที่มีการแทรกสอดหนาแน่น โดยงานวิจัย [13] มีสมมติฐานว่าเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 และเครือข่ายแทรกสอด IEEE 802.11b/g นั้น เลือกใช้ CCA วิธีที่ 1 Energy above Threshold หรือวิธี ED เนื่องจากสามารถตรวจพบสัญญาณต่างมาตรฐานกันได้ โดยไม่จำเป็นต้องรู้จักการมอดูเลตหรือคุณสมบัติใดๆของสัญญาณแทรกสอด

เนื่องจาก IEEE 802.15.4 และ IEEE 802.11b/g เลือกใช้วิธี ED ดังนั้นการสูญเสียของ IEEE 802.15.4 ส่วนใหญ่จะเป็น Inhibition Loss ซึ่งทำให้โนดใดๆที่ต้องการส่งแพ็กเกตข้อมูลจำเป็นต้องใช้งาน CCA หลายครั้ง ซึ่งนอกจากจะสิ้นเปลืองเวลาจากการ backoff แล้วยังทำให้สิ้นเปลืองพลังงานอีกด้วย นอกจากนี้ด้วยลักษณะกลไก CSMA-CA ของทั้งสองมาตรฐาน IEEE 802.15.4 จะค่อนข้างเสียเปรียบในการแข่งขันกันเพื่อเข้าถึงช่องสัญญาณเมื่อเทียบกับ IEEE 802.11b/g ดังนั้น งานวิจัย [13] จึงเสนอขั้นตอนวิธีเพื่อลด Inhibition Loss โดยกำหนดให้ทุกโนดพิจารณาค่าอัตราส่วนความล้มเหลวในการเข้าถึงช่องสัญญาณ (channel access failure ratio, ζ) ซึ่งคำนวณจากจำนวนครั้งที่ล้มเหลวในการเข้าถึงช่องสัญญาณและจำนวนครั้งที่พยายามเข้าถึงช่องสัญญาณ เมื่อโนดใดๆมีค่า ζ มากกว่าค่า ζ_{max} ที่กำหนด โนดนั้นจะปรับเพิ่มค่า ED threshold ตามขนาด step-up size (δ_i) ที่กำหนด และจะดำเนินการเช่นนี้ไปเรื่อยๆตราบเท่าที่ ζ ยังคงมีค่ามากกว่า ζ_{max} อย่างไรก็ตามค่า ED threshold จะไม่เพิ่มสูงกว่าค่า ED threshold สูงสุดที่กำหนด เมื่อเพิ่มค่า ED threshold จนถึงจุดหนึ่ง ซึ่งทำให้โนดนั้นๆสามารถเข้าถึงช่องสัญญาณได้จะทำให้ค่า ζ ลดลงเรื่อยๆ จนกระทั่ง ζ มีค่าน้อยกว่า ζ_{min} ที่กำหนด โนดนั้นๆจะปรับลดค่า ED threshold ตามขนาด step-down size (δ_d) ที่กำหนด แต่ค่า ED threshold จะไม่ลดต่ำกว่าค่า ED threshold เริ่มต้น (initial ED threshold) ด้วยขั้นตอนวิธีนี้ เมื่อเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เผชิญกับการแทรกสอดที่หนาแน่น โนดต่างๆจะสามารถลด Inhibition Loss ได้ในลักษณะกระจายตัว โดยแต่ละโนดจะค่อยๆปรับเพิ่มค่า ED threshold ตามสภาวะของการแทรกสอดที่โนดนั้นๆ และเมื่อการแทรกสอดบรรเทาลงหรือหายไป แต่ละโนดจะค่อยๆปรับลดค่า ED threshold กลับสู่ค่าเริ่มต้นเพื่อหลีกเลี่ยงความได้เปรียบเหนือโนดอื่นๆในการเข้าถึงช่องสัญญาณ ทั้งนี้พารามิเตอร์ต่างๆสามารถปรับเปลี่ยนได้ตามความเหมาะสมของแต่ละกาประยุกต์ใช้งานของเครือข่ายเซ็นเซอร์ไร้สาย

บทที่ 3

วิธีการที่นำเสนอ

เมื่อได้เรียนรู้กระบวนการรับส่งข้อมูลของเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b.g การเกิดการแทรกสอดระหว่างเครือข่ายทั้งสอง รวมถึงแนวทางในการแก้ปัญหาการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b/g ในรูปแบบต่างๆที่ได้มีผู้เสนอไว้แล้ว ดังรายละเอียดที่ได้กล่าวไปแล้วในบทที่ 2 สำหรับเนื้อหาในบทที่ 3 นี้จะเป็นการนำความรู้จากหลักการทำงานของกระบวนการรับส่งข้อมูลของทั้งสองเครือข่าย รวมถึงแนวคิดในการพัฒนาและการแก้ปัญหาการแทรกสอดในรูปแบบต่างๆ มาประยุกต์และพัฒนาเป็นแนวทางการแก้ปัญหาการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b/g อีกรูปแบบหนึ่งซึ่งเป็นวิธีการที่นำเสนอสำหรับงานวิจัยนี้ดังรายละเอียดที่จะอธิบายต่อไป สำหรับผลการจำลองการทำงานของวิธีการที่นำเสนอจะกล่าวถึงถัดไปในบทที่ 4

3.1 วิธีการที่นำเสนอ

จากการวิเคราะห์งานวิจัยเพื่อแก้ปัญหาการแทรกสอดกันระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b/g ที่มีผู้เสนอไว้พบว่ามี 2 แนวทาง คือ การย้ายช่องสัญญาณไปยังช่องสัญญาณอื่นที่ไม่มีการแทรกสอดไม่ว่าจะเป็นการย้ายช่องสัญญาณของทั้งเครือข่าย หรือการย้ายช่องสัญญาณเฉพาะโนดที่ได้รับผลกระทบจากการแทรกสอด ซึ่งถือเป็นการแก้ปัญหาในชั้น PHY และอีกแนวทางหนึ่งคือการปรับเปลี่ยนค่า ED threshold ของ CCA ซึ่งเป็นการแก้ปัญหาในชั้น MAC

ทั้งนี้ การย้ายไปยังช่องสัญญาณที่ปราศจากการแทรกสอดนั้น ถือเป็นแนวทางที่แก้ปัญหาการแทรกสอดได้อย่างสมบูรณ์ หากทุกโนดในเครือข่ายสามารถย้ายไปยังช่องสัญญาณที่ปราศจากการแทรกสอดจากเครือข่าย IEEE 802.11b/g ได้ แต่ขั้นตอนในการย้ายช่องสัญญาณนั้นจะเห็นว่าในทุกงานวิจัยที่เลือกใช้วิธีย้ายช่องสัญญาณนั้น จำเป็นต้องมีการส่งข้อมูลข่าวสารระหว่างโนดทั้งสิ้น ซึ่งในสภาวะที่มีการแทรกสอดหนาแน่นนั้น มีความเป็นไปได้ที่ข้อมูลข่าวสารเหล่านี้จะส่งไม่สำเร็จ ซึ่งอาจทำให้บางโนดไม่สามารถย้ายช่องสัญญาณได้ นอกจากนี้หากพิจารณาถึงรูปแบบการทำงานของเครือข่าย IEEE 802.11b/g ที่ใช้งานกันโดยทั่วไป เช่น Wi-Fi ลักษณะการใช้งานจะเป็นการ download เป็นส่วนมาก นั่นคือ ทราฟฟิกส่วนใหญ่จะเป็นการส่งจากอุปกรณ์ Access Point ไปยังโนดอื่นๆ โดยจะมีทราฟฟิกจากโนดอื่นๆไปยัง Access point

บ้างแต่ไม่หนาแน่นมากนัก และในขณะใดขณะหนึ่ง สำหรับเครือข่ายหนึ่งๆของ Wi-Fi จะมีโนดที่ทำการส่งข้อมูลได้เพียงโนดเดียวเท่านั้น ดังนั้นจึงสามารถพิจารณาได้ว่าปัญหาการแทรกสอดจาก Wi-Fi มักจะเกิดขึ้นจากอุปกรณ์ Access Point เป็นหลัก ซึ่งการแทรกสอดดังกล่าวมักจะครอบคลุมเพียงบางส่วนของเครือข่ายเซ็นเซอร์ไร้สายเท่านั้น (ลักษณะเดียวกับรูปที่ 2.13)

นอกจากปัญหาที่อาจเกิดขึ้นจากการไม่สามารถส่งข้อมูลข่าวสารเพื่อช่วยในการย้ายช่องสัญญาณในสภาวะที่มีการแทรกสอดหนาแน่นแล้ว วิธี *Frequency Agility* [7], [8] อาจไม่เหมาะสมนักในการใช้งานกับเครือข่ายเซ็นเซอร์ไร้สายขนาดใหญ่ เนื่องจากมีช่วงเวลา scan หาช่องสัญญาณใหม่ค่อนข้างนาน ซึ่งในช่วงเวลานี้เครือข่ายเซ็นเซอร์ไร้สายจะไม่สามารถรับส่งข้อมูลตามปกติได้เลย ส่วนวิธี *Adaptive Radio Channel Allocation* [9] ซึ่งเสนอให้ย้ายช่องสัญญาณเฉพาะโนดที่อยู่ในพื้นที่ที่มีการแทรกสอดเท่านั้น จึงอาจไม่มีปัญหาเรื่องระยะเวลาในการย้ายช่องสัญญาณมากนัก แต่การที่เครือข่าย IEEE 802.15.4 เดียวกันใช้ช่องสัญญาณต่างกัน โดยใช้ Border Node เป็นโนดที่คอยสลับช่องสัญญาณระหว่างช่องสัญญาณของโนดภายใน GF กับโนดภายนอก GF โดยใช้การตั้ง schedule ในการสลับช่องสัญญาณ ทำให้ Border Node ต้องรับภาระหนัก และการตั้ง schedule ให้ทำงานได้อย่างเหมาะสมทำได้ยากในทางปฏิบัติ เช่นเดียวกับวิธี *Distributed Adaptive Interference-Avoidance Multi-channel MAC Protocol* [11] ที่เสนอให้ย้ายช่องสัญญาณเฉพาะโนดที่ได้รับผลกระทบจากการแทรกสอดเช่นกัน และมีแนวคิดคล้ายๆวิธี *Adaptive Radio Channel Allocation* จึงน่าจะมีปัญหาคล้ายๆกัน ในขณะที่วิธี *Adaptive Interference-Aware Multi-Channel Clustering Algorithm* [10] ซึ่งเสนอให้ใช้ทุกโนดใช้ PRSG ในการกำหนดช่องสัญญาณใหม่นั้น กระบวนการย้ายช่องสัญญาณจะขึ้นอยู่กับ CCBM เป็นอย่างมาก โดยหากโนดใดโนดหนึ่งโดยเฉพาะโนดที่เป็น CLH หรือ PNC ไม่สามารถย้ายช่องสัญญาณได้จะทำให้เสียเวลาในการเรียกใช้แบบแผนการตรวจจับการแทรกสอดและแบบแผนการหลีกเลี่ยงการแทรกสอดใหม่อีกครั้ง

สำหรับวิธี Adaptive CCA [13] เลือกแนวทางการแก้ปัญหาในชั้น MAC โดยเป็นแนวทางแบบ Distribute ซึ่งแต่ละโนดสามารถทำงานด้วยตนเองโดยไม่จำเป็นต้องมีการส่งข้อมูลข่าวสารระหว่างโนด แต่วิธีนี้จะใช้ได้ก็ต่อเมื่อทั้งเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b/g เลือกใช้ CCA วิธี ED เท่านั้น เนื่องจากวิธีนี้พิจารณาเพียงการลด Inhibition Loss แต่ไม่ได้พิจารณาถึง Collision Loss ซึ่งในความเป็นจริงแล้วเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b/g สามารถส่งแพ็กเกตข้อมูลพร้อมกันได้โดยไม่เกิดปัญหาแต่อย่างใด หากโนดของ IEEE 802.15.4 และ IEEE 802.11b/g อยู่ห่างกันมากเพียงพอ หรือมี Signal to Interference-plus-

Noise Ratio (SINR) สูงเพียงพอ ดังนั้นการที่เครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b/g เลือกใช้วิธี ED ทั้งคู่นั้น อาจส่งผลให้ throughput ของทั้งสองเครือข่ายลดลงอย่างมากโดยไม่จำเป็น

ในงานวิจัยนี้จึงเลือกใช้แนวทางการแก้ปัญหาในชั้น MAC และเป็นแบบ Distribute นั่นคือเซ็นเซอร์โนดแต่ละตัวจะจัดการงานของตนเองได้ โดยไม่จำเป็นต้องส่งข้อมูลข่าวสารระหว่างกัน โดยจะเสนอให้โนดส่งใช้วิธีที่ 3 *Carrier sense with energy above energy threshold* โดยใช้ตัวดำเนินการทางตรรกศาสตร์ OR ในการทำ CCA หรืออธิบายได้ว่าโนดส่งจะใช้ทั้งวิธี ED และวิธี CS ในการตรวจสอบช่องสัญญาณ และจะรายงานว่าช่องสัญญาณไม่ว่างทันที หากพบว่าการตรวจสอบโดยวิธี ED หรือวิธี CS กรณีใดกรณีหนึ่งหรือทั้ง 2 กรณีตรวจสอบพบว่าช่องสัญญาณไม่ว่าง ซึ่งการเลือกใช้วิธี CCA เช่นนี้ ก็เพื่อการดึงเอาข้อดีข้อวิธี ED และวิธี CS มาใช้ประโยชน์ โดยสามารถพิจารณาข้อดี ข้อเสียของวิธี ED และวิธี CS ได้ ดังนี้

วิธี ED เหมาะสำหรับการใช้งานในกรณีที่สัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b/g มีพลังงานสูงเพียงพอที่จะทำให้แพ็กเกตข้อมูลของ IEEE 802.15.4 มีโอกาสผิดพลาดหรือมีค่า PER (Packet Error Rate) สูง โดยหากเลือกใช้วิธี ED โนดของ IEEE 802.15.4 จะไม่ส่งข้อมูลในช่วงนี้ เนื่องจากการส่งแพ็กเกตข้อมูลในช่วงนี้จะมีโอกาสล้มเหลวสูงทำให้อาจต้องส่งข้อมูลซ้ำ ซึ่งจะเสียเวลาและสิ้นเปลืองพลังงาน

วิธี CS เหมาะสำหรับการใช้งานในกรณีที่ไม่มีสัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b/g หรือสัญญาณแทรกสอดมีพลังงานไม่สูงขนาดที่จะส่งผลกระทบให้การส่งแพ็กเกตข้อมูลของ IEEE 802.15.4 ผิดพลาด

ดังนั้น อาจสรุปได้ว่าหากค่า SINR ที่โนดใดๆของเครือข่าย IEEE 802.15.4 สูงกว่าค่าๆหนึ่ง โนดนั้นควรเลือกใช้วิธี CS ซึ่งจะตรวจสอบเพียงทราฟฟิกของมาตรฐาน IEEE 802.15.4 ด้วยกันเท่านั้น แต่หากค่า SINR ต่ำกว่าค่าๆหนึ่งซึ่งจะทำให้การส่งแพ็กเกตข้อมูลมีโอกาสผิดพลาดสูง ควรเลือกใช้วิธี ED เพื่อรอจนกว่าช่องสัญญาณว่างและจึงค่อยทำการส่งแพ็กเกตข้อมูล ซึ่งจะทำให้โอกาสส่งแพ็กเกตข้อมูลสำเร็จสูงขึ้น และช่วยให้ประหยัดพลังงานมากขึ้น

แต่เนื่องจากโนดในมาตรฐาน IEEE 802.15.4 ไม่สามารถวัดค่า SINR ได้โดยตรง ดังนั้นงานวิจัยนี้จึงเลือกใช้การทำ ED scan เพื่อวัดพลังงานของสัญญาณแทรกสอด เพื่อนำมากำหนดเป็นค่า ED threshold สำหรับการทำ CCA ตามวิธีที่กำหนด โดยแบบแผนที่นำเสนอจะเริ่มต้นจากการกำหนดให้เซ็นเซอร์โนดทุกตัวในเครือข่ายเลือกใช้แบบวิธี CS ในช่วงเริ่มต้น นั่นคือสมมติว่ายัง

ไม่มีการแทรกสอดในช่วงเริ่มต้นนั่นเอง โดยจะเลือกใช้แบบแผนการตรวจจับการแทรกสอดแบบ NACK ในลักษณะใกล้เคียงกับงานวิจัย [8] และ [10] นั่นคือ เซ็นเซอร์โนดที่ได้ส่งแพ็กเกตข้อมูลไปแล้วจะตรวจสอบสัญญาณ ACK โดยหากไม่ได้รับ ACK ภายในระยะเวลาที่กำหนด ค่า NACK จะเพิ่มขึ้นครั้งละ 1 และเซ็นเซอร์โนดนั้นๆจะส่งข้อมูลซ้ำ (Retransmission) อีกครั้ง หากค่า NACK มีค่าสูงกว่าค่า $NACK_{th}$ ที่กำหนด (ซึ่งในงานวิจัยนี้จะกำหนดค่า $NACK_{th}$ ให้สอดคล้องกับค่าปริยายของ *macMaxFrameRetrie*s) เซ็นเซอร์โนดจะหยุดการส่งแพ็กเกตข้อมูลทันทีและเรียกใช้ ED scan อย่างไรก็ตาม การใช้ ED scan เพื่อตรวจสอบการแทรกสอดโดยนำค่า RSSI มาเปรียบเทียบกับค่า threshold ที่กำหนด ดังวิธีที่เสนอใน [8] และ [9] นั้น ในทางปฏิบัติเป็นเรื่องยากที่จะกำหนดค่า threshold ที่เหมาะสมได้ เนื่องจากในความเป็นจริงแล้วสิ่งที่จะกำหนดว่าเกิดการแทรกสอดที่มีผลกระทบขึ้นหรือไม่นั้นคือค่า SINR ซึ่งค่า RSSI ที่วัดได้จาก ED scan นั้นจะบ่งบอกเพียงระดับพลังงานที่วัดในขณะนั้นเท่านั้น ไม่สามารถทำให้ทราบค่า SINR ได้ จึงเป็นเรื่องยากที่จะทราบว่าค่าพลังงานในระดับที่วัดได้จาก ED scan นั้นทำให้เกิดผลกระทบจากการแทรกสอดหรือไม่ ดังนั้นในงานวิจัยนี้จะเรียกใช้ ED scan เพื่อนำค่า RSSI ที่วัดได้ไปกำหนดเป็น ED threshold ในขั้นตอนต่อไปเท่านั้น ไม่ได้นำมาใช้พิจารณาว่าเกิดการแทรกสอดขึ้นหรือไม่ โดยจะถือว่าการแทรกสอดเกิดขึ้นเพียงแค่ในกรณีที่ค่า NACK มีค่าสูงกว่า $NACK_{th}$ ที่กำหนดเท่านั้นในลักษณะเดียวกับแบบแผนการตรวจจับการแทรกสอดใน [10]

แบบแผนการตรวจจับการแทรกสอดที่เสนอ มีข้อดีคือ สามารถทำงานได้ในขั้นตอนการส่งแพ็กเกตข้อมูลปกติของกลไก CSMA-CA ซึ่งเซ็นเซอร์โนดทุกตัวต้องตรวจสอบสถานะของช่องสัญญาณทุกครั้งก่อนส่งแพ็กเกตข้อมูลอยู่แล้ว ซึ่งวิธี CS จะเป็นการตรวจสอบเฉพาะทราฟฟิกของเครือข่าย IEEE 802.15.4 ด้วยกันเท่านั้น ดังนั้นเซ็นเซอร์โนดตัวใดที่สามารถส่งข้อมูลแพ็กเกตข้อมูลได้ก็หมายความว่าเซ็นเซอร์โนดนั้นไม่ตรวจพบการใช้ช่องสัญญาณของโนด IEEE 802.15.4 อื่นๆ ในขณะนั้น ดังนั้นการที่ไม่ได้รับสัญญาณ ACK กลับมาหลังจากพยายามส่งข้อมูลมากกว่าจำนวนครั้งที่กำหนด น่าจะเพียงพอที่จะสรุปได้ว่าการส่งแพ็กเกตข้อมูลครั้งนั้นๆเกิดการสูญเสีย (loss) จากการชนกับทราฟฟิกจากมาตรฐานอื่นนั่นเอง ยกเว้นกรณีที่เกิดปัญหา Hidden node ซึ่งอาจทำให้แพ็กเกตข้อมูลของเซ็นเซอร์โนดชนกันได้ แม้ว่าเซ็นเซอร์โนดแต่ละตัวไม่ตรวจพบการใช้ช่องสัญญาณของ IEEE 802.15.4 ในขณะนั้นก็ตาม อย่างไรก็ตามปัญหา Hidden node จะไม่อยู่ในขอบเขตของงานวิจัยนี้

การทำ ED Scan เมื่อค่า NACK มีค่ามากกว่า $NACK_{th}$ ในแบบแผนการตรวจจับการแทรกสอดที่เสนออาจส่งผลกระทบต่อการสมรรถนะการทำงานบ้าง เนื่องจากการทำ ED scan

จะต้อง scan หาระดับพลังงานที่สูงที่สุดในช่วง 8 symbol period ซึ่งคิดเป็นระยะเวลา 128 μs แต่หากพิจารณาว่าการทำ ED scan จะทำก็ต่อเมื่อส่งแพ็กเกตข้อมูลไปแล้วไม่ได้รับ ACK กลับมามากกว่าจำนวนครั้งที่กำหนดเท่านั้น ดังนั้นจึงไม่ส่งผลกระทบต่อการทำงานโดยรวมมากนัก

เมื่อเซ็นเซอร์โนดตัวใดตรวจพบการแทรกสอดจากแบบแผนการตรวจจับการแทรกสอดข้างต้น ก็จะเปลี่ยนไปใช้กลไก CSMA-CA วิธีที่ 3 *Carrier sense with energy above energy threshold* โดยใช้ตัวดำเนินการทางตรรกศาสตร์ OR ดังที่ได้กล่าวไปแล้วข้างต้น โดยกลไก CSMA-CA วิธีนี้จะมีการตรวจสอบสถานะของช่องสัญญาณทั้งจากวิธี ED และวิธี CS ซึ่งการตรวจสอบช่องสัญญาณด้วยวิธี CS นั้นเพื่อให้มั่นใจว่าไม่มีทราฟฟิกจากโนด IEEE 802.15.4 อื่นๆ กำลังใช้งานช่องสัญญาณอยู่ในขณะนั้น ส่วนการตรวจสอบช่องสัญญาณด้วยวิธี ED จะใช้ค่า ED threshold ตามค่า RSSI ที่ได้จากการทำ ED scan ในขั้นตอนการตรวจจับการแทรกสอดที่ผ่านมา (ในการใช้งานจริงอาจกำหนดค่า ED threshold ให้ต่ำกว่าค่า RSSI ที่วัดได้เล็กน้อย เนื่องจากค่าระดับพลังงานของสัญญาณแทรกสอดเดิมๆอาจไม่เท่ากันในแต่ละครั้งของการทำ ED scan) ดังนั้นด้วยวิธีที่เสนอ CCA เซ็นเซอร์โนดต้นทางจะรายงานว่าช่องสัญญาณไม่ว่างก็ต่อเมื่อในขณะนั้นมี ทราฟฟิกจากเครือข่าย IEEE 802.15.4 เดียวกันกำลังใช้งานช่องสัญญาณอยู่ หรือมีสัญญาณใดๆซึ่งมีพลังงานมากกว่าค่า ED threshold ในช่องสัญญาณที่เซ็นเซอร์โนดกำลังใช้งานอยู่ ซึ่งมีความเป็นได้สูงที่จะเป็นสัญญาณจากโนด IEEE 802.11b/g ที่ทำให้เซ็นเซอร์โนดส่งแพ็กเกตข้อมูลล้มเหลวในตอนแรกนั่นเอง ทั้งนี้ ไม่ว่าโนด IEEE 802.11b/g นี้จะทำให้เกิดการแทรกสอดที่เซ็นเซอร์โนดต้นทางหรือปลายทางก็ตาม เซ็นเซอร์โนดต้นทางจะจดจำโนด IEEE 802.11b/g นี้จากค่า RSSI ที่วัดได้ ดังนั้นเซ็นเซอร์โนดต้นทางจะสามารถส่งแพ็กเกตข้อมูลได้ก็ต่อเมื่อโนด IEEE 802.11b/g ดังกล่าวไม่ได้อยู่ในระหว่างส่งแพ็กเกตข้อมูลอยู่ในขณะนั้น

การใช้วิธี CS ในตอนเริ่มต้นก็เพื่อช่วยประหยัดพลังงานในการทำ CCA ที่จะประหยัดพลังงานมากกว่าวิธี CCA ที่เสนอ และอีกเหตุผลหนึ่งคือเพื่อที่จะสามารถอัพเดตค่า ED threshold ครั้งแรกได้เมื่อตรวจพบการแทรกสอด เนื่องจากโดยทั่วไปค่าปริยายของ ED threshold จะตั้งไว้เท่ากับค่า receiver sensitivity ซึ่งเป็นระดับพลังงานต่ำที่สุดที่โนดรับสามารถรับสัญญาณได้ หรืออาจตั้งไว้สูงกว่าค่า receiver sensitivity เพียงเล็กน้อยเท่านั้น ดังนั้น หากใช้ CCA วิธีที่เสนอตั้งแต่แรกจะทำให้เซ็นเซอร์โนดต้นทางรายงานว่าช่องสัญญาณไม่ว่างตลอดเวลาเมื่อตรวจพบสัญญาณแทรกสอดที่อาจไม่ส่งผลกระทบให้การส่งแพ็กเกตข้อมูลล้มเหลว แต่หากใช้วิธี CS ก่อนในตอนเริ่มต้นก็จะทำให้สามารถใช้ค่า ED threshold จากค่า RSSI ที่วัดได้ โดยไม่ต้องใช้ค่าปริยาย

ทั้งนี้หลังจากมีการอัปเดตค่า ED threshold จากค่า RSSI ที่วัดได้ไปแล้ว หากเซ็นเซอร์โนดตรวจสอบสถานะช่องสัญญาณแล้วพบว่าช่องสัญญาณว่าง แต่เมื่อส่งแพ็กเกตข้อมูลไปแล้วไม่ได้รับ ACK มากกว่าจำนวนครั้งที่กำหนด (ลักษณะเดียวกับแบบแผนการตรวจจับการแทรกสอดในตอนแรก) อาจเป็นไปได้ว่ายังมีสัญญาณจากโนด IEEE 802.11b/g อื่นๆ ซึ่งมีระดับพลังงานต่ำกว่าค่า ED threshold ของเซ็นเซอร์โนดต้นทางที่ส่งผลให้การส่งข้อมูลครั้งนั้นล้มเหลว ดังนั้นเซ็นเซอร์โนดต้นทางจะทำ ED scan และนำค่า RSSI ที่ได้มาอัปเดตเป็นค่า ED threshold ใหม่อีกครั้ง โดยยังคงใช้ CCA วิธีเดิม ดังนั้น อาจสรุปได้ว่าค่า ED threshold จะมีการอัปเดตไปเรื่อยๆ ตราบใดที่ยังมีสัญญาณ IEEE 802.11b/g ที่มีระดับพลังงานต่ำกว่า ED threshold ทำให้การส่งแพ็กเกตข้อมูลของเซ็นเซอร์โนดล้มเหลว หรือ อาจกล่าวได้ว่า ED threshold ได้มาจากระดับพลังงานที่ต่ำที่สุดซึ่งส่งผลให้การส่งแพ็กเกตข้อมูลของเซ็นเซอร์โนดล้มเหลวนั่นเอง

ในวิธีที่เสนอ เมื่อเซ็นเซอร์โนดตัวใดเปลี่ยนมาใช้วิธี CCA ที่เสนอไปแล้ว ก็จะใช้วิธีนี้ต่อไปเรื่อยๆ ค่า ED threshold ก็จะถูกอัปเดตไปเรื่อยๆจนกว่าจะถึงจุดที่เป็นระดับพลังงานที่ต่ำที่สุดซึ่งส่งผลให้การส่งแพ็กเกตข้อมูลของเซ็นเซอร์โนดล้มเหลว แม้ว่าเมื่อระยะเวลาผ่านไประยะหนึ่งการแทรกสอดจากเครือข่าย IEEE 802.11b/g หายไป เครือข่าย IEEE 802.15.4 ก็ยังสามารถใช้วิธีที่เสนอโดยใช้ค่า ED threshold ที่อัปเดตล่าสุดได้โดยไม่ส่งผลให้สมรรถนะของเครือข่ายลดลงแต่อย่างใดเมื่อเปรียบเทียบกับวิธี CS ซึ่งเหมาะสมสำหรับการใช้งานในกรณีที่ไม่มีการแทรกสอด

แต่หากพิจารณาในด้านพลังงานแล้ว วิธี CS จะใช้พลังงานน้อยกว่าวิธีที่เสนอซึ่งจะต้องตรวจสอบสถานะของช่องสัญญาณจากทั้งวิธี ED และวิธี CS ดังนั้น หากการแทรกสอดหายไป การเปลี่ยนกลับมาใช้วิธี CS น่าจะเหมาะสมกว่า และยังสามารถเปลี่ยนกลับมาใช้วิธีที่เสนอได้ทันทีหากเกิดการแทรกสอดขึ้นอีกครั้ง เนื่องจากวิธีที่เสนอก็เริ่มต้นจากการใช้วิธี CS อยู่แล้ว แต่เนื่องจากงานวิจัยนี้สนใจเฉพาะสมรรถนะการทำงานของเครือข่ายเท่านั้นและไม่ได้วัดผลในด้านการใช้พลังงาน วิธีที่เสนอจึงยังไม่รวมขั้นตอนวิธีในการตรวจสอบสภาวะการแทรกสอดเพื่อเปลี่ยนกลับไปใช้วิธี CS

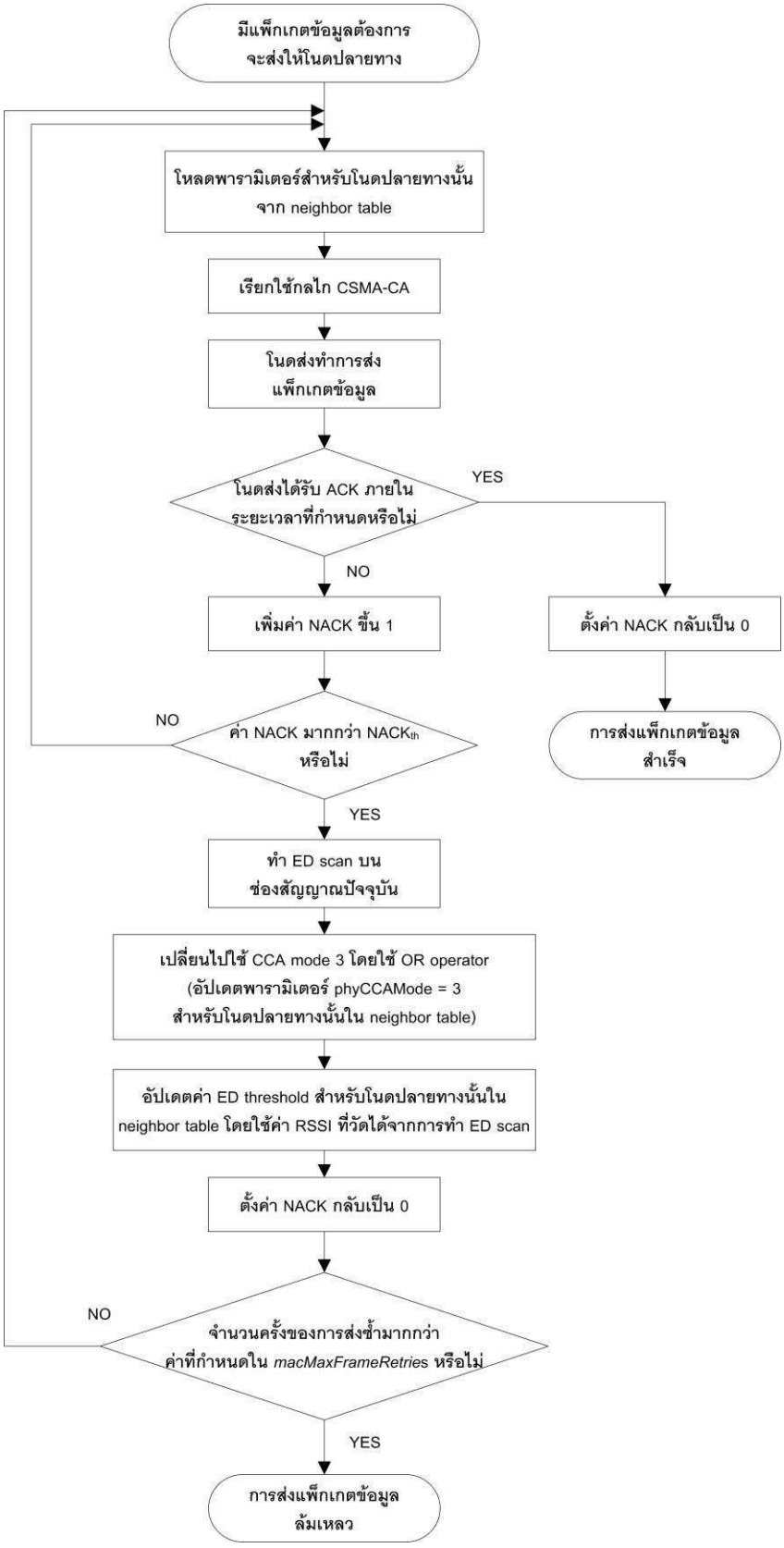
ในการทำงานของแบบแผนที่เสนอนี้ เซ็นเซอร์โนดทุกตัว จะต้องจดจำค่า ED threshold และวิธี CCA ที่ใช้ในการส่งแพ็กเกตข้อมูลครั้งล่าสุดไปยังโนดปลายทางแต่ละตัวของตนไว้ใน neighbor table ของตน ดังนั้นในการส่งแพ็กเกตข้อมูลไปยัง neighbor แต่ละตัว อาจจะใช้วิธี CCA ต่างกัน และใช้ค่า ED threshold ต่างกัน ทั้งนี้ เนื่องจากสภาวะของการแทรกสอดที่เซ็นเซอร์โนดปลายทางแต่ละตัวจะแตกต่างกันไป ด้วยการทำงานในรูปแบบนี้จะทำให้เซ็นเซอร์โนดทุกตัวสามารถใช้งานช่องสัญญาณได้อย่างคุ้มค่าที่สุด

เนื่องจากวิธีที่เสนอจะมีการอัปเดตค่า ED threshold อย่างต่อเนื่องตามสภาวะการแทรกสอดของคู่ของเซ็นเซอร์โนดต้นทางและปลายทางใดๆ ดังนั้น งานวิจัยนี้กำหนดให้วิธีที่เสนอมีชื่อเรียกว่า แบบแผน ED threshold แบบปรับค่าได้ หรือ Adaptive ED threshold

การทำงานของแบบแผนที่นำเสนอ สามารถสรุปเป็นผังงานได้ ดังรูปที่ 3.1 ซึ่งแบบแผนการทำงานวิธีที่เสนอจะมีลักษณะใกล้เคียงกับแบบแผนการตรวจจับการแทรกสอดแบบ NACK ในงานวิจัย [8] และ [10] แต่จะแตกต่างกันตรงการทำ ED scan ในแบบแผนที่เสนอนั้นทำเพื่อนำค่า RSSI ที่วัดได้ไปกำหนดเป็นค่า ED threshold ซึ่งจะแตกต่างกับงานวิจัย [8] ที่ทำ ED scan เพื่อตรวจสอบให้มั่นใจเท่านั้นว่ามีพลังงานที่สูงกว่าค่า threshold ที่กำหนดซึ่งทำให้การส่งแพ็กเกตข้อมูลล้มเหลวจริงๆ

ในวิธีที่เสนอในรูปที่ 3.1 นั้น ขั้นตอนเรียกใช้กลไก CSMA-CA จะเป็นไปตามกลไก unslotted CSMA-CA ปกติของ IEEE 802.15.4 ดังรูปที่ 2.4 โดยตอนเริ่มต้นจะใช้ CCA วิธี CS สำหรับทุกๆโนดปลายทางดังที่ได้กล่าวไปแล้ว แต่หากพบว่าการส่งแพ็กเกตข้อมูลจากโนดส่งไปยังโนดปลายทางใดๆล้มเหลวตามแนวทางการตรวจสอบการแทรกสอดของวิธีที่เสนอ โนดส่งจะอัปเดตวิธี CCA สำหรับโนดปลายทางนั้นเป็นวิธีที่ 3 และจะใช้ CCA วิธีที่ 3 ทุกครั้งที่มีแพ็กเกตข้อมูลที่ต้องการส่งไปยังโนดปลายทางดังกล่าว แต่สำหรับโนดปลายทางอื่นที่ยังไม่มีการอัปเดตวิธี CCA ใหม่ โนดส่งก็จะใช้วิธี CS ตามปกติในการส่งแพ็กเกตข้อมูลไปยังโนดปลายทางดังกล่าว

ทั้งนี้วิธีที่เสนอจะไม่สามารถนำมาใช้กับการส่งสัญญาณ ACK ตอบกลับจากโนดปลายทางไปยังโนดต้นทางได้ ซึ่งการส่ง ACK นั้น จะสามารถส่งได้ทันทีโดยไม่ต้องใช้กลไก CSMA-CA เพื่อควบคุมการเข้าถึงช่องสัญญาณ ดังนั้น โอกาสที่การส่งแพ็กเกตข้อมูลล้มเหลวยังอาจเกิดขึ้นได้หากสัญญาณ ACK ได้รับผลกระทบจากการแทรกสอดทำให้การส่ง ACK ล้มเหลว แต่โดยปกติแล้วสัญญาณ ACK จะมีขนาดเฟรมเล็กกว่าแพ็กเกตข้อมูล ดังนั้นโอกาสที่สัญญาณ ACK จะเกิดการชนกับสัญญาณแทรกสอดจะมีน้อยกว่าโอกาสที่แพ็กเกตข้อมูลชนกับสัญญาณแทรกสอด



รูปที่ 3.1 ผังงานของแบบแผนที่เสนอ

3.2 แบบจำลองในการวิเคราะห์การแทรกสอด

งานวิจัยนี้ใช้แบบจำลอง (Model) ในการวิเคราะห์การแทรกสอด ดังนี้

3.2.1 การแทรกสอดภายในเครือข่าย IEEE 802.15.4

หากแพ็กเกตข้อมูลจากโนดใดๆภายในเครือข่าย IEEE 802.15.4 เดียวกันเกิดการชนกัน จะถือว่าแพ็กเกตข้อมูลทั้งหมดสูญเสีย เนื่องจากแพ็กเกตข้อมูลมีลักษณะการมอดูเลตและการแผ่สเปกตรัมเหมือนกัน

3.2.2 การแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับ IEEE 802.11b

ดังที่ได้กล่าวไปแล้วในบทที่ 2 ว่ามาตรฐาน IEEE 802.11g เป็นส่วนขยายที่พัฒนาเพิ่มเติมจากมาตรฐาน IEEE 802.11b เพื่อรองรับอัตราข้อมูลที่สูงขึ้น ในขณะที่กระบวนการรับส่งข้อมูลยังคงเป็นรูปแบบเดียวกัน เพียงแต่ค่าของพารามิเตอร์ต่างๆของทั้งสองโพรโทคอลนี้อาจจะแตกต่างกันอยู่บ้าง โดยงานวิจัยนี้จะเลือกใช้ค่าพารามิเตอร์จากมาตรฐาน IEEE 802.11b เป็นหลัก โดยจะใช้แบบจำลองการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับ IEEE 802.11b จาก [2] และ [14] คือ หากแพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b เกิดการชนกัน จะใช้ค่า PER (Packet Error Rate) ในการกำหนดความน่าจะเป็นที่แพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 จะสูญเสีย ซึ่งค่า PER ดังกล่าว สามารถคำนวณได้จากค่า BER (Bit Error Rate) โดยใช้สมการหาค่า BER สำหรับมาตรฐาน IEEE 802.15.4 ที่แถบความถี่ 2.4 GHz ซึ่งกำหนดใน [2] ดังนี้

$$BER = \frac{8}{15} \times \frac{1}{16} \times \sum_{k=2}^{16} (-1)^k \binom{16}{k} e^{\left(20 \times SINR_{dB} \times \left(\frac{1}{k} - 1\right)\right)} \qquad (1)$$

โดย $SINR_{dB}$ คือ Signal to Interference-plus-Noise Ratio มีหน่วยเป็น dB

และสามารถคำนวณค่า PER ได้ ดังนี้

$$PER = 1 - (1 - BER)^{(8 \times l)} \qquad (2)$$

โดย l คือ ความยาวของแพ็กเกต (packet length) มีหน่วยเป็นออกเตต

จากสมการที่ (1) และ (2) จะเห็นว่าค่า PER จะขึ้นอยู่กับค่า SINR เท่านั้น ซึ่งค่า SINR สามารถคำนวณได้ดังนี้

$$SINR_{dB} = 10\log_{10}\left(\frac{P_c}{\sum_n P_i(n) + P_n}\right) \quad (3)$$

โดย P_c คือ กำลังของสัญญาณพาห์ที่โนด IEEE 802.15.4 ปลายทาง

$P_i(n)$ คือ กำลังของสัญญาณแทรกสอด (interference) แหล่งที่ n ที่โนด IEEE 802.15.4 ปลายทาง

P_n คือ กำลังของสัญญาณรบกวน (noise) ที่โนด IEEE 802.15.4 ปลายทาง

โดยปกติแล้ว ขนาดของ P_n จะเล็กกว่า P_i มาก โดยทั่วไปจึงมักไม่พิจารณา P_n โดยจะใช้ค่า SIR (Signal to Interference Ratio) แทนค่า SINR ดังนี้

$$SIR_{dB} = 10\log_{10}\left(\frac{P_c}{\sum_n P_i(n)}\right) \quad (4)$$

แต่หากพิจารณาว่าในพื้นที่หนึ่ง การใช้งานเครือข่าย IEEE 802.11b มักจะเลือกใช้งานช่องสัญญาณที่ไม่ซ้อนทับกัน เช่น ช่องสัญญาณที่ 1 ช่องสัญญาณที่ 6 และช่องสัญญาณที่ 11 ดังนั้นจึงสามารถสรุปได้ว่าช่องสัญญาณหนึ่งของเครือข่าย IEEE 802.15.4 โดยทั่วไปแล้วจะมีการแทรกสอดจากเครือข่าย IEEE 802.11b เพียงเครือข่ายเดียว และในเครือข่าย IEEE 802.11b หนึ่งๆ จะมีโนดที่ทำการส่งแพ็กเกตข้อมูลอยู่เพียงโนดเดียวเท่านั้นในขณะใดขณะหนึ่ง ดังนั้นในขณะใดขณะหนึ่ง สัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b จะมีเพียงสัญญาณเดียว ดังนั้น หากพิจารณาในขณะใดขณะหนึ่ง

$$SIR_{dB} = 10\log_{10}\left(\frac{P_c}{P_i}\right) \quad (5)$$

ค่า P_c และ P_i ที่โนด IEEE 802.15.4 ปลายทาง สามารถคำนวณได้จากค่ากำลังส่งที่โนดต้นทางลบด้วยค่ากำลังสูญเสียตามระยะทาง (path loss) โดยใช้ path loss model ตาม [14] ดังนี้

$$P_l(d) = \begin{cases} 20\log_{10}\left(\frac{4\pi d}{\lambda}\right) & , d \le 8m \\ 20\log_{10}\left(\frac{4\pi d}{\lambda}\right) + 33\log_{10}\left(\frac{d}{8}\right) & , d > 8m \end{cases} \quad (6)$$

โดย $P_l(d)$ คือ กำลังสูญเสียที่ถูกลดทอน (attenuation) ตามระยะทาง d มีหน่วยเป็น dB

d คือ ระยะทางระหว่างโนดต้นทางกับโนดปลายทาง มีหน่วยเป็น m

λ คือ ความยาวคลื่นของสัญญาณพาห์ มีหน่วยเป็น m

นอกจากนี้ การที่แบนด์วิดท์ของช่องสัญญาณ IEEE 802.11b กว้างกว่าแบนด์วิดท์ของช่องสัญญาณ IEEE 802.15.4 อยู่มาก (22 MHz และ 2 MHz ตามลำดับ) ดังนั้นพลังงานของสัญญาณ IEEE 802.11b เพียงบางส่วนเท่านั้นที่จะอยู่ในช่วงแบนด์วิดท์ของช่องสัญญาณ IEEE 802.15.4 และเนื่องจาก power spectral density ของ IEEE 802.11b ไม่ได้กระจายแบบเอกรูป (uniform) ตลอดช่วงแบนด์วิดท์ 22 MHz ดังนั้น ค่า spectrum factor ซึ่งเป็นค่าสัดส่วนของพลังงานจากสัญญาณ IEEE 802.11b ที่อยู่ในช่วงแบนด์วิดท์ของช่องสัญญาณ IEEE 802.15.4 จะแตกต่างกันขึ้นอยู่กับค่า frequency offset หรือความห่างระหว่างความถี่กลาง (center frequency) ของช่องสัญญาณ IEEE 802.11b กับช่องสัญญาณ IEEE 802.15.4

งานวิจัย [15] ได้คำนวณหาค่า spectrum factor ระหว่างเครือข่าย IEEE 802.11b กับเครือข่าย IEEE 802.15.4 ตามแต่ละค่า frequency offset ซึ่งสามารถสรุปได้ดังตารางที่ 3.1

ตารางที่ 3.1 ค่า spectrum factor เปรียบเทียบกับค่า frequency offset

IEEE 802.15.4		IEEE 802.11b		frequency offset	spectrum factor
ช่องสัญญาณ	ความถี่กลาง	ช่องสัญญาณ	ความถี่กลาง		
11	2405	1	2412	7	0.040997
12	2410	1	2412	2	0.169460
13	2415	1	2412	3	0.147610
14	2420	1	2412	8	0.022485
15	2425	6	2437	12	0
16	2430	6	2437	7	0.040997
17	2435	6	2437	2	0.169460
18	2440	6	2437	3	0.147610
19	2445	6	2437	8	0.022485
20	2450	11	2462	12	0
21	2455	11	2462	7	0.040997
22	2460	11	2462	2	0.169460
23	2465	11	2462	3	0.147610
24	2470	11	2462	8	0.022485
25	2475	11	2462	13	0
26	2480	11	2462	18	0

ดังนั้น ค่า P_c และ P_i ที่โนด IEEE 802.15.4 ปลายทาง สามารถคำนวณได้ ดังนี้

$$P_c = \left(P_{t,c} - P_{l,c}(d_c)\right) \quad (7)$$

$$P_i = spectrum\ factor \times \left(P_{t,i} - P_{l,i}(d_i)\right) \quad (8)$$

โดย $P_{t,c}$ คือ กำลังส่งของสัญญาณพาห์

$P_{l,c}(d_c)$ คือ ค่า path loss ของสัญญาณพาห์ (คำนวณจากสมการ (6))

d_c คือ ระยะทางระหว่างโนด IEEE 802.15.4 ต้นทางกับปลายทาง

$P_{t,i}$ คือ กำลังส่งของสัญญาณแทรกสอด

$P_{l,i}(d_i)$ คือ ค่า path loss ของสัญญาณแทรกสอด (คำนวณจากสมการ (6))

d_i คือ ระยะทางระหว่างโนดส่งของสัญญาณแทรกสอด กับโนด IEEE 802.15.4 ปลายทาง

บทที่ 4

ผลการวิจัย

การวิเคราะห์สมรรถนะของวิธีที่เสนอ จะใช้การเปรียบเทียบสมรรถนะของวิธีที่เสนอเปรียบเทียบกับวิธี ED และวิธี CS ซึ่งเป็นวิธีแบบเดิมสำหรับการทำ CCA ที่กำหนดอยู่ในมาตรฐาน IEEE 802.15.4 โดยใช้การสร้างแบบจำลองการทำงานของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เมื่อใช้วิธีที่เสนอ วิธี ED และวิธี CS ในการควบคุมการเข้าถึงช่องสัญญาณ และสร้างแบบจำลองการทำงานของเครือข่าย IEEE 802.11b เพื่อใช้เป็นสัญญาณแทรกสอด

เนื้อหาภายในบทนี้จะอธิบายถึงแบบจำลองการทำงานของเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b ที่ใช้ในการจำลองการทำงาน และแสดงการวิเคราะห์ผลที่ได้จากการจำลองเครือข่ายเปรียบเทียบระหว่างวิธีที่เสนอ กับวิธี ED และวิธี CS

4.1 แบบจำลองเครือข่ายที่ใช้ในการทดสอบ

เพื่อให้การวิเคราะห์ผลจากการจำลองเครือข่ายของวิธีที่เสนอ วิธี ED และวิธี CS สามารถวิเคราะห์ความแตกต่างได้อย่างชัดเจน งานวิจัยนี้จะแบ่งรูปแบบการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b ออกเป็น 4 scenario ดังนี้

Scenario 1: สัญญาณแทรกสอดส่งผลให้การส่งแพ็กเกตข้อมูลล้มเหลว โดยที่โนดส่งสามารถตรวจจับสัญญาณแทรกสอดนี้ได้

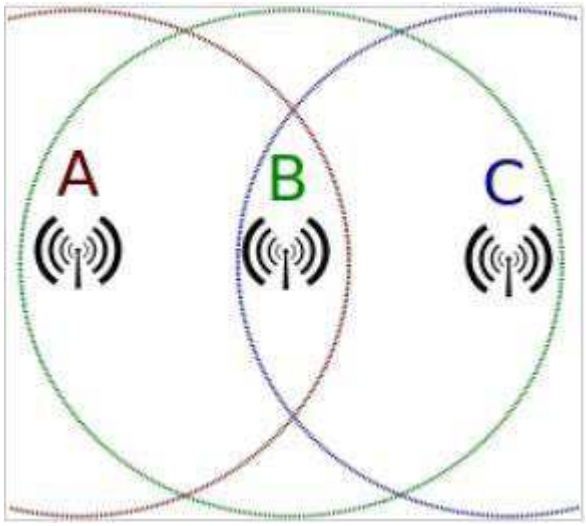
Scenario 2: สัญญาณแทรกสอดส่งผลให้การส่งแพ็กเกตข้อมูลล้มเหลว โดยที่โนดส่งไม่สามารถตรวจจับสัญญาณแทรกสอดนี้ได้

Scenario 3: สัญญาณแทรกสอดไม่ทำให้การส่งแพ็กเกตข้อมูลล้มเหลว แต่โนดส่งสามารถตรวจจับสัญญาณแทรกสอดนี้ได้

Scenario 4: สัญญาณแทรกสอดไม่ทำให้การส่งแพ็กเกตข้อมูลล้มเหลว และโนดไม่ส่งสามารถตรวจจับสัญญาณแทรกสอดนี้ได้ รวมถึงกรณีที่ไม่มีการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b เกิดขึ้น

ทั้งนี้จะถือว่าเครือข่าย IEEE 802.15.4 เป็นผู้ได้รับผลกระทบ โดยมีเครือข่าย IEEE 802.11b เป็นสัญญาณแทรกสอดเท่านั้น เนื่องจากถือว่าเครือข่าย IEEE 802.11b จะไม่ได้รับผลกระทบจากการแทรกสอดโดยเครือข่าย IEEE 802.15.4 จากการศึกษาใน [5]

นอกจากนี้ กรณี Scenario 2 ไม่สามารถใช้วิธีที่เสนอเพื่อช่วยลดผลกระทบจากการแทรกสอดได้ เนื่องจากโนดส่งไม่สามารถตรวจจับสัญญาณแทรกสอดได้ ซึ่งความจริงแล้วไม่ว่าวิธีการใดที่ใช้กลไก CSMA-CA ตามรูปแบบเดิมของมาตรฐาน IEEE 802.15.4 ล้วนไม่สามารถแก้ปัญหาการแทรกสอดในกรณีนี้ได้ ซึ่ง Scenario 2 นี้มีลักษณะใกล้เคียงกับปัญหา hidden node ของเครือข่าย IEEE 802.11 ซึ่ง Access Point (AP) สามารถมองเห็นโนดทั้งหมดในเครือข่ายได้ แต่บางโนดในเครือข่ายอาจไม่สามารถมองเห็นกันเองได้ ตัวอย่างปัญหา hidden node แสดงดังรูปที่ 4.1 ซึ่งโนด A และโนด C สามารถตรวจจับสัญญาณกับโนด B ได้ แต่ไม่สามารถตรวจจับสัญญาณระหว่างกันได้ จึงอาจเกิดปัญหาขึ้นหากโนด A และ โนด C ต้องการส่งข้อมูลไปให้โนด B พร้อมๆกัน ดังนั้น ขอบเขตของงานวิจัยนี้จะไม่ครอบคลุมกรณี Scenario 2 ด้วยเหตุผลข้างต้น



รูปที่ 4.1 ตัวอย่างการเกิดปัญหา hidden node

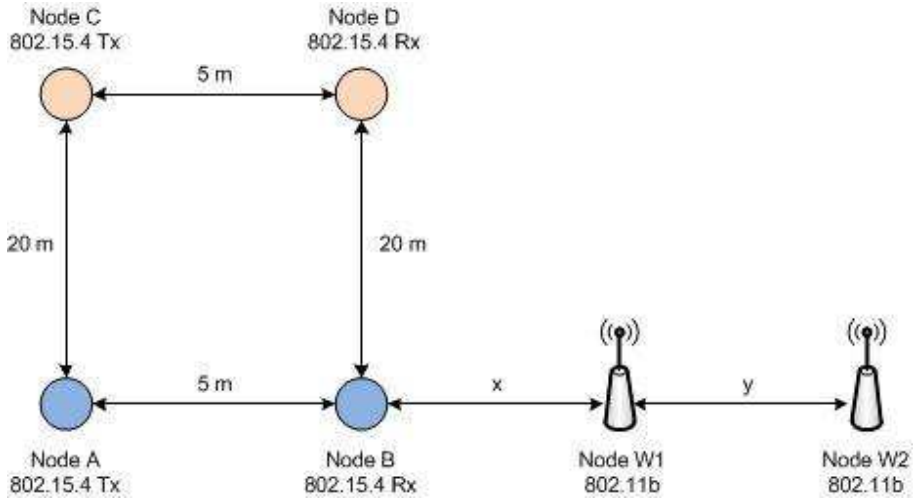
สำหรับกรณี Scenario 3 วิธีที่เสนอควรจะมีสมรรถนะดีกว่าวิธี ED เนื่องจากโนดส่งสามารถส่งแพ็กเกตข้อมูลไปยังโนดรับได้ แม้ว่าในขณะนั้นจะมีการแทรกสอดจากเครือข่าย IEEE 802.11b อยู่ก็ตาม หากพลังงานของสัญญาณแทรกสอดดังกล่าวต่ำกว่าค่า ED threshold ซึ่งเป็นค่าพลังงานต่ำที่สุดที่ส่งผลให้การส่งแพ็กเกตข้อมูลไปยังโนดรับดังกล่าวล้มเหลว ดังนั้น หากสัญญาณแทรกสอดมีพลังงานต่ำกว่าค่า ED threshold การส่งแพ็กเกตข้อมูลก็น่าจะสำเร็จ

กรณี Scenario 1 วิธีที่เสนอกับวิธี ED ควรจะมีสมรรถนะใกล้เคียงกัน เนื่องสัญญาณแทรกสอดส่งผลให้การส่งข้อมูลล้มเหลว โนดส่งจึงไม่สามารถส่งแพ็กเกตข้อมูลได้ระหว่างที่มีสัญญาณแทรกสอด

ส่วนกรณี Scenario 4 แม้ว่าจะมีการแทรกสอดหรือไม่ก็ตาม แต่ผลจากการแทรกสอดจะเสมือนกับไม่มีการแทรกสอดเกิดขึ้น เนื่องจากจะไม่เกิดทั้ง Inhibition Loss และ Collision Loss ดังนั้น วิธีที่เสนอ วิธี ED และวิธี CS จะมีสมรรถนะเช่นเดียวกันทั้งหมด

อย่างไรก็ตาม ในการประยุกต์ใช้งานจริง การแทรกสอดจากเครือข่าย IEEE 802.11b/g มักจะไม่อยู่ใน Scenario ใดตลอดเวลา โดยสามารถเปลี่ยนแปลงระหว่าง 4 scenario ข้างต้นได้ตลอดเวลา เช่น เครือข่าย Wi-Fi ซึ่งในช่วงเวลาหนึ่งจะมีโนดที่สามารถใช้งานช่องสัญญาณได้เพียงโนดเดียวเท่านั้น ดังนั้นในพื้นที่ที่มีผู้ใช้งานเครือข่าย Wi-Fi จำนวนมาก สัญญาณแทรกสอดมีแนวโน้มจะเปลี่ยนแปลงระหว่างทั้ง 4 scenario ตลอดเวลา ขึ้นอยู่กับตำแหน่งของโนดที่กำลังส่งแพ็กเกตข้อมูลอยู่ในขณะนั้น

ในการจำลองการทำงานของวิธีที่เสนอเปรียบเทียบกับวิธี ED และวิธี CS จะใช้การจำลองการทำงานของเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b โดยทั้งสองเครือข่ายจะมีการแทรกสอดซึ่งกันและกัน นั่นคือจะมีการใช้งานแถบความถี่ซ้อนทับกันในช่วงเวลาเดียวกัน สำหรับเครือข่าย IEEE 802.15.4 จะกำหนดโนด IEEE 802.15.4 จำนวน 2 คู่ คือ ในคู่ที่ 1 จะมีโนด A เป็นโนดส่ง และโนด B เป็นโนดรับ และคู่ที่ 2 มีโนด C เป็นโนดส่ง และโนด D เป็นโนดรับ โดยคู่ของโนด A และโนด B จะเป็นทราฟฟิกหลักในการพิจารณา สำหรับคู่ของโนด C และโนด D จะจำลองการทำงานขึ้นมาเพื่อให้เป็นการแทรกสอดภายในเครือข่าย IEEE 802.15.4 ด้วยกันเท่านั้น ซึ่งถือเป็นเรื่องปกติของเครือข่ายเซ็นเซอร์ไร้สาย IEEE 802.15.4 ที่โนดข้างเคียงกันอาจต้องการส่งแพ็กเกตข้อมูลพร้อมๆกันได้ สำหรับเครือข่าย IEEE 802.11b จะกำหนดโนด IEEE 802.11b จำนวน 1 คู่ คือ โนด W1 และโนด W2 ซึ่งจะสลับกันเป็นโนดส่งและโนดรับตลอดช่วงของการจำลองการทำงาน โดยจะกำหนดรูปแบบของเครือข่ายและตำแหน่งของโนดทั้งหมด รวมทั้งเพื่อให้เกิดสภาวะการแทรกสอดทั้งกรณี Scenario 1 และ Scenario 3 ซึ่งมีผลกระทบต่อสมรรถนะของเครือข่าย IEEE 802.15.4 ดังรูปที่ 4.2 โดยจะไม่ทดสอบ Scenario 2 ด้วยเหตุผลที่กล่าวไปแล้วข้างต้น อย่างไรก็ตาม ด้วยรูปแแบบจำลองการแทรกสอดที่ใช้ในงาวิจัยนี้จะไม่ทำให้เกิดการแทรกสอดในกรณี Scenario 2 อยู่แล้ว สำหรับการทดสอบ Scenario 4 จะทำโดยการกำหนดช่วงเวลาที่เกิดการแทรกสอดเพื่อเปรียบเทียบสมรรถนะระหว่างช่วงที่เกิดการแทรกสอดกับช่วงที่ไม่เกิดการแทรกสอดของวิธีที่เสนอ วิธี ED และวิธี CS



รูปที่ 4.2 รูปแบบเครือข่ายที่ใช้ในการจำลองการทำงาน

ทั้งนี้ การสลับโนด W1 และโนด W2 ให้เป็นทั้งโนดส่งและโนดรับ ก็เพื่อให้เกิดการแทรกสอดได้ 2 scenario พร้อมๆกัน โดยตำแหน่งของโนด W1 และโนด W2 จะปรับเปลี่ยนไปขึ้นอยู่กับการทดสอบแต่ละครั้งว่าต้องการให้การแทรกสอดจากโนด W1 และโนด W2 เป็น scenario โดยจะถือว่าโนด W1 เป็นตัวแทนของการแทรกสอดกรณี scenario หนึ่ง และโนด W2 เป็นตัวแทนของการแทรกสอดกรณีในอีก scenario หนึ่ง ซึ่งการสลับการเป็นโนดส่งและโนดรับก็เพื่อให้สอดคล้องกับลักษณะการใช้งานจริงซึ่งภายในเครือข่าย IEEE 802.11 ใดๆ จะมีเพียงโนดเดียวที่สามารถส่งข้อมูลได้ในช่วงเวลาหนึ่ง ทำให้อาจเกิดการแทรกสอดใน scenario ที่แตกต่างกันสลับกันไปตลอดเวลา

สำหรับรูปแบบการทำงานของทั้งเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b จะจำลองการทำงานให้ใกล้เคียงกับกลไก CSMA/CA ของทั้ง 2 เครือข่าย ตามที่กำหนดไว้ [2] และ [3] ให้มากที่สุด โดยกรณีเครือข่าย IEEE 802.11b จะจำลองการทำงานในกรณี Basic Access เพื่อลดความซับซ้อน สำหรับค่าพารามิเตอร์ต่างๆที่ใช้ในการจำลองการทำงานของทั้ง 2 เครือข่ายนี้ จะใช้ค่าโดยปริยาย (Default value) ที่กำหนดไว้ใน [2] และ [3] เป็นหลัก

ในส่วนของลักษณะการส่งแพ็กเกตข้อมูล สำหรับเครือข่าย IEEE 802.15.4 ทั้งโนด A และโนด C ซึ่งเป็นโนดส่งในเครือข่าย IEEE 802.15.4 จะมีแพ็กเกตข้อมูลที่ต้องการส่งเกิดขึ้นทุกช่วงเวลาที่กำหนดโดยตัวแปรสุ่มแบบปัวส์ซอง (Poisson random variable) แม้ว่าการส่งแพ็กเกตข้อมูลเดิมจะยังไม่เสร็จสิ้นก็ตาม โดยจะทดสอบที่ค่า λ = 30 ms

สำหรับเครือข่าย IEEE 802.11b จะจำลองลักษณะการส่งแพ็กเกต ข้อมูลให้ส่งผลต่อเป็นกรณีเลวร้ายที่สุด (worst case scenario) นั่นคือแพ็กเกต IEEE 802.11b จะถูกส่งอย่างต่อเนื่องโดยทันทีที่การส่งแพ็กเกตข้อมูลครั้งล่าสุดเสร็จสิ้น และใช้วิธี CS ในการตรวจสอบช่องสัญญาณ นั่นคือเครือข่าย IEEE 802.11b จะไม่สนใจทราฟฟิกของเครือข่าย IEEE 802.15.4 ในการพยายามเข้าถึงช่องสัญญาณ ในส่วนของการสลับการเป็นโนดส่งและโนดรับระหว่างโนด W1 กับโนด W2 จะถูกควบคุมโดยพารามิเตอร์ *Consecutive_Packet* ซึ่งเป็นค่าของจำนวนแพ็กเกตข้อมูลที่โนดนั้นๆจะทำการส่งต่อเนื่องก่อนที่จะสลับไปเป็นโนดรับ และสลับโนดรับเดิมมาเป็นโนดส่งแทน พารามิเตอร์ *Consecutive_Packet* จะกำหนดโดยตัวแปรสุ่มแบบปัวส์ซองซึ่งมีค่า λ เท่ากับ 5 แพ็กเกต และปัดให้เป็นเลขจำนวนเต็มโดยใช้ฟังก์ชัน round

สำหรับช่องสัญญาณที่ใช้ในการจำลองการทำงาน สำหรับเครือข่าย IEEE 802.15.4 จะใช้ช่องสัญญาณที่ 12 ซึ่งมีความถี่กลาง 2,410 MHz และเครือข่าย IEEE 802.11b ใช้ช่องสัญญาณที่ 1 ซึ่งมีความถี่กลาง 2,412 MHz เพื่อให้มีค่า frequency offset ต่ำที่สุด คือ 2 MHz ซึ่งเป็นค่า frequency offset ที่ต่ำที่สุดที่เป็นไปได้ (พิจารณาตารางที่ 3.1 ประกอบ) ซึ่งจะทำให้ผลกระทบจากการแทรกสอดรุนแรงที่สุด

สรุปค่าพารามิเตอร์สำคัญในการจำลองเครือข่ายได้ดังตารางที่ 4.1

ตารางที่ 4.1 พารามิเตอร์สำคัญในการจำลองเครือข่าย

พารามิเตอร์	**IEEE 802.15.4**	**IEEE 802.11b**
กำลังส่ง	0 dBm	14 dBm
วิธี CCA	วิธีที่เสนอ/ ED / CS	CS
ความไวในการรับสัญญาณ	-85 dBm	-76 dBm
อัตราข้อมูล	250 kbps	11 Mbps
ความถี่กลาง	2410 MHz	2412 MHz
ขนาดแพ็กเกตข้อมูล	22 bytes	1024 bytes
ขนาดแพ็กเกต ACK	11 bytes	14 bytes
รูปแบบการส่งข้อมูล	ทุกๆ Poisson($\lambda = 30$ ms)	ต่อเนื่อง
macMaxCSMAbackoffs	4	-
macMaxFrameRetries	3	-

ในการจำลองการทำงานจะแบ่งงานของแต่ละโนดคือ โนด A, B, C, D, W1 และ W2 แยกออกจากกัน โดยแต่ละโนดจะเก็บค่าตัวแปรต่างๆที่ใช้ในการจำลองการทำงานของตนไว้ในตัวแปร structure ของตนเอง การจำลองการทำงานจะมีลักษณะเป็นการวนลูป โดยจะกำหนดสถานะของแต่ละโนดขึ้นมาให้สอดคล้องตามการทำงานของกลไล CSMA/CA ของมาตรฐาน IEEE 802.15.4 และ IEEE 802.11b ซึ่งในแต่ละลูปของการจำลองการทำงานนั้น จะจำลองการทำงานเฉพาะโนดที่มีค่า time instant ต่ำที่สุดเพียงโนดเดียว และพิจารณาว่าปัจจุบันโนดดังกล่าวอยู่ในสถานะใด ซึ่งในแต่ละสถานะจะกำหนดขั้นตอนการทำงานและระยะเวลาการทำงานในสถานะนั้นๆเอาไว้ หากสถานะใดที่การทำงานโนดนั้นๆต้องเกี่ยวข้องกับโนดอื่นๆก็จะดึงค่าตัวแปรของโนดที่เกี่ยวข้องมาใช้ในการจำลองการทำงานด้วย เมื่อเสร็จสิ้นขั้นตอนการทำงานในสถานะนั้นๆ ก็จะเพิ่มค่า time instant ของโนดดังกล่าวตามระยะเวลาทำงานของสถานะนี้ และเปลี่ยนตัวแปรสถานะของโนดดังกล่าวเป็นสถานะถัดไปตามรูปแบบของกลไก CSMA/CA จากนั้นก็จะวนลูปใหม่โดยจำลองการทำงานสำหรับโนดที่มีค่า time instant ต่ำสุดอีกครั้ง

สถานะที่มีความเกี่ยวข้องกันระหว่างหลายโนดนั้นจะเป็นสถานะที่เกี่ยวข้องกับกระบวนงาน CCA ซึ่งต้องมีการตรวจสอบสัญญาณจากโนดอื่นๆที่ใช้งานช่องสัญญาณอยู่ในขณะนั้น และสถานะที่เกี่ยวข้องกับการส่งแพ็กเกตข้อมูล ซึ่งต้องตรวจสอบว่ามีสัญญาณจากโนดอื่นๆที่ใช้งานช่องสัญญาณอยู่หรือไม่ และหากเกิดการแทรกสอดขึ้นจะส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลของโนดใดบ้าง ซึ่งการแทรกสอดดังกล่าวส่งผลกระทบต่อโนดที่ไม่ได้อยู่ระหว่างการจำลองการทำงานในลูปนี้ ก็จะเข้าไปปรับเปลี่ยนค่าตัวแปรของโนดนั้นๆทันที เช่น ในลูปก่อนหน้าโนด A ส่งแพ็กเกตข้อมูลไปแล้วและอยู่ในสถานะรอสัญญาณ ACK (waiting_for_ACK) แต่ในลูปถัดไป โนด W1 ได้ทำการส่งแพ็กเกตข้อมูลด้วย ส่งผลให้การส่งแพ็กเกตข้อมูลของ A ในลูปก่อนหน้าล้มเหลว ก็จะเข้าไปปรับเปลี่ยนตัวแปรของโนด A จากสถานะรอสัญญาณ ACK เป็นสถานะการส่งล้มเหลว (NACK) ทันที ดังนั้น เมื่อถึงรอบการจำลองการทำงานของโนด A อีกครั้ง โนด A จะทำงานต่อไปในสถานการส่งล้มเหลว

สรุปสถานะทั้งหมดที่ใช้ในแบบจำลองเครือข่ายได้ดังนี้

<u>เครือข่าย IEEE 802.15.4</u>

1. สถานะ idle - เป็นสถานะที่โนดอยู่ในระหว่างรอการเริ่มต้นส่งแพ็กเกตข้อมูล ในสถานะ idle จะทำการสุ่มค่า time instant ที่จะเริ่มส่งแพ็กเกตข้อมูลครั้งถัดไป และตั้งค่าสถานะถัดไปเป็นสถานะ start_send_packet

2. สถานะ start_send_packet - เป็นสถานะเริ่มต้นกระบวนการส่งแพ็กเกตข้อมูล โดยจะกำหนด packet_ID ของแพ็กเกตที่กำลังจะส่ง และตั้งค่าสถานะถัดไปเป็นสถานะ start_backoff
3. สถานะ retransmission - มีรูปแบบการทำงานใกล้เคียงกับสถานะ start_send_packet แต่จะเป็นการเริ่มต้นกระบวนการส่งแพ็กเกตข้อมูลในกรณีที่เป็นการส่งซ้ำ (Retransmission) ดังนั้นในสถานะ retransmission จะใช้ packet_ID เดิม และตั้งค่าสถานะถัดไปเป็นสถานะ start_backoff
4. สถานะ start_backoff – เป็นสถานะเริ่มต้นการ backoff โดยจะเป็นการกำหนดค่าพารามิเตอร์เริ่มต้นต่างๆที่ใช้ในการ backoff และทำการ backoff รอบแรก สถานะถัดไปจะเป็นสถานะ start_CCA
5. สถานะ backoff – เป็นสถานะสำหรับการ backoff รอบที่ 2 เป็นต้นไป ซึ่งจะเกิดขึ้นกรณีที่ในการ backoff รอบแรก CCA ตรวจพบว่าช่องสัญญาณไม่ว่าง สถานะถัดไปจะเป็นสถานะ start_CCA
6. สถานะ start_CCA – เป็นสถานะเริ่มต้นการทำ CCA โดยจะเป็นการกำหนดค่าพารามิเตอร์เริ่มต้นต่างๆสำหรับการทำ CCA สถานะถัดไปจะเป็นสถานะ perform_CCA
7. สถานะ perform_CCA – เป็นสถานะของการทำ CCA คือ ตรวจสอบช่องสัญญาณว่าว่างหรือไม่ ตามวิธี CCA ที่กำหนดในสถานะ start_CCA ซึ่งผลที่ได้จากการทำ CCA จะเป็นตัวกำหนดสถานะถัดไป คือ หากการทำ CCA ตรวจพบว่าช่องสัญญาณไม่ว่าง สถานะถัดไปจะเป็นสถานะ CCA_busy แต่หากตรวจพบว่าช่องสัญญาณว่างอยู่ สถานะถัดไปจะเป็นสถานะ CCA_idle
8. สถานะ CCA_busy – เป็นขั้นตอนที่ CCA รายงานผลว่าช่องสัญญาณไม่ว่าง และต้องกลับไปทำการ backoff ใหม่ คือ กลับไปสู่สถานะ backoff
9. สถานะ CCA_idle – เป็นขั้นตอนที่ CCA รายงานผลว่าช่องสัญญาณว่าง และพร้อมจะส่งแพ็กเกตข้อมูลได้ทันที สถานะถัดไปคือ start_transmit_packet
10. สถานะ start_transmit_packet – เป็นสถานะที่โนดเริ่มต้นการส่งแพ็กเกตข้อมูลผ่านช่องสัญญาณ และตรวจสอบว่าการส่งแพ็กเกตข้อมูลดังกล่าวสำเร็จหรือไม่ รวมถึง

ส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลของโนดอื่นๆหรือไม่ หากผลการตรวจสอบพบว่าการส่งแพ็กเกตข้อมูลล้มเหลว สถานะถัดไปจะเป็นสถานะ fail_transmit_packet แต่หากผลการตรวจสอบพบว่าการส่งแพ็กเกตข้อมูลสำเร็จ สถานะถัดไปจะเป็นสถานะ finish_transmit_packet

11. สถานะ finish_transmit_packet – เป็นสถานะที่โนดต้นทางส่งแพ็กเกตข้อมูลเสร็จสิ้นและโนดปลายทางได้รับแพ็กเกตข้อมูลอย่างสมบูรณ์ และเตรียมส่งแพ็กเกต ACK กลับไปให้โนดต้นทาง ดังนั้นในสถานะนี้จะสลับโนดปลายทางเดิมมาเป็นโนดส่ง เพื่อส่ง ACK ไปให้โนดต้นทางเดิม โดยจะกำหนดสถานะถัดไปของโนดปลายทางเดิมเป็นสถานะ start_transmit_ack ในขณะที่โนดต้นทางเดิมจะเปลี่ยนสถานะจาก finish_transmit_packet เป็นสถานะ waiting_for_ack
12. สถานะ fail_transmit_packet – เป็นสถานะที่โนดต้นทางส่งแพ็กเกตข้อมูลเสร็จสิ้นและโนดปลายทางไม่ได้รับแพ็กเกตข้อมูล (การส่งล้มเหลว) ดังนั้น โนดปลายทางจะไม่มีการทำงานใดๆ ในขณะที่โนดต้นทางจะเปลี่ยนสถานะจาก fail_transmit_packet เป็น waiting_for_ack (เนื่องจากในการทำงานจริง โนดต้นทางจะไม่ทราบว่าการส่งแพ็กเกตข้อมูลสำเร็จหรือไม่ในขั้นตอนนี้ และจำเป็นต้องรอแพ็กเกต ACK ตามระยะเวลาที่กำหนด)
13. สถานะ start_transmit_ack – เป็นสถานะที่โนดปลายทางเริ่มต้นส่งแพ็กเกต ACK เพื่อแจ้งกลับโนดต้นทางว่าได้รับแพ็กเกตข้อมูลแล้ว รวมทั้งจะมีการตรวจสอบผลของการส่งแพ็กเกต ACK ในลักษณะเดียวกับในสถานะ start_transmit_packet หากผลการตรวจสอบพบว่าการส่งแพ็กเกต ACK ล้มเหลว สถานะถัดไปจะเป็นสถานะ fail_transmit_ack แต่หากผลการตรวจสอบพบว่าการส่งแพ็กเกต ACK สำเร็จ สถานะถัดไปจะเป็นสถานะ finish_transmit_ack
14. สถานะ finish_transmit_ack – เป็นสถานะที่โนดปลายทางเดิมส่งแพ็กเกต ACK เสร็จสิ้นและโนดต้นทางเดิมได้รับแพ็กเกต ACK อย่างสมบูรณ์ โดยจะกำหนดสถานะถัดไปของโนดปลายทางเดิมเป็นสถานะ idle และกำหนดสถานะถัดไปของโนดต้นทางเดิมเป็นสถานะ ack_received
15. สถานะ fail_transmit_ack – เป็นสถานะที่โนดปลายทางเดิมส่งแพ็กเกต ACK เสร็จสิ้นแล้ว แต่โนดต้นทางเดิมไม่ได้รับแพ็กเกต ACK ดังกล่าว (การส่ง ACK ล้มเหลว)

ดังนั้น โนดต้นทางเดิมจะไม่มีการเปลี่ยนแปลงสถานะใดๆ (ยังอยู่ในสถานะ waiting_for_ack) แต่โนดปลายทางเดิมจะเปลี่ยนสถานะถัดไปเป็น idle เนื่องจากถือว่าได้รับแพ็กเกตข้อมูลและส่งแพ็กเกต ACK เสร็จสิ้นแล้ว (ในกรณีนี้ถือว่าการส่งแพ็กเกตข้อมูลของโนดต้นทางสำเร็จแล้ว แต่เนื่องจากโนดต้นทางไม่ได้รับแพ็กเกต ACK จึงทำการส่งซ้ำอีกครั้ง ซึ่งแพ็กเกตข้อมูลเดิมที่เคยส่งสำเร็จไปแล้ว และทำส่งซ้ำจนสำเร็จอีกครั้งจะนำมานับในการคำนวณ throughput เพียงครั้งแรกครั้งเดียว เนื่องจากในการคำนวณ throughput จะใช้ packet_ID ในการนับว่ามีการส่งแพ็กเกตข้อมูลสำเร็จกี่แพ็กเกต)

16. สถานะ waiting_for_ack – เป็นสถานะที่โนดต้นทางอยู่ในระหว่างการรอแพ็กเกต ACK จากโนดปลายทาง โดยจะรอเป็นระยะเวลาเท่ากับจำนวน symbol ที่กำหนดโดยพารามิเตอร์ *macAckWaitDuration* ซึ่งหากโนดต้นทางอยู่ในสถานะนี้จนหมดเวลาดังกล่าว จะถือว่าไม่ได้รับแพ็กเกต ACK ภายในระยะเวลาที่กำหนด และกำหนดสถานะถัดไปเป็น NACK แต่หากโนดต้นทางได้รับแพ็กเกต ACK ก่อนหมดระยะเวลาดังกล่าว สถานะของโนดต้นทางจะถูกเปลี่ยนเป็น ack_received จากการทำงานของสถานะ finish_transmit_ack โดยโนดปลายทางไปแล้ว

17. สถานะ ack_received – เป็นสถานะที่โนดต้นทางได้รับแพ็กเกต ACK และถือว่าการส่งแพ็กเกตข้อมูลครั้งนี้เสร็จสิ้นสมบูรณ์ และจะตั้งค่าพารามิเตอร์ที่เกี่ยวข้องกลับเป็นค่าเริ่มต้น และเปลี่ยนสถานะถัดไปเป็น idle เพื่อรอการส่งแพ็กเกตข้อมูลถัดไป

18. สถานะ NACK – เป็นสถานะที่โนดต้นทางไม่ได้รับแพ็กเกต ACK ภายในระยะเวลาที่กำหนด จึงถือว่าการส่งแพ็กเกตข้อมูลครั้งนี้ล้มเหลว โดยในการจำลองการทำงานของวิธี ED และ CS สถานะถัดไปของ NACK จะเป็น retransmission เสมอ แต่ในกรณีของวิธีที่เสนอ สถานะถัดไปจะเป็น retransmission จนกว่าจำนวนครั้งที่โนดต้นทางไม่ได้รับแพ็กเกต ACK สูงกว่าค่า threshold ที่กำหนด ซึ่งในกรณีดังกล่าว สถานะถัดไปจะเป็น ED_scan

19. สถานะ ED_scan – เป็นสถานะที่ใช้สำหรับวิธีที่เสนอเท่านั้น โดยเมื่อโนดต้นทางส่งแพ็กเกตข้อมูลไปแล้ว แต่ไม่ได้รับแพ็กเกต ACK เกินจำนวนครั้งที่กำหนด โนดต้นทางจะทำ ED scan เพื่อตรวจวัดระดับพลังงานของสัญญาณแทรกสอดในขณะนั้นมากำหนดเป็นค่า ED threshold และเมื่อดำเนินการดังกล่าวเสร็จสิ้นแล้ว หากจำนวน

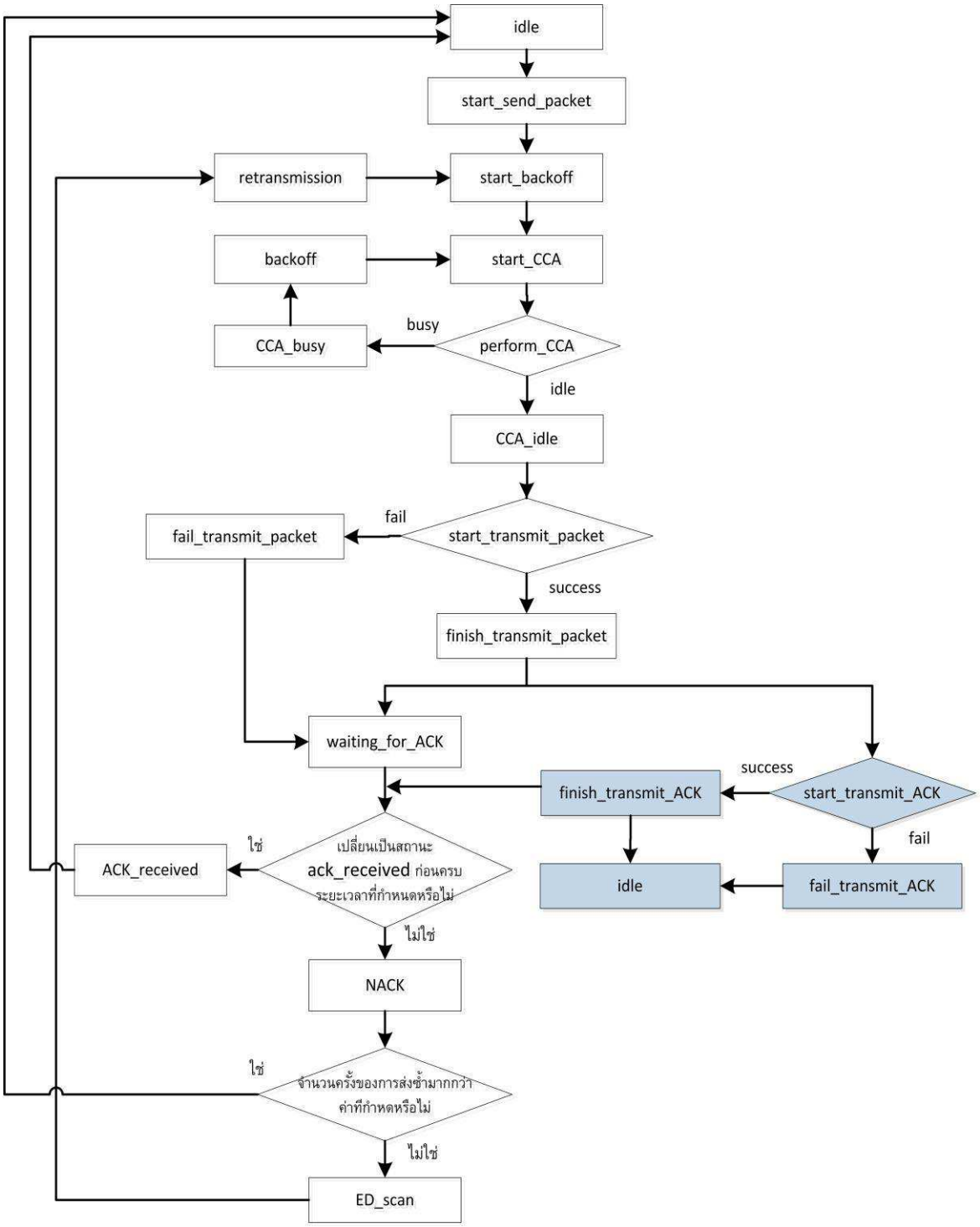
ครั้งของการส่งซ้ำที่ผ่านมา ยังไม่เกินค่าที่กำหนดใน *macMaxFrameRetries* จะกำหนดสถานะถัดไปเป็น retransmission แต่หากจำนวนครั้งของการส่งซ้ำเท่ากับบค่าที่กำหนดใน *macMaxFrameRetries* แล้ว สถานะถัดไปจะเป็น idle โดยที่ยังคงค่า ED threshold ดังกล่าวเอาไว้

<u>เครือข่าย IEEE 802.11b</u>

สถานะสำหรับเครือข่าย IEEE 802.11b จะใกล้เคียงกับเครือข่าย IEEE 802.15.4 เกือบทั้งหมด โดยจะแตกต่างกันอยู่เพียงบางสถานะ ดังนี้

1. สถานะ w_start_check_channel และ w_start_check_channel_2 – เป็นสถานะของการตรวจสอบช่องสัญญาณว่าว่างหรือไม่ เช่นเดียวกับการทำ CCA ของเครือข่าย IEEE 802.15.4 แต่จะแตกต่างกันที่กรณีเครือข่าย IEEE 802.11b การตรวจสอบช่องสัญญาณจะทำทันทีเมื่อเริ่มต้นกระบวนการส่งแพ็กเกตข้อมูล และเมื่อตรวจสอบพบว่าช่องสัญญาณไม่ว่างจึงค่อยทำการ backoff ในขณะที่เครือข่าย IEEE 802.15.4 จะทำการ backoff ทันทีในการเริ่มต้นกระบวนการส่งแพ็กเกตข้อมูล และจะตรวจสอบช่องสัญญาณหรือการทำ CCA ก็ต่อเมื่อเสร็จสิ้นการ backoff แล้ว
2. เครือข่าย IEEE 802.11b จะไม่มีสถานะ w_fail_transmit_packet และ w_fail_transmit_ack เนื่องจากถือว่าเครือข่าย IEEE 802.11b ไม่ได้รับผลกระทบจากการแทรกสอดจากเครือข่าย IEEE 802.15.4 ดังที่ได้กล่าวไปแล้วในช่วงต้นของหัวข้อ 4.1 นี้
3. เครือข่าย IEEE 802.11b จะไม่มีสถานะ w_ED_scan เนื่องจากเป็นสถานะที่ใช้สำหรับวิธีที่เสนอเท่านั้น

ขั้นตอนของโปรแกรมที่ใช้ในการจำลองการทำงานของวิธีที่เสนอแสดงดังผังงานในรูปที่ 4.3 ซึ่งเป็นการแสดงผังงานของการจำลองเครือข่าย IEEE 802.15.4 สำหรับรายละเอียดของการทำงานในแต่ละสถานะได้อธิบายไว้แล้วข้างต้น สำหรับผังงานของการจำลองเครือข่าย IEEE 802.11b จะมีลักษณะเดียวกับเครือข่าย IEEE 802.11b ยกเว้นบางสถานะที่จะมีความแตกต่างกันซึ่งได้อธิบายไปแล้วเช่นกัน



รูปที่ 4.3 ขั้นตอนของโปรแกรมที่ใช้ในการจำลองการทำงานของวิธีที่เสนอ

หมายเหตุ: ขั้นตอนที่ระบายสีฟ้าจะเป็นขั้นตอนที่ทำงานโดยโนดปลายทาง ซึ่งเป็นขั้นตอนที่เกี่ยวข้องกับการส่งสัญญาณ ACK

4.2 การวิเคราะห์ผลจากการจำลองเครือข่าย

การวิเคราะห์สมรรถนะของวิธีที่เสนอจะใช้การเปรียบเทียบสมรรถนะกับวิธี ED และวิธี CS โดยจะเปรียบเทียบโดยใช้ 3 พารามิเตอร์เป็นหลัก คือ ค่า throughput, อัตราความผิดพลาดในการส่งแพ็กเกตข้อมูล (Packet Error Rate: PER) และอัตราการเข้าถึงช่องสัญญาณล้มเหลว (Channel Access Failure Ratio) และอาจใช้พารามิเตอร์อื่นๆเพื่อช่วยในการวิเคราะห์ผลแล้วแต่กรณีไป

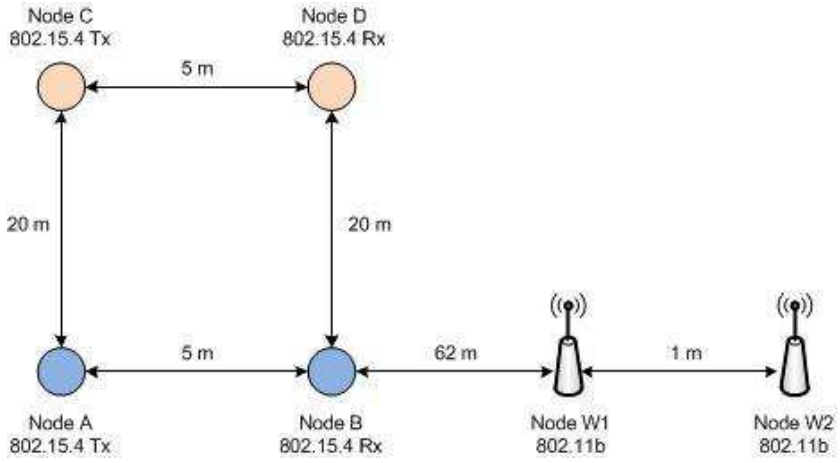
การวิเคราะห์ผลในขั้นแรกจะเปรียบเทียบสมรรถนะในกรณีมีการแทรกสอดที่มี scenario แตกต่างกัน พร้อมทั้งวิเคราะห์สมรรถนะของวิธีที่เสนอสำหรับการแทรกสอดในแต่ละ scenario จากนั้นจะนำ scenario ที่วิธีที่เสนอสามารถช่วยบรรเทาปัญหาจากการแทรกสอดได้มาวิเคราะห์ผลกระทบต่อสมรรถนะที่อาจเกิดจากพารามิเตอร์อื่นๆ เช่น ความหนาแน่นของแพ็กเกตข้อมูล ขนาดแพ็กเกตข้อมูล และกรณีที่เครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b มีค่า frequency offset อื่นๆ

ในการจำลองการทำงานของเครือข่าย จะตั้งค่าโปรแกรมให้จำลองการทำงานเสมือนว่าเครือข่ายทำงานเป็นระยะเวลา 180 วินาที โดยจะเริ่มมีสัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b ตั้งแต่วินาทีที่ 30 เป็นต้นไป และสัญญาณแทรกสอดดังกล่าวจะหายไปหลังจากวินาทีที่ 150 นั่นคือ จะมีช่วงที่เกิดการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b อยู่ 120 วินาที

4.2.1 การวิเคราะห์ผลจากการแทรกสอด Scenario ต่างๆ

ในหัวข้อนี้จะแสดงการจำลองการทำงานเพื่อเปรียบเทียบสมรรถนะของวิธีที่เสนอ วิธี ED และวิธี CS ในกรณีที่มีการแทรกสอด scenario แตกต่างกัน เพื่อแสดงให้เห็นข้อดี ข้อเสีย และความเหมาะสมของวิธีที่เสนอ วิธี ED และวิธี CS ที่มีต่อการแทรกสอดในแต่ละ scenario

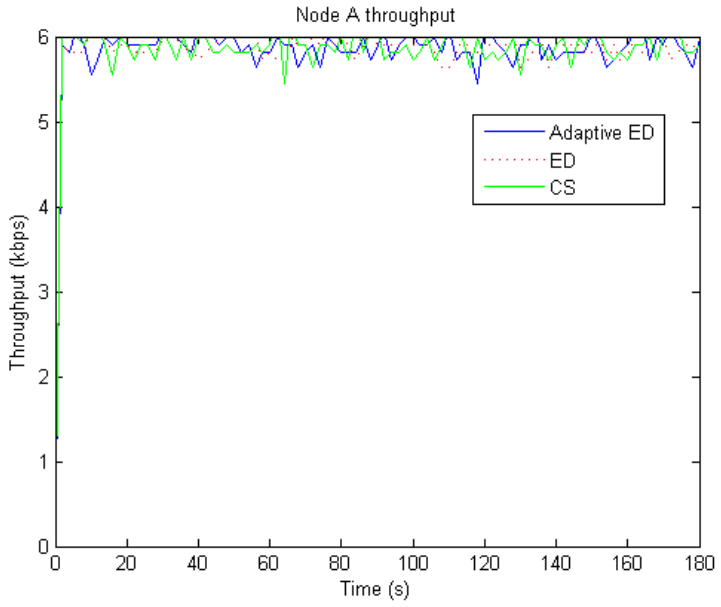
4.2.1.1 กรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2



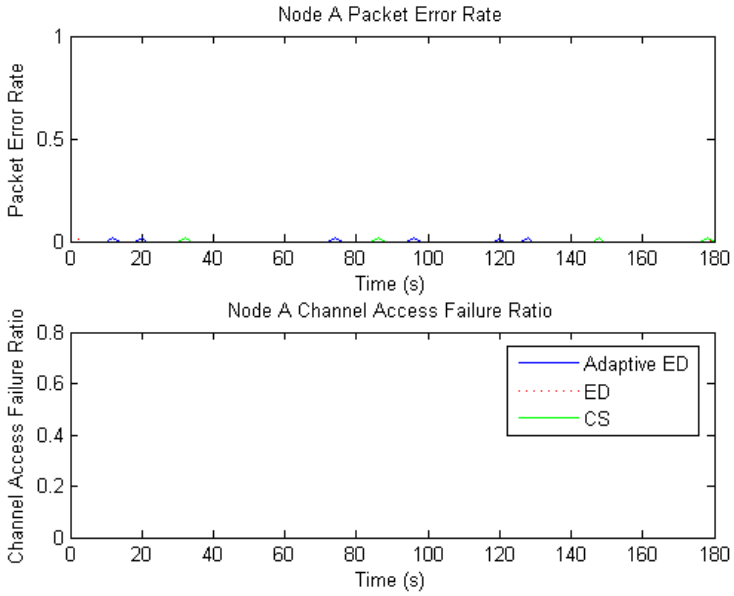
รูปที่ 4.4 รูปแบบเครือข่ายกรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2 แสดงดังรูปที่ 4.4 ซึ่งในกรณีนี้ ตลอดช่วงของการจำลองเครือข่าย จะไม่มีการแทรกสอดจากเครือข่าย IEEE 802.11b เกิดขึ้น เนื่องจากทราฟฟิกจากโนด W1 และโนด W2 จะไม่ส่งผลกระทบใดๆต่อเครือข่าย IEEE 802.15.4 ซึ่งการทดสอบในกรณีนี้นั้นเพื่อเปรียบเทียบสมรรถนะของวิธีที่เสนอ วิธี ED และวิธี CS ว่าแตกต่างกันหรือไม่ในกรณีที่ไม่มีการแทรกสอดเกิดขึ้น

ผลการจำลองเครือข่ายกรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2 แสดงดังกราฟในรูปที่ 4.5 และรูปที่ 4.6 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.2



รูปที่ 4.5 Throughput ของโนด A กรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2



รูปที่ 4.6 ค่า PER และ Channel Access Failure ratio ของโนด A
กรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2

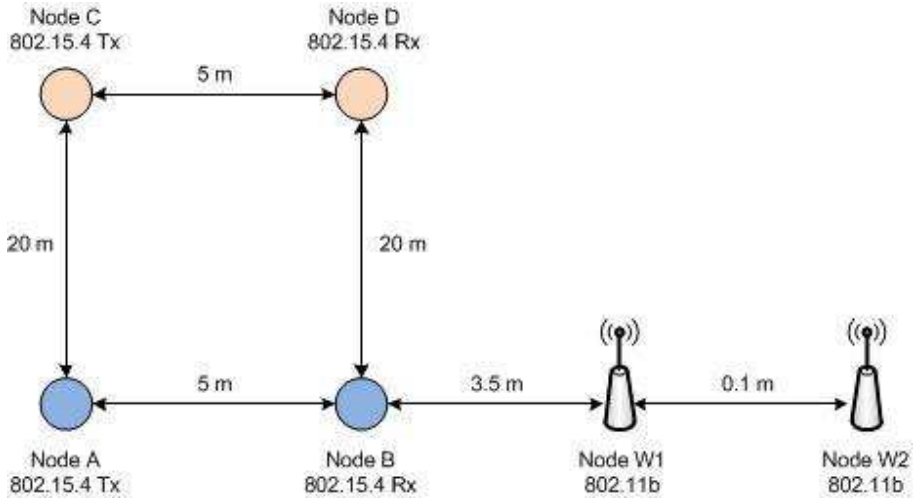
ตารางที่ 4.2 ผลการจำลองเครือข่ายกรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2

	Adaptive ED	ED	CS
Throughput	5.890	5.878	5.914
PER	0.001	0.001	0.001
Channel Access Failure ratio	0	0	0

จากผลการจำลองเครือข่ายจะเห็นได้ว่ากรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2 ค่า throughput ของโนด A สำหรับวิธีที่เสนอ วิธี ED หรือวิธี CS จะมีค่าใกล้เคียงกันทั้งหมด คือ 5.890 kbps 5.878 kbps และ 5.914 kbps ตามลำดับ และทั้ง 3 วิธีจะมีค่า PER ประมาณ 0.001 ซึ่งค่า PER ดังกล่าว เกิดจากการชนกันของแพ็กเกตข้อมูลจากโนด A กับแพ็กเกต ACK จากโนด D ทั้งนี้ เนื่องจากการส่งแพ็กเกต ACK นั้นจะเป็นการส่งทันทีโดยไม่มีการใช้กลไก CSMA-CA ดังนั้นจึงมีโอกาสที่จะเกิดกรณีที่แพ็กเกต ACK ชนกับแพ็กเกตข้อมูลจากโนดอื่นๆได้ สำหรับค่า Channel Access Failure ratio ของทั้ง 3 วิธีจะเท่ากับ 0 ทั้งหมด เนื่องจากไม่มีสัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b ซึ่งการแข่งกันเข้าถึงช่องสัญญาณภายในเครือข่าย IEEE 802.15.4 ด้วยกันนั้นแทบไม่ส่งผลให้เกิด Channel Access Failure ซึ่งจะเกิดขึ้นเมื่อโนดส่งไม่

สามารถเข้าถึงช่องสัญญาณได้หลังจากการพยายามเป็นจำนวนครั้งมากกว่า 4 ครั้ง (ใช้ค่า *macMaxCSMAbackoffs* เท่ากับ 4 ซึ่งเป็นค่าปริยายของมาตรฐาน IEEE 802.15.4)

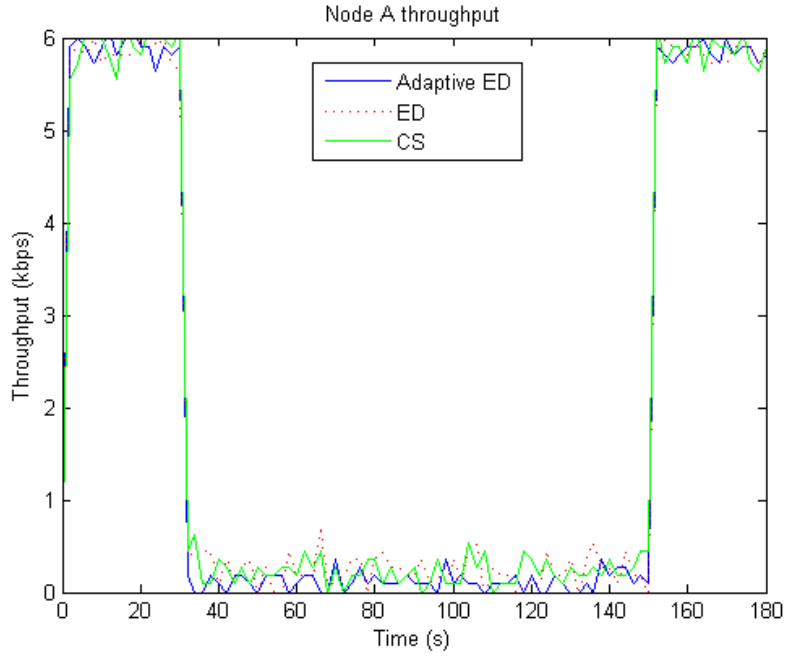
4.2.1.2 การแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1)



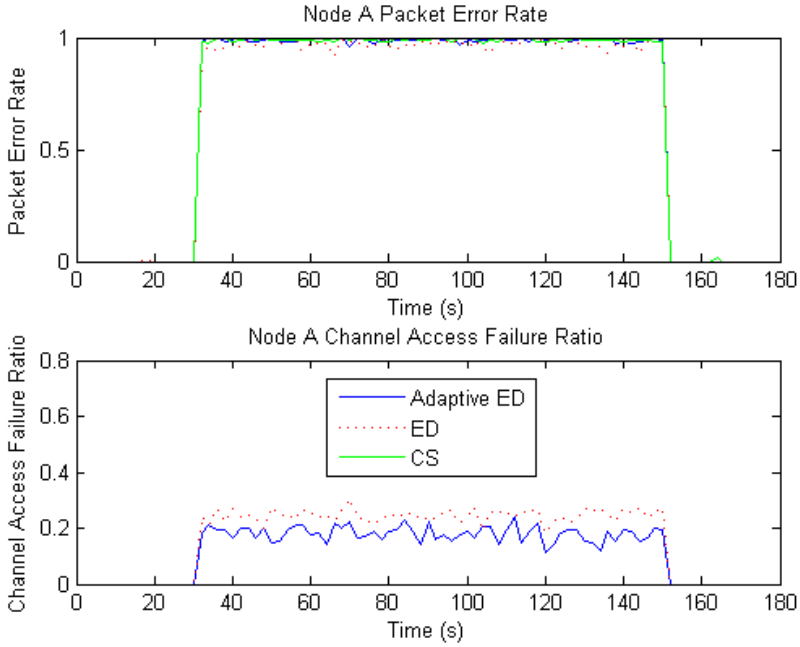
รูปที่ 4.7 รูปแบบเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1)

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1) แสดงดังรูปที่ 4.7 ซึ่งในกรณีนี้ การแทรกสอดจากโนด W1 และโนด W2 เป็นการแทรกสอดแบบ Scenario 1 ทั้งคู่ โดยการแทรกสอดจากทั้งโนด W1 และโนด W2 ล้วนทำให้การส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B เกิดความผิดพลาด 100% หรือมี PER=1 โดยที่โนด A สามารถตรวจจับสัญญาณแทรกสอดของทั้งโนด W1 และโนด W2 ได้ในการทำ CCA

ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1) แสดงดังกราฟในรูปที่ 4.8 และรูปที่ 4.9 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.3



รูปที่ 4.8 Throughput ของโนด A กรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1)



รูปที่ 4.9 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1)

ตารางที่ 4.3 ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1)

	Adaptive ED	ED	CS
Throughput	0.111	0.232	0.227
PER	0.990	0.971	0.990
Channel Access Failure ratio	0.181	0.246	0

จากผลการจำลองเครือข่ายจะเห็นว่าในช่วง 30 วินาทีแรกซึ่งยังไม่มีการแทรกสอดจากเครือข่าย IEEE 802.11b และในช่วงหลังจากวินาทีที่ 150 ซึ่งการแทรกสอดจากเครือข่าย IEEE 802.11b หายไป ผลที่ได้จากการจำลองเครือข่ายจะใกล้เคียงกับกรณีไม่มีการแทรกสอดจากทั้งโนด W1 และโนด W2 ในหัวข้อ 4.2.1.1 ซึ่งจะเป็นเช่นนี้ในทุก scenario ของการทดสอบ ดังนั้นการวิเคราะห์ผลการทดสอบหลังจากนี้จะสนใจแต่ผลการทดสอบในช่วงที่มีการแทรกสอดจากเครือข่าย IEEE 802.11b คือช่วงหลังจากวินาทีที่ 30 ถึงวินาทีที่ 150 เท่านั้น

ในกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1) ค่า throughput ของโนด A ไม่ว่าจะใช้วิธีที่เสนอ วิธี ED หรือวิธี CS จะมีค่าต่ำมาก โดยวิธีที่เสนอจะมีค่า throughput ต่ำที่สุด คือ 0.111 kbps ขณะที่วิธี ED และวิธี CS จะมีค่า throughput ใกล้เคียงกันคือ 0.232 kbps และ 0.227 kbps ตามลำดับ

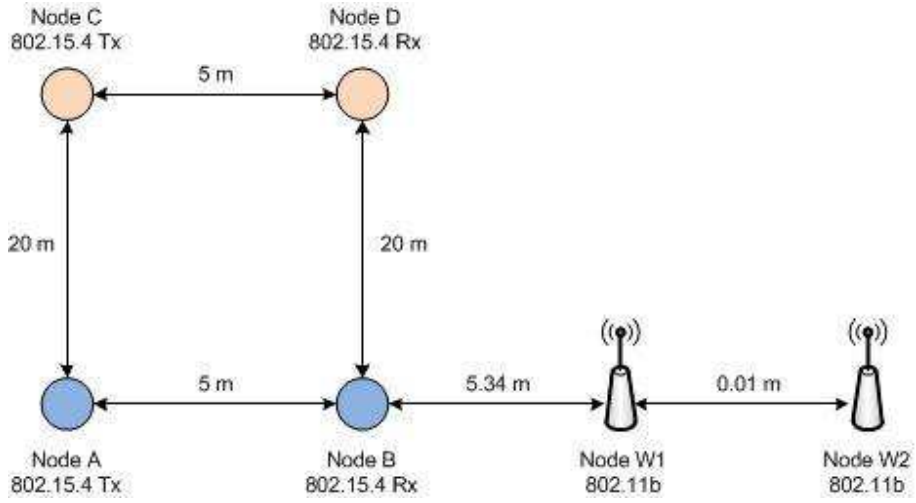
สำหรับค่า PER จะเห็นว่าทั้งวิธีที่เสนอ วิธี ED และวิธี CS จะมีค่า PER สูงมาก คือ 0.990 0.971 และ 0.990 ตามลำดับ ทั้งนี้เนื่องจากสัญญาณแทรกสอดจากทั้งโนด W1 และโนด W2 ส่งผลให้การส่งแพ็กเกตข้อมูลของโนด A ล้มเหลว 100% นอกจากนี้ การตรวจสอบช่องสัญญาณของโนด W1 และ W2 ในงานวิจัยนี้จะใช้วิธี CS ซึ่งจะไม่สนใจทราฟฟิกโนด A เลย รวมถึงการที่ความหนาแน่นของทราฟฟิก IEEE 802.11b จะเป็นการส่งอย่างต่อเนื่องทันทีที่การส่งแพ็กเกตข้อมูลครั้งล่าสุดสำเร็จ เพื่อให้เกิดกรณี worst case scenario ทำให้ถึงแม้โนด A จะใช้วิธี ED ซึ่งตรวจสอบสัญญาณจากเครือข่าย IEEE 802.11b แล้วก็ตาม แต่ก็ยังทำให้ PER สูงถึง 0.971 อยู่ดี สำหรับวิธีที่เสนอจะไม่เกิดประโยชน์สำหรับการแทรกสอด scenario นี้ เนื่องจากทราฟฟิกจากทั้งโนด W1 และโนด W2 ล้วนส่งผลให้การส่งแพ็กเกตข้อมูลของโนด A ล้มเหลวเสมอ ส่วนกรณีใช้วิธี CS โดยปกติจะมีค่า throughput สูงกว่าวิธีอื่นๆอยู่แล้ว เนื่องจากวิธี CS โนดส่งจะส่งแพ็กเกต

ข้อมูลโดยไม่สนใจว่ามีการแทรกสอดจากเครือข่าย IEEE 802.11b หรือไม่ ทำให้มีจำนวนครั้งของการส่งมากกว่าวิธีอื่นๆ อย่างไรก็ตามการใช้วิธี CS จะทำให้ค่า PER สูงกว่าวิธีอื่นๆด้วยเช่นกัน

สาเหตุที่วิธีที่เสนอมีค่า throughput ต่ำที่สุด และมีค่า PER สูงเท่าๆกับวิธี CS นั้น เมื่อพิจารณาจากค่าตัวแปรในโปรแกรมเมื่อสิ้นสุดการจำลองการทำงานแล้วนั้น พบว่าจำนวนครั้งที่แพ็กเกตข้อมูลของโนด A ชนกับแพ็กเกตข้อมูลของโนด W2 จะมากกว่าจำนวนครั้งที่ชนกับโนด W1 อยู่ประมาณ 50% แต่ในกรณีวิธี ED และวิธี CS จำนวนครั้งที่แพ็กเกตข้อมูลของโนด A ชนกับแพ็กเกตข้อมูลของโนด W1 และโนด W2 จะใกล้เคียงกันมาก ทั้งนี้เนื่องจากโนด W1 อยู่ใกล้โนด A มากกว่าโนด W2 ดังนั้น เมื่อใช้วิธีที่เสนอ ช่วงที่โนด A นำค่าพลังงานของโนด W1 มาใช้เป็นค่า ED threshold โนด A จะสามารถส่งแพ็กเกตข้อมูลได้เมื่อโนด W2 ใช้งานช่องสัญญาณอยู่ ซึ่งการส่งดังกล่าวจะล้มเหลว 100% จึงทำให้วิธีที่เสนอมีค่า PER สูงเท่าๆกับวิธี CS นอกจากนี้ การแทรกสอด scenario นี้ วิธีที่เสนอจะต้องเสียเวลาในการทำ ED scan เกือบทุกรอบของการพยายามส่งแพ็กเกตข้อมูล ทำให้วิธีที่เสนอมีค่า throughput ต่ำที่สุด

สำหรับค่า Channel Access Failure ratio วิธี ED จะมี Channel Access Failure ratio เท่ากับ 0.246 มากกว่าวิธีที่เสนอซึ่งมีค่าเท่ากับ 0.181 ทั้งนี้เนื่องจากวิธีที่เสนอจะถือว่าช่องสัญญาณว่างในขณะที่โนด W2 ใช้งานช่องสัญญาณอยู่ ในช่วงที่โนด A ใช้ค่าพลังงานของโนด W1 มาเป็นค่า ED threshold ดังที่กล่าวไปแล้วในย่อหน้าที่ผ่านมา

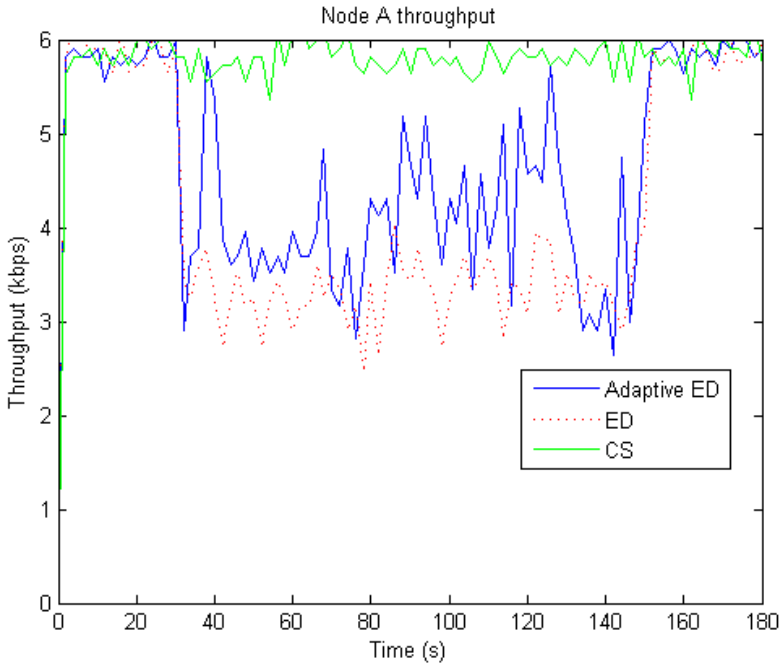
4.2.1.3 การแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5)



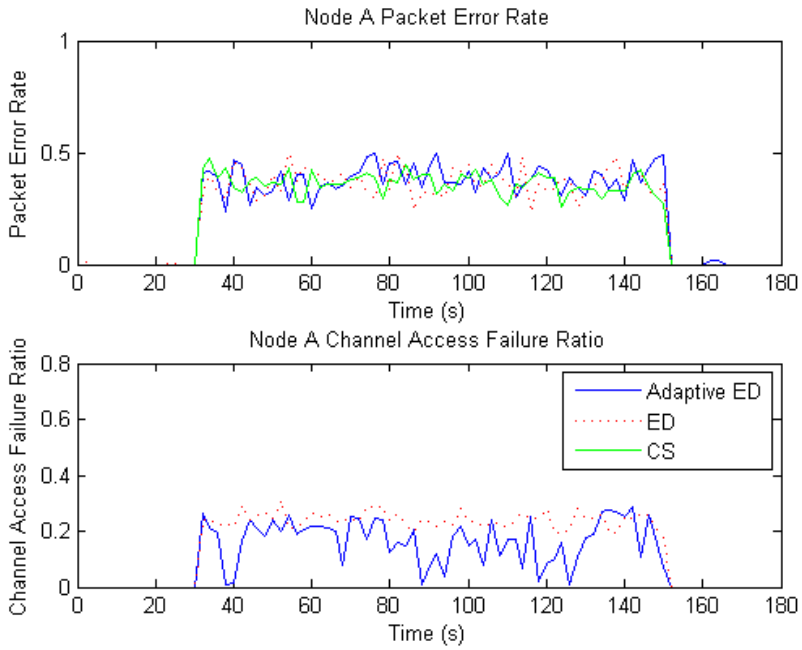
รูปที่ 4.10 รูปแบบเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5)

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5) แสดงดังรูปที่ 4.10 ในกรณีนี้ การแทรกสอดจากโนด W1 และโนด W2 เป็นการแทรกสอดแบบ Scenario 1 ทั้งคู่ โดยการแทรกสอดจากทั้งโนด W1 และโนด W2 ล้วนทำให้การส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B มีโอกาสเกิดความผิดพลาดประมาณ 50% หรือมี PER ประมาณ 0.5 โดยที่โนด A สามารถตรวจจับสัญญาณของแทรกสอดของทั้งโนด W1 และโนด W2 ได้ในการทำ CCA

ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1) แสดงดังกราฟในรูปที่ 4.11 และรูปที่ 4.12 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.4



รูปที่ 4.11 Throughput ของโนด A กรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5)



รูปที่ 4.12 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5)

ตารางที่ 4.4 ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5)

	Adaptive ED	ED	CS
Throughput	4.017	3.341	5.770
PER	0.385	0.386	0.358
Channel Access Failure ratio	0.175	0.245	0

จากผลการจำลองเครือข่ายในกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5) จะเห็นว่าค่า throughput ของโนด A เมื่อใช้วิธีที่เสนอและวิธี ED จะลดลงมาจากช่วงที่ไม่มีการแทรกสอดอย่างเห็นได้ชัด คือ จากประมาณ 5.9 kbps ลดลงมาเหลือ 4.017 kbps และ 3.341 kbps ตามลำดับ ซึ่งวิธีที่เสนอจะมีค่า throughput สูงกว่าวิธี ED ประมาณหนึ่ง ในขณะที่วิธี CS ค่า throughput จะลดลงมาเพียงเล็กน้อยเท่านั้น คือ ลดลงมาเหลือ 5.770 kbps

ในส่วนของค่า PER ในกรณีนี้กลับเป็นวิธี CS ที่มีค่า PER ต่ำที่สุด คือ 0.358 ในขณะที่วิธีที่เสนอกับวิธี ED จะมีค่า PER เท่าๆกัน คือ 0.385 และ 0.386 ตามลำดับ สาเหตุที่วิธี CS มีค่า

PER ต่ำกว่าวิธีที่เสนอและวิธี ED เนื่องจากการส่งแพ็กเกตข้อมูลทุกครั้งมี PER=0.5 ซึ่งความจริงแล้วยังมีกรณีที่เฟรมข้อมูลของเครือข่าย IEEE 802.15.4 อาจชนกับสัญญาณแทรกสอดเพียงช่วงเวลาสั้นๆทำให้อัตราการส่งแพ็กเกตข้อมูลล้มเหลวจริงๆจะต่ำกว่า 50% (การจำลองการทำงานในงานวิจัยนี้ จะกำหนดค่า PER จากตำแหน่งของโนด ดังนั้น กรณี PER=0.5 อัตราการส่งแพ็กเกตข้อมูลล้มเหลวจะเท่ากับ 50% เมื่อเฟรมแพ็กเกตข้อมูลทั้งเฟรมชนกับสัญญาณแทรกสอดเท่านั้น และเนื่องจากการจำลองเครือข่ายแต่ละโนดจะทำงานเป็นอิสระ จึงไม่สามารถบังคับให้อัตราการส่งแพ็กเกตข้อมูลล้มเหลวจะเท่ากับ 50% ในทุกครั้งได้) เป็นสาเหตุให้การส่งด้วยวิธี CS มีโอกาสสำเร็จมากกว่าล้มเหลว ในขณะที่วิธีที่เสนอและวิธี ED จะเสียโอกาสในช่วงที่รอช่องสัญญาณว่าง เนื่องจากการส่งแพ็กเกตข้อมูลในช่วงนี้มีโอกาสสำเร็จมากกว่าล้มเหลว

สำหรับค่า Channel Access Failure ratio วิธี ED จะมี Channel Access Failure ratio เท่ากับ 0.245 มากกว่าวิธีที่เสนอซึ่งมีค่าเท่ากับ 0.175 ซึ่งเป็นค่าที่ใกล้เคียงกับกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1) ในหัวข้อ 4.2.1.2 โดยสาเหตุที่เป็นเช่นนี้เป็นเหตุผลเดียวกับกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 เช่นกัน

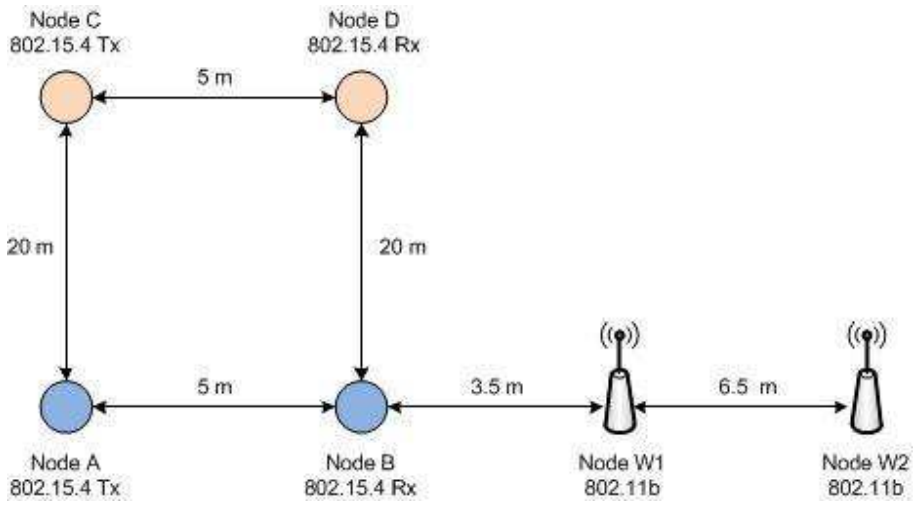
4.2.1.4 การแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) โนด W2 เป็น Scenario 3

ในกรณีนี้ การแทรกสอดจากโนด W1 เป็นการแทรกสอดแบบ Scenario 1 โดยจะทำให้การส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B มีโอกาสเกิดความผิดพลาด 100% หรือมี PER=1 ในขณะที่การแทรกสอดจากโนด W2 เป็นการแทรกสอดแบบ Scenario 3 ซึ่งจะไม่ส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B โดยที่โนด A สามารถตรวจจับสัญญาณแทรกสอดของทั้งโนด W1 และโนด W2 ได้ในกระบวนงาน CCA

อย่างไรก็ตาม ด้วยวิธีที่เสนอซึ่งจะใช้ระดับพลังงานของสัญญาณแทรกสอดที่ทำให้การส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B ล้มเหลวมาตั้งเป็นค่า ED threshold ซึ่งในที่นี้ก็คือระดับพลังงานของโนด W1 นั่นเอง ซึ่งโนด W2 ที่ทำให้เกิดการแทรกสอด scenario 3 นั้น อาจจะมีระดับพลังงานสูงกว่าหรือต่ำกว่าค่า ED threshold นี้ก็ได้ ขึ้นอยู่กับตำแหน่งของโนด W2 คือ หากโนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 ระดับพลังงานของโนด W2 ก็จะสูงกว่าค่า ED threshold ทำให้โนด A ไม่สามารถส่งแพ็กเกตข้อมูลได้ในขณะที่โนด W2 กำลังใช้งานช่องสัญญาณอยู่ แม้ว่าโนด W2 จะไม่ส่งผลกระทบให้การส่งแพ็กเกตข้อมูลจากโนด A ไปยังโนด B ล้มเหลวก็ตาม ซึ่งในกรณีดังกล่าวจะไม่สามารถใช้ประโยชน์จากวิธีที่เสนอได้

ดังนั้น ในหัวข้อนี้ จะแบ่งการจำลองการทำงานออกเป็น 2 กรณี คือ กรณีที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 และกรณีที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1

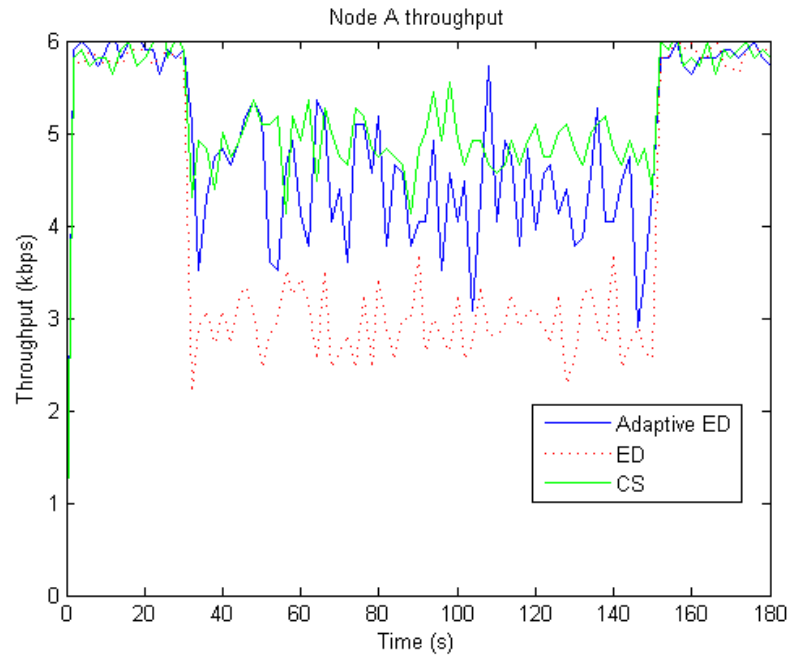
กรณีที่ 1 โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1



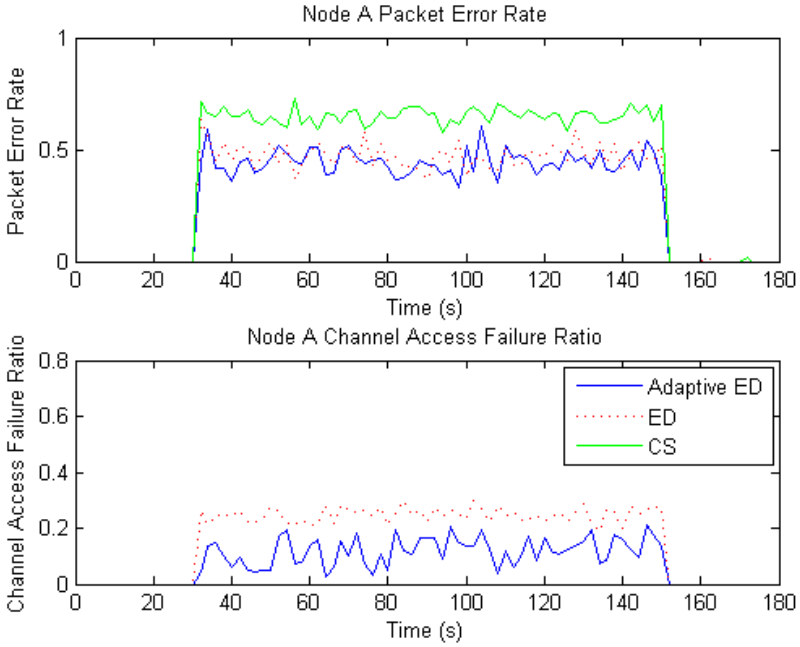
รูปที่ 4.13 รูปแบบเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 แสดงดังรูปที่ 4.13

ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1) แสดงดังกราฟในรูปที่ 4.14 และรูปที่ 4.15 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.5



รูปที่ 4.14 Throughput ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1



รูปที่ 4.15 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1

ตารางที่ 4.5 ผลการจำลองเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 และโนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1

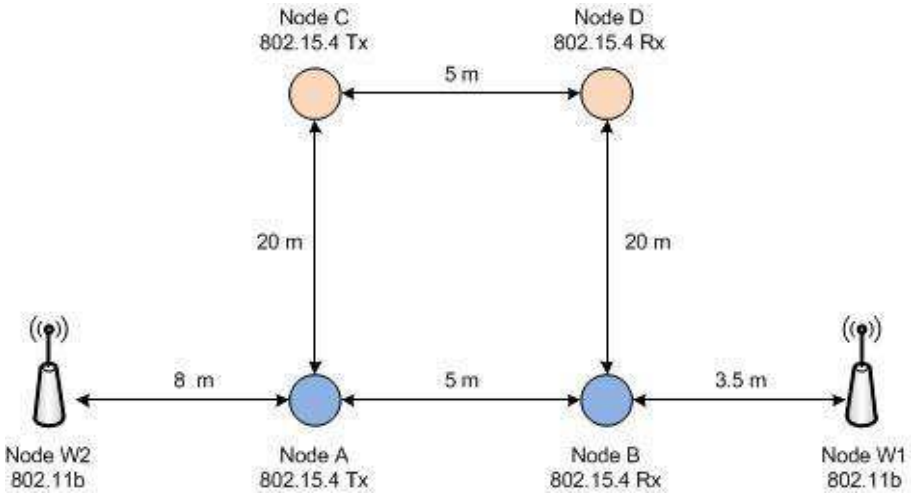
	Adaptive ED	ED	CS
Throughput	4.416	2.926	4.881
PER	0.446	0.475	0.652
Channel Access Failure ratio	0.119	0.248	0

จากผลการจำลองเครือข่ายในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 จะเห็นว่าเมื่อใช้วิธีที่เสนอ ค่า throughput ของโนด A จะสูงกว่าวิธี ED อย่างเห็นได้ชัด (4.416 kbps และ 2.926 kbps ตามลำดับ) และต่ำกว่ากรณีใช้วิธี CS ซึ่งมีค่า throughput 4.881 kbps ไม่มากนัก ทั้งนี้เนื่องจาก โนด A สามารถส่งแพ็กเกตข้อมูลได้ในช่วงที่โนด W2 ใช้งานช่องสัญญาณอยู่ ซึ่งในกรณีนี้ สัญญาณแทรกสอดจากโนด W2 จะไม่ส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลจากโนด A ไปยังโนด B อยู่แล้ว โดยที่โนด A จะไม่ส่งแพ็กเกตข้อมูลกรณีที่โนด W1 กำลังใช้งานช่องสัญญาณอยู่เท่านั้น

สำหรับค่า PER จะเห็นว่าวิธีที่เสนอมีค่า PER ต่ำที่สุดคือ 0.446 โดยจะต่ำกว่าการใช้วิธี ED ซึ่งมีค่า PER เท่ากับ 0.475 ด้วย ที่เป็นเช่นนี้เนื่องมาจากการที่โนด A สามารถส่งแพ็กเกตข้อมูลได้ในช่วงที่โนด W2 ใช้งานช่องสัญญาณอยู่ ซึ่งจะแตกต่างจากกรณีใช้วิธี ED ซึ่งโนด A จะไม่ส่งแพ็กเกตข้อมูลในช่วงนี้ ทำให้เมื่อนำมาคิดสัดส่วนการส่งแพ็กเกตข้อมูลสำเร็จ วิธีที่เสนอจะมีสัดส่วนการส่งแพ็กเกตข้อมูลสำเร็จสูงกว่าวิธี ED ส่งผลให้มีค่า PER ต่ำกว่า ในขณะที่วิธี CS จะมี PER สูงที่สุดโดยปกติอยู่แล้ว เนื่องจากจะไม่สนใจสัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b ในการทำ CCA

สำหรับค่า Channel Access Failure ratio วิธีที่เสนอจะมี Channel Access Failure ratio เท่ากับ 0.119 ต่ำกว่าวิธี ED ซึ่งมีค่าเท่ากับ 0.248 ทั้งนี้เนื่องจากวิธีที่เสนอจะถือว่าช่องสัญญาณว่างในขณะที่โนด W2 กำลังใช้งานช่องสัญญาณอยู่

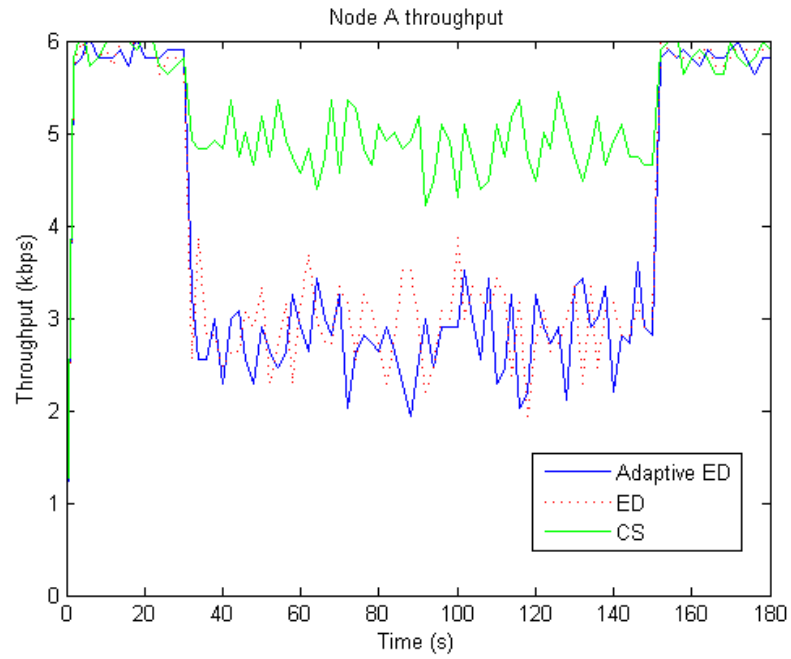
กรณีที่ 2 โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1



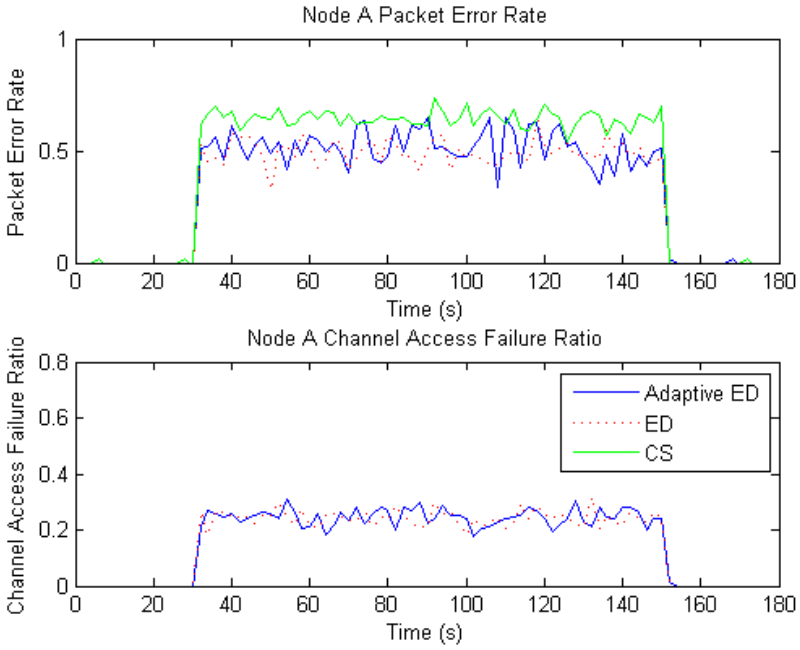
รูปที่ 4.16 รูปแบบเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 แสดงดังรูปที่ 4.16

ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=1) แสดงดังกราฟในรูปที่ 4.17 และรูปที่ 4.18 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.6



รูปที่ 4.17 Throughput ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1



รูปที่ 4.18 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1

ตารางที่ 4.6 ผลการจำลองเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 และโนด W2 อยู่ใกล้โนด A มากกว่าโนด W1

	Adaptive ED	ED	CS
Throughput	2.793	2.935	4.875
PER	0.518	0.496	0.648
Channel Access Failure ratio	0.245	0.243	0

จากผลการจำลองเครือข่ายในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 จะเห็นว่าทั้งวิธี ED และวิธี CS จะได้ผลเช่นเดียวกับกรณีที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 ในกรณีที่ 1 ที่ผ่านมา แต่ในวิธีที่เสนอผลที่ได้จะด้อยกว่ากรณีที่ 1 ทุกพารามิเตอร์ คือ ค่า throughput ลดลงจาก 4.416 kbps ลงมาเหลือ 2.793 kbps ค่า PER เพิ่มขึ้นจาก 0.446 เป็น 0.518 และ Channel Access Failure ratio เพิ่มขึ้นจาก 0.119 เป็น 0.245 เป็นไปตามที่คาดหมายไว้ในการแบ่งกรณีการทดสอบ เนื่องจากโนด A จะใช้ระดับพลังงานของโนด W1 ซึ่งทำให้การส่งแพ็กเกตข้อมูลจากโนด A ล้มเหลวมาตั้งค่าเป็น ED threshold ในขณะที่โนด W2 ซึ่งไม่ทำให้การส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B ล้มเหลว กลับมีค่าพลังงานสูงกว่า ED threshold โนด A จึงไม่ส่งแพ็กเกตข้อมูลในช่วงที่โนด W2 กำลังใช้งานช่องสัญญาณอยู่ จึงทำให้วิธีที่เสนอจะมีลักษณะเหมือนกับวิธี ED แค่สาเหตุที่ทำให้วิธีที่เสนอมีค่า throughput ต่ำกว่า และมีค่า PER สูงกว่าวิธี ED เล็กน้อย เนื่องมาจากการทำ ED scan ซึ่งจะใช้เวลา 128 μs ต่อครั้ง ทำให้วิธีที่เสนอมีค่า throughput ต่ำกว่าวิธี ED และในช่วงที่ทำ ED scan นี้มีโอกาสทำให้เกิดการวัดพลังงานผิดพลาดในกรณีที่โนด W1 และโนด W2 สลับการทำงานกันพอดี โนด A จึงใช้ค่าพลังงานจากโนด W2 มาตั้งเป็น ED threshold แทนที่จะเป็นพลังงานจากโนด W1 ส่งผลให้โนด A สามารถส่งแพ็กเกต ข้อมูลได้ในช่วงที่โนด W1 ใช้งานช่องสัญญาณอยู่ เนื่องจากโนด W1 มีพลังงานต่ำกว่า ED threshold ซึ่งการที่โนด A ส่งแพ็กเกตข้อมูลในขณะที่โนด W1 ใช้งานช่องสัญญาณอยู่นั้นจะทำให้โอกาสเกิดการล้มเหลวสูงมาก

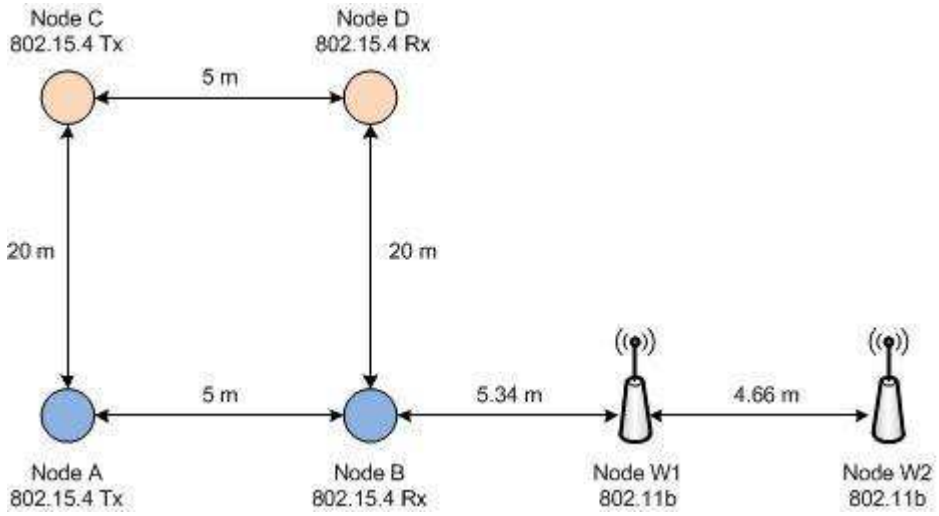
4.2.1.5 การแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) โนด W2 เป็น Scenario 3

ในกรณีนี้ การแทรกสอดจากโนด W1 เป็นการแทรกสอดแบบ Scenario 1 โดยจะทำให้การส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B มีโอกาสเกิดความผิดพลาดประมาณ 50% หรือมี PER

ประมาณ 0.5 ในขณะที่การแทรกสอดจากโนด W2 เป็นการแทรกสอดแบบ Scenario 3 ซึ่งจะไม่ส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B โดยที่โนด A สามารถตรวจจับสัญญาณแทรกสอดของทั้งโนด W1 และโนด W2 ได้ในกระบวนงาน CCA

การวิเคราะห์ผลการจำลองเครือข่ายในกรณีนี้จะคล้ายกับกรณีหัวข้อ 4.2.1.4 โดยจะแบ่งการจำลองการทำงานออกเป็น 2 กรณี คือ กรณีที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 และกรณีที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 เช่นเดียวกัน

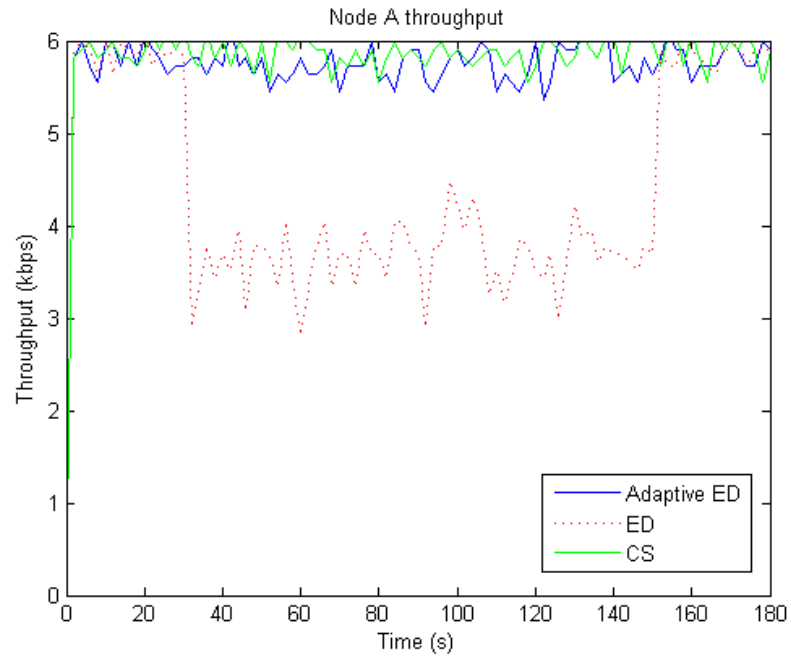
กรณีที่ 1 โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1



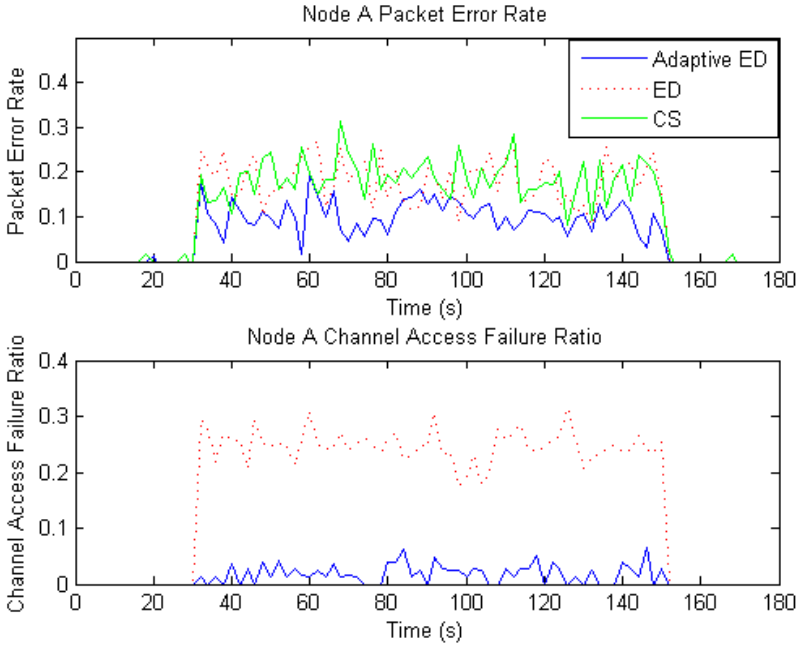
รูปที่ 4.19 รูปแบบเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 แสดงดังรูปที่ 4.19

ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5) แสดงดังกราฟในรูปที่ 4.20 และรูปที่ 4.21 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.7



รูปที่ 4.20 Throughput ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1



รูปที่ 4.21 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1

ตารางที่ 4.7 ผลการจำลองเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER= 0.5) และโนด W2 เป็น Scenario 3 และโนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1

	Adaptive ED	ED	CS
Throughput	5.666	3.689	5.886
PER	0.101	0.199	0.190
Channel Access Failure ratio	0.026	0.241	0

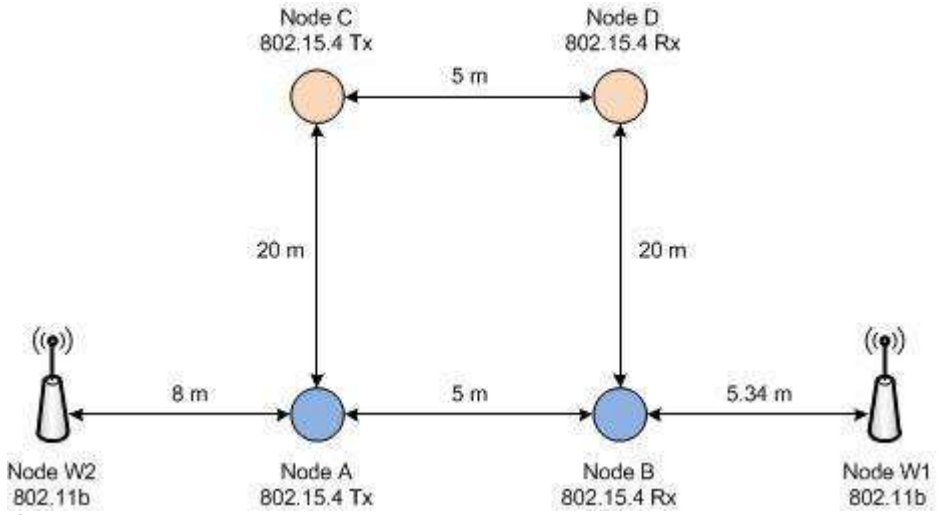
ผลการจำลองเครือข่ายในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 จะมีลักษณะใกล้เคียงกับกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 (กรณีที่ 1 ในหัวข้อที่ 4.2.1.4) คือ วิธีที่เสนอจะมีค่า throughput สูงใกล้เคียงกับวิธี CS และมี PER น้อยที่สุด ทั้งนี้เมื่อใช้วิธีที่เสนอ โนด A จะไม่ส่งแพ็กเกตข้อมูลในขณะที่โนด W1 กำลังใช้งานช่องสัญญาณอยู่ เช่นเดียวกับกรณี หัวข้อ 4.2.1.4 ซึ่งที่จริงแล้วสัญญาณจากโนด W1 มีโอกาสต่ำกว่า 50% ที่จะทำให้การส่งแพ็กเกตข้อมูลของโนด A ล้มเหลว (ค่า PER 0.5 กับโอกาสการส่งแพ็กเกตข้อมูลล้มเหลวของโนด A ได้อธิบายไว้แล้วในหัวข้อที่ 4.2.1.3) ซึ่งหากใช้วิธี CS โนด A จะสามารถส่งแพ็กเกตข้อมูลได้ในช่วงนี้ ส่งผลให้มีค่า throughput สูงขึ้นเล็กน้อย ขณะที่ค่า PER ก็จะสูงขึ้นเช่นกัน

อย่างไรก็ตาม ด้วยโนด W1 ส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลของโนด A น้อยกว่ากรณี PER=1 ในหัวข้อ 4.2.1.3 ดังนั้น การที่โนด W1 ใช้วิธี CS ซึ่งไม่สนใจสัญญาณของโนด A ในการตรวจสอบช่องสัญญาณจึงมีผลกระทบน้อยลงด้วย ส่งผลให้ค่า throughput ของทุกวิธีสูงขึ้นจากเดิมค่อนข้างมาก และค่า PER ของทุกวิธีก็ลดลงมากเช่นกัน

นอกจากนี้ วิธีที่เสนอจะมี Channel Access Failure ratio เพียง 0.026 ต่ำกว่ากรณีที่ 1 ในหัวข้อ 4.2.1.4 (การแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1)) ซึ่งมี Channel Access Failure ratio เท่ากับ 0.119 เนื่องจากในกรณีนี้ สัญญาณจากโนด W1 มีโอกาสที่จะทำให้การส่งแพ็กเกตข้อมูลของโนด A ล้มเหลวต่ำกว่า 50% ดังที่ได้กล่าวไปแล้ว ดังนั้น กรณีที่แพ็กเกตข้อมูลจากโนด A ชนกับแพ็กเกตข้อมูลจากโนด W1 ก็ยังมีโอกาสที่โนด A จะส่งแพ็กเกตข้อมูลได้สำเร็จ แต่ในกรณีหัวข้อ 4.2.1.4 หากแพ็กเกตข้อมูลจากโนด A ชนกับแพ็กเกตข้อมูลจากโนด W1 โอกาสที่แพ็กเกตข้อมูลของโนด A จะสูญเสียมีสูงมาก ส่งผลให้โนด A ต้องเริ่มกระบวนการส่งซ้ำใน

ขณะที่โนด W1 ก็ยังคงใช้งานช่องสัญญาณอยู่ ทำให้ Channel Access Failure ratio สำหรับกรณีหัวข้อ 4.2.1.4 มีค่าสูงกว่ากรณีนี้

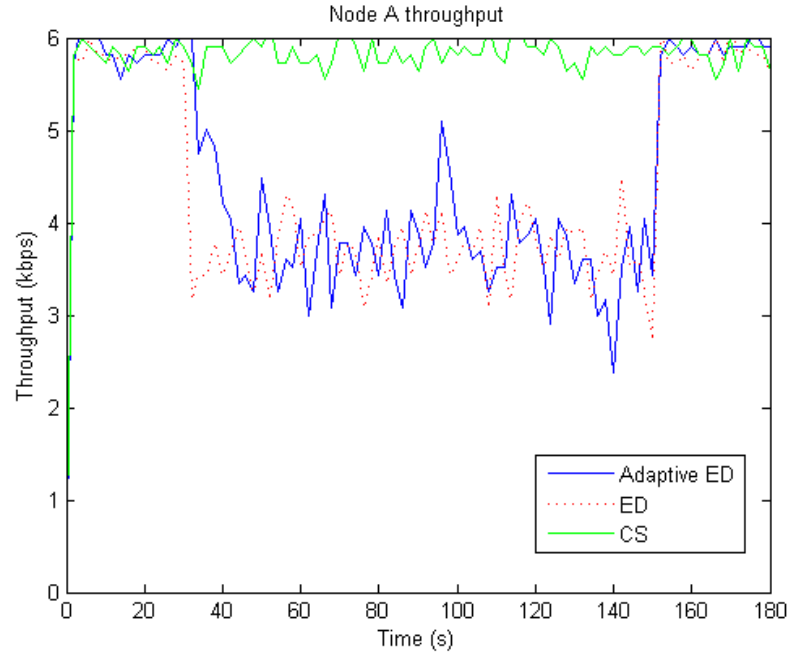
กรณีที่ 2 โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1



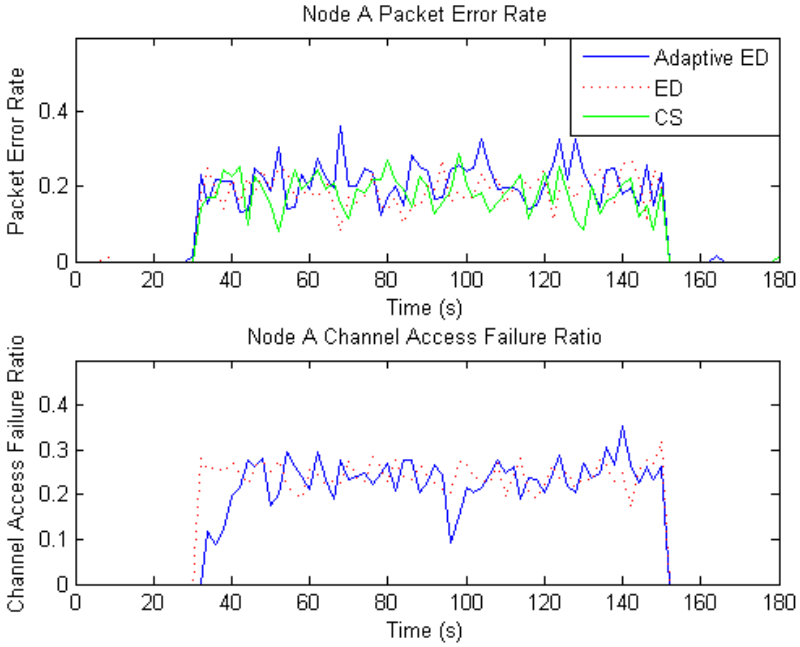
รูปที่ 4.22 รูปแบบเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 แสดงดังรูปที่ 4.22

ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5) แสดงดังกราฟในรูปที่ 4.23 และรูปที่ 4.24 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.8



รูปที่ 4.23 Throughput ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1



รูปที่ 4.24 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1

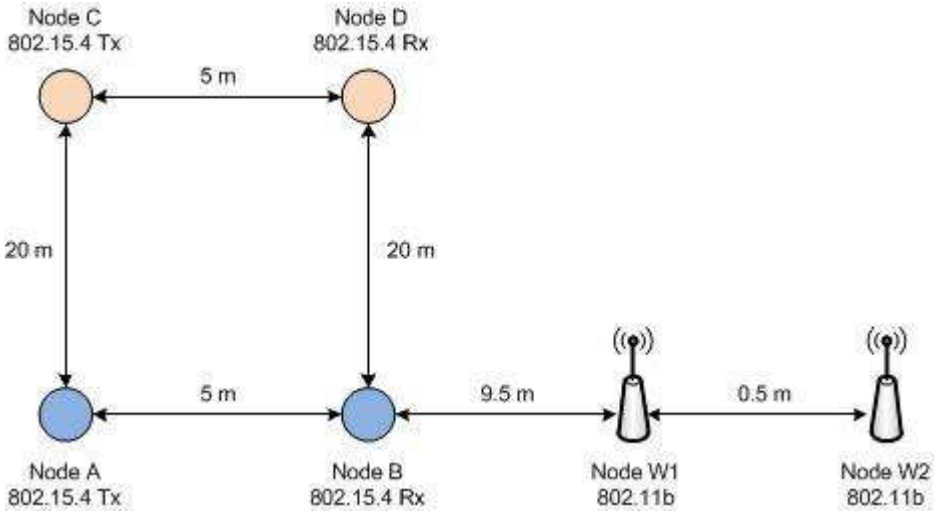
ตารางที่ 4.8 ผลการจำลองเครือข่ายกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER= 0.5) และโนด W2 เป็น Scenario 3 และโนด W2 อยู่ใกล้โนด A มากกว่าโนด W1

	Adaptive ED	ED	CS
Throughput	3.781	3.680	5.836
PER	0.210	0.192	0.185
Channel Access Failure ratio	0.230	0.245	0

ผลการจำลองเครือข่ายในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 จะมีลักษณะใกล้เคียงกับกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 (กรณีที่ 2 ในหัวข้อที่ 4.2.1.4) คือวิธีที่เสนอจะมีผลใกล้เคียงกับวิธี ED โดยจะมีค่า PER สูงกว่าวิธี ED เล็กน้อยเช่นเดียวกับหัวข้อ 4.2.1.4 ด้วยสาเหตุเดียวกันคือ ช่วงที่ทำ ED scan ซึ่งใช้เวลาประมาณ 128 μs มีโอกาสทำให้เกิดการวัดพลังงานผิดพลาดในกรณีที่โนด W1 และโนด W2 สลับการทำงานกันพอดี ทำให้โนด A อาจใช้ค่าพลังงานจากโนด W2 มาตั้งเป็น ED threshold แทนที่จะเป็นพลังงานจากโนด W1 ส่งผลให้โนด A สามารถส่งแพ็กเกตข้อมูลได้ในช่วงที่โนด W1 ใช้งานช่องสัญญาณอยู่ ซึ่งการส่งแพ็กเกตข้อมูลในช่วงนี้มีโอกาสที่จะล้มเหลวอยู่บ้าง ในขณะเดียวกันก็มีโอกาสสำเร็จด้วยเช่นกัน ดังนั้น วิธีที่เสนอจึงมีค่า throughput สูงกว่าวิธี ED แต่ก็มีค่า PER สูงกว่าเช่นกัน โดยทั้งวิธีที่เสนอและวิธี ED นั้นโนด A จะไม่ส่งแพ็กเกตข้อมูลในขณะที่โนด W2 ใช้งานช่องสัญญาณอยู่ จึงทำให้มี throughput ต่ำกว่าวิธี CS นอกจากนี้ การที่วิธี CS สามารถส่งแพ็กเกตข้อมูลได้สำเร็จในช่วงที่โนด W2 ใช้งานช่องสัญญาณอยู่ ยังส่งผลให้สัดส่วนการส่งแพ็กเกตข้อมูลสำเร็จของโนด A สูงขึ้น ทำให้วิธี CS มีค่า PER ต่ำที่สุดด้วย

4.2.1.6 การแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3

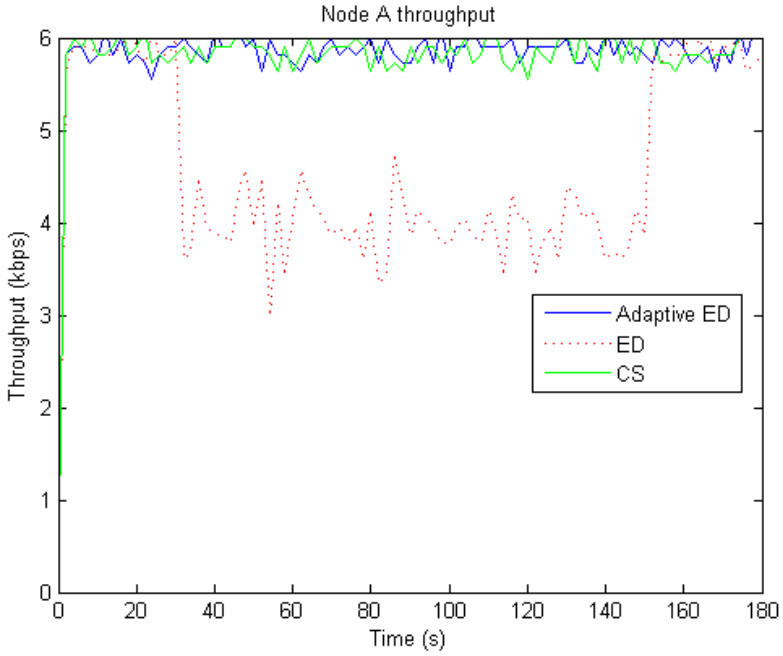
ในกรณีนี้ การแทรกสอดจากโนด W1 และโนด W2 เป็นการแทรกสอดแบบ Scenario 3 ทั้งคู่ โดยการแทรกสอดจากทั้งโนด W1 และโนด W2 จะไม่ส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลจากโนด A ไปโนด B แต่โนด A สามารถตรวจจับสัญญาณแทรกสอดของทั้งโนด W1 และโนด W2 ได้ในกระบวนงาน CCA



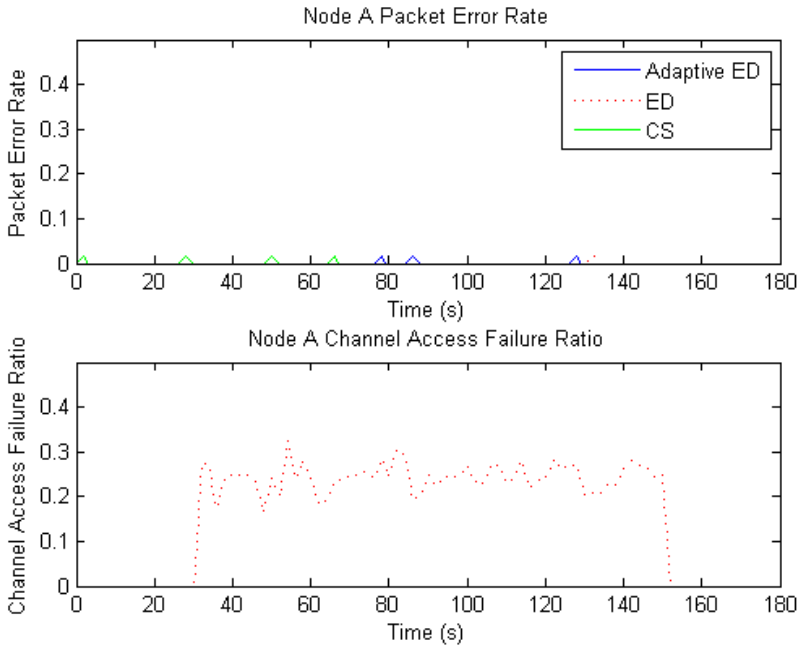
รูปที่ 4.25 รูปแบบเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3

รูปแบบของเครือข่ายสำหรับการทดสอบในกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3 แสดงดังรูปที่ 4.25

ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3 แสดงดังกราฟในรูปที่ 4.26 และรูปที่ 4.27 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.9



รูปที่ 4.26 Throughput ของโนด A กรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3



รูปที่ 4.27 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3

ตารางที่ 4.9 ผลการจำลองเครือข่ายกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3

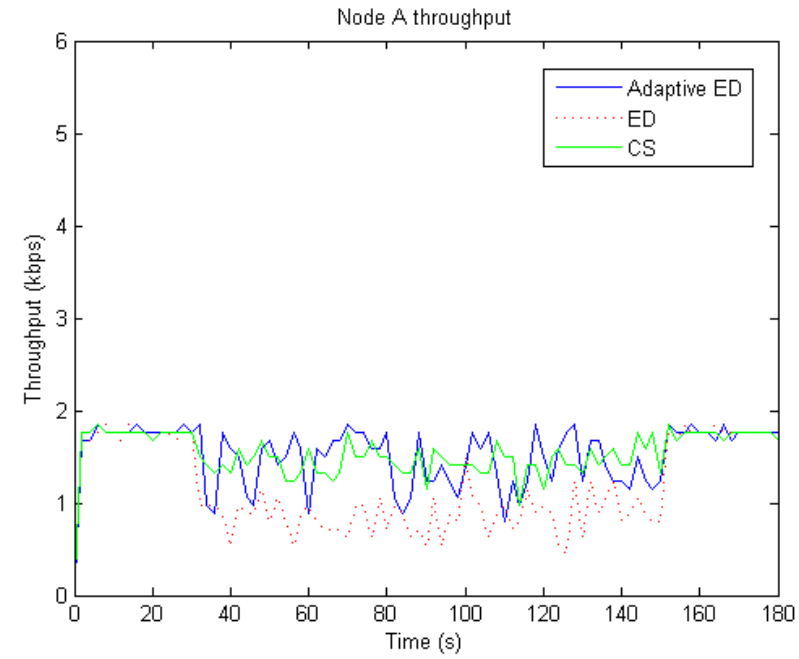
	Adaptive ED	ED	CS
Throughput	5.870	3.951	5.842
PER	0	0	0
Channel Access Failure ratio	0	0.245	0

จากผลการจำลองเครือข่ายในกรณีการแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 จะเห็นว่าวิธีที่เสนอมีสมรรถนะเหมือนกับวิธี CS เนื่องจากในกรณีที่การแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3 นั้น จะไม่ทำให้วิธีที่เสนอเปลี่ยนไปใช้ CCA วิธีที่ 3 ได้ ดังนั้นวิธีที่เสนอจึงใช้วิธี CS ต่อไปเรื่อยๆ นอกจากนี้จะเห็นได้ชัดเจนว่าในกรณีที่การแทรกสอดจากทั้งโนด W1 และโนด W2 เป็น Scenario 3 วิธี ED จะมีสมรรถนะต่ำกว่าวิธีอื่นๆอย่างชัดเจน เนื่องจากวิธี ED จะไม่ส่งแพ็กเกตข้อมูลในขณะที่โนด W1 หรือโนด W2 ใช้งานช่องสัญญาณอยู่ แม้ว่าทั้งโนด W1 และโนด W2 จะไม่ส่งผลกระทบให้การส่งแพ็กเกตข้อมูลของโนด A ล้มเหลวก็ตาม

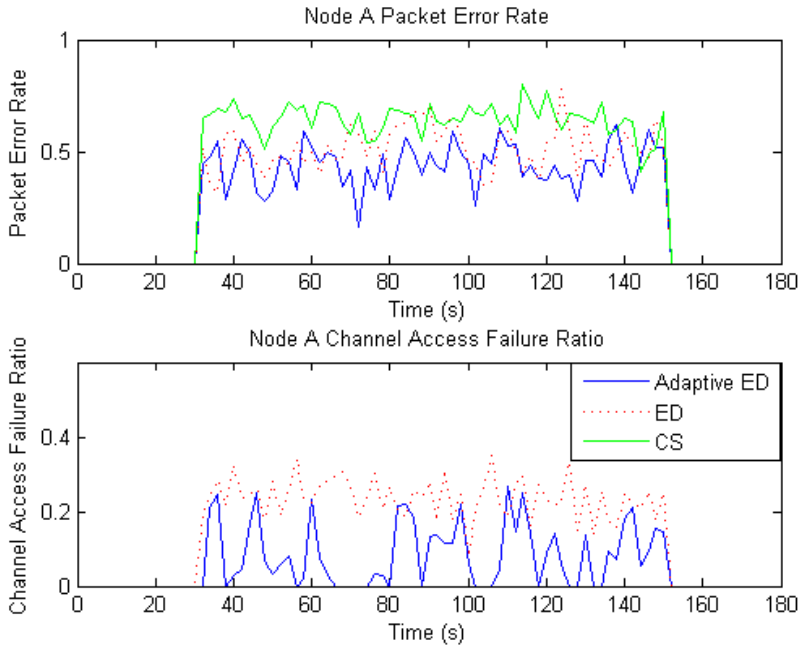
4.2.2 ผลกระทบจากความหนาแน่นของแพ็กเกตข้อมูล

การวิเคราะห์ผลกระทบจากความหนาแน่นของแพ็กเกตข้อมูลของโนด A จะวิเคราะห์ในรูปแบบ scenario ของการแทรกสอดที่วิธีที่เสนอช่วยบรรเทาปัญหาจากการแทรกสอดได้ดีที่สุด นั่นคือกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 (หัวข้อ 4.2.1.4 กรณีที่ 1) โดยจะปรับเปลี่ยนรูปแบบการส่งข้อมูลจากเดิมซึ่งกำหนดให้เป็นทุกๆ Poisson(λ = 30 ms) เป็นทุกๆ Poisson(λ = 100 ms) หรือกำหนดให้ความถี่ของแพ็กเกตข้อมูลของโนดส่งในเครือข่าย IEEE 802.15.4 ซึ่งก็คือโนด A และโนด C มีความถี่น้อยลงนั่นเอง

ผลการจำลองเครือข่ายกรณีรูปแบบการส่งข้อมูลเป็นทุกๆ Poisson(λ = 100 ms) แสดงดังกราฟในรูปที่ 4.28 และรูปที่ 4.29 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.10



รูปที่ 4.28 Throughput ของโนด A กรณีรูปแบบการส่งข้อมูลเป็นทุกๆ Poisson(λ = 100 ms)



รูปที่ 4.29 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีรูปแบบการส่งข้อมูลเป็นทุกๆ Poisson(λ = 100 ms)

ตารางที่ 4.10 ผลการจำลองเครือข่ายกรณีรูปแบบการส่งข้อมูลเป็นทุกๆ Poisson(λ = 100 ms)

	Adaptive ED	ED	CS
Throughput	1.468	0.862	1.439
PER	0.441	0.518	0.646
Channel Access Failure ratio	0.088	0.238	0

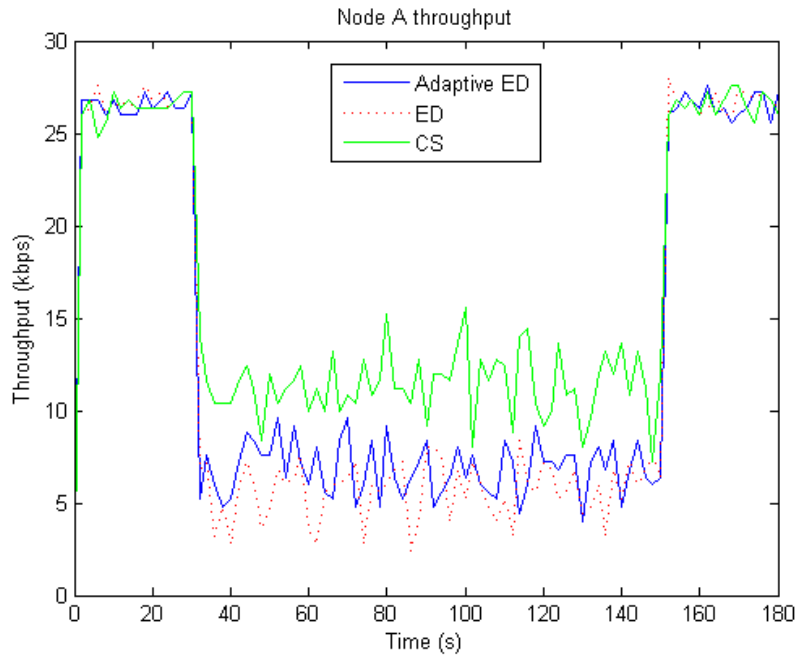
จากผลการจำลองเครือข่ายในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 เมื่อปรับเปลี่ยนรูปแบบการส่งข้อมูลจากเดิมทุกๆ Poisson(λ = 30 ms) เป็นทุกๆ Poisson(λ = 100 ms) จะเห็นว่าค่า throughput ของทั้งวิธีที่เสนอ วิธี ED และวิธี CS ลดลงจากเดิมอย่างมาก คือ จาก 4.416 kbps, 2.926 kbps และ 4.881 kbps เป็น 1.468 kbps, 0.862 kbps, และ 1.439 kbps ตามลำดับ เนื่องจากความถี่ของแพ็กเกตข้อมูลที่จะส่งลดลงนั่นเอง โดยในกรณีนี้วิธีที่เสนอจะมีค่า throughput สูงกว่าวิธี CS เนื่องจากการที่ระยะเวลาระหว่างแต่ละแพ็กเกตนานขึ้น ทำให้วิธีที่เสนอมีโอกาสในการส่งแพ็กเกตข้อมูลได้สำเร็จมากขึ้นนั่นเอง

สำหรับค่า PER และ Channel Access Failure ratio สำหรับทุกวิธียังถือว่าใกล้เคียงกรณีที่รูปแบบการส่งข้อมูลเป็นทุกๆ Poisson(λ = 30 ms) มาก ดังนั้นจึงพอสรุปได้ว่าความถี่ของแพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 มีผลน้อยมากต่อค่า PER และ Channel Access Failure ratio

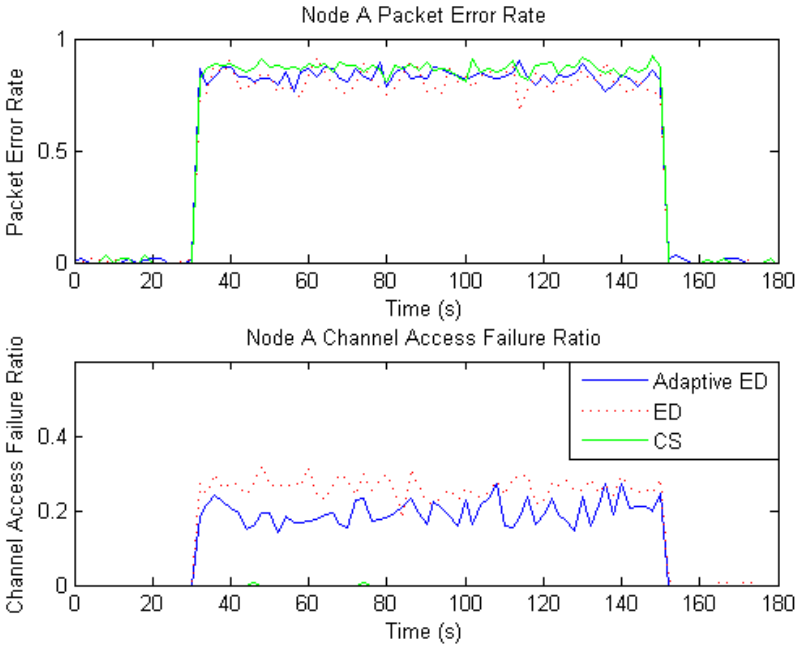
4.2.3 ผลกระทบจากขนาดแพ็กเกตข้อมูล

การวิเคราะห์ผลกระทบจากขนาดแพ็กเกตข้อมูลของโนด A จะวิเคราะห์กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 (หัวข้อ 4.2.1.4 กรณีที่ 1) เช่นเดียวกัน โดยจะปรับเปลี่ยนขนาดแพ็กเกตข้อมูลจากเดิมซึ่งกำหนดไว้ที่ 22 bytes ให้เป็น 100 bytes

ผลการจำลองเครือข่ายกรณีขนาดแพ็กเกตข้อมูลเท่ากับ 100 bytes แสดงดังกราฟในรูปที่ 4.30 และรูปที่ 4.31 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.11



รูปที่ 4.30 Throughput ของโนด A กรณีขนาดแพ็กเกตข้อมูลเท่ากับ 100 bytes



รูปที่ 4.31 ค่า PER และ Channel Access Failure ratio ของโนด A กรณีขนาดแพ็กเกตข้อมูลเท่ากับ 100 bytes

ตารางที่ 4.11 ผลการจำลองเครือข่ายกรณีขนาดแพ็กเกตข้อมูลเป็น 100 bytes

	Adaptive ED	ED	CS
Throughput	6.847	5.727	11.440
PER	0.834	0.809	0.868
Channel Access Failure ratio	0.196	0.263	0

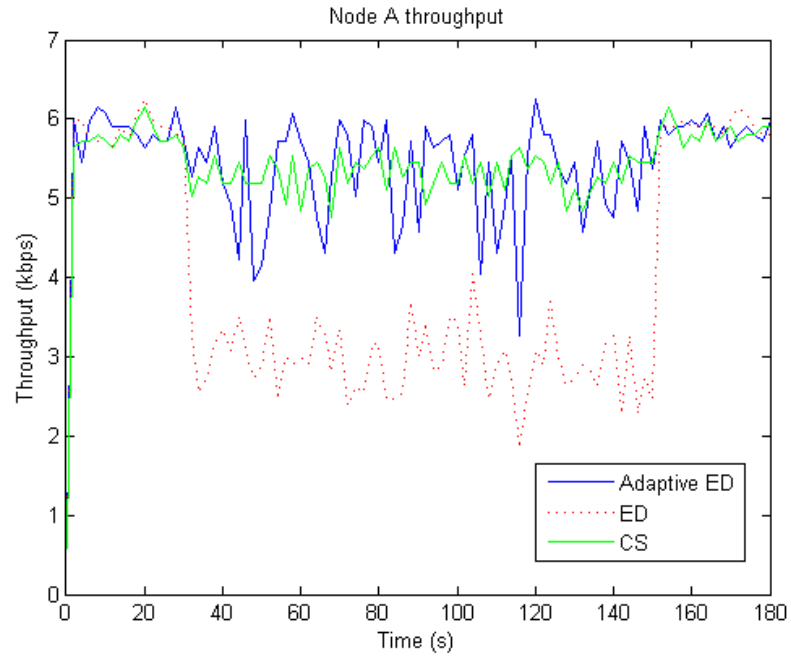
จากผลการจำลองเครือข่ายในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 เมื่อปรับเปลี่ยนรูปแบบขนาดแพ็กเกตข้อมูลจากเดิม 30 bytes เป็น 100 bytes จะเห็นว่าค่า throughput ของทั้งวิธีที่เสนอ วิธี ED และวิธี CS สูงขึ้นจากเดิมอย่างมาก คือ จาก 4.416 kbps, 2.926 kbps และ 4.881 kbps เป็น 6.847 kbps, 5.727 kbps, และ 11.440 ตามลำดับ เนื่องจากขนาดแพ็กเกตข้อมูลใหญ่กว่าเดิมมาก ทำให้การส่งแพ็กเกตข้อมูลสำเร็จหนึ่งครั้งจะส่งผลต่อค่า throughput เพิ่มมากขึ้น ทำให้วิธี CS ซึ่งมีจำนวนครั้งของการพยายามส่งแพ็กเกตข้อมูลมากที่สุดจึงมีค่า throughput สูงกว่าวิธีที่เสนอและวิธี ED มาก

เนื่องจากแพ็กเกตข้อมูลมีขนาดใหญ่ขึ้นจึงต้องใช้เวลาในการส่งมากขึ้น ส่งผลให้มีโอกาสมากขึ้นที่แพ็กเกตข้อมูลของโนด A จะชนกับสัญญาณแทรกสอดจากโนด W1 ทำให้ค่า PER ของทุกวิธีมีค่าสูงมาก เช่นเดียวกับค่า Channel Access Failure ratio ของวิธีที่เสนอ และวิธี ED ที่จะสูงขึ้นกว่ากรณีขนาดแพ็กเกตข้อมูล 22 bytes เล็กน้อย ซึ่งมีผลต่อเนื่องมาจากการที่มีค่า PER สูงขึ้น ทำให้จำนวนครั้งของการส่งซ้ำของโนด A มากขึ้น ซึ่งการส่งซ้ำส่วนใหญ่จะมาจากการที่แพ็กเกตข้อมูลของโนด A จะชนกับสัญญาณแทรกสอดจากโนด W1 ดังนั้นในการพยายามส่งซ้ำก็มีแนวโน้มว่าโนด W1 ก็ยังคงใช้งานช่องสัญญาณอยู่ ส่งผลให้ Channel Access Failure ratio สูงขึ้นเล็กน้อย

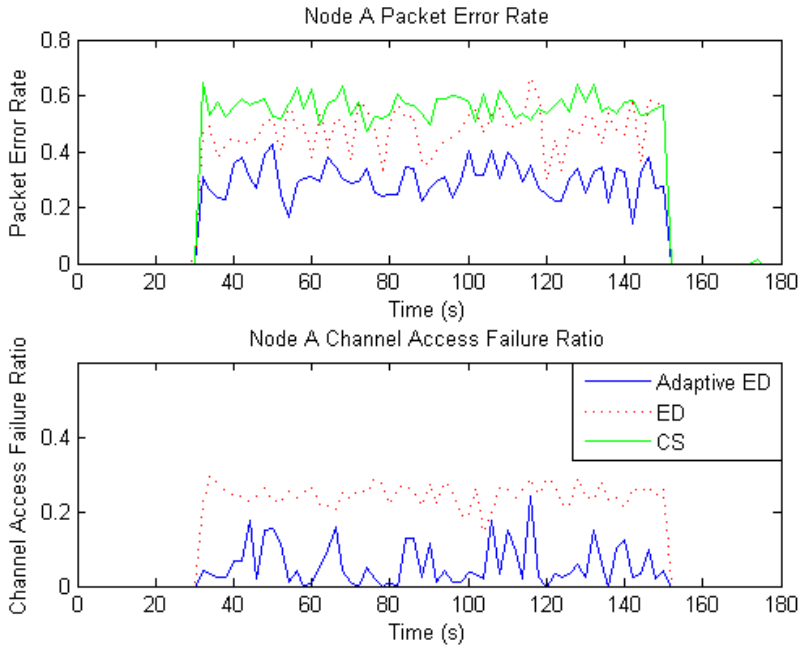
4.2.4 สมรรถนะเครือข่ายกรณีที่มีค่า frequency offset อื่น ๆ

การวิเคราะห์สมรรถนะเครือข่ายกรณีที่มีค่า frequency offset อื่นๆ จะวิเคราะห์กรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 เช่นกัน แต่จะเปลี่ยนช่องสัญญาณของเครือข่าย IEEE 802.15.4 จากช่องสัญญาณที่ 12 (ความถี่กลาง 2,410 MHz) เป็นช่องสัญญาณที่ 11 (ความถี่กลาง 2,405 MHz) ซึ่งจะทำให้ค่า frequency offset เพิ่มจาก 2 MHz เป็น 7 MHz

ผลการจำลองเครือข่ายกรณีค่า frequency offset เท่ากับ 7 MHz แสดงดังกราฟในรูปที่ 4.32 และรูปที่ 4.33 และสรุปค่าเฉลี่ยของผลการจำลองเครือข่ายได้ดังตารางที่ 4.12



รูปที่ 4.32 Throughput ของโนด A กรณี frequency offset เท่ากับ 7 MHz



รูปที่ 4.33 ค่า PER และ Channel Access Failure ratio ของโนด A กรณี frequency offset เท่ากับ 7 MHz

ตารางที่ 4.12 ผลการจำลองเครือข่ายกรณี frequency offset เท่ากับ 7 MHz

	Adaptive ED	ED	CS
Throughput	5.281	2.944	5.302
PER	0.299	0.480	0.563
Channel Access Failure ratio	0.058	0.245	0

จากผลการจำลองเครือข่ายในกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=1) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 เมื่อกำหนดให้ frequency offset ระหว่างความถี่กลางของเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b มีค่าเพิ่มขึ้นจาก 2 MHz เป็น 7 MHz จะเห็นว่าค่า throughput ของวิธีที่เสนอ และวิธี CS สูงขึ้นจากเดิม คือ จาก 4.416 kbps และ 4.881 kbps เป็น 5.281 kbps และ 5.302 kbps ตามลำดับ ขณะที่ค่า throughput ของวิธี ED ยังมีค่าใกล้เคียงกรณี frequency offset 2 MHz ทั้งนี้เนื่องจากการที่ค่า frequency offset สูงขึ้น จะทำให้พลังงานของเครือข่าย IEEE 802.11b ตกอยู่ในช่วงแบนด์วิดท์ของเครือข่าย IEEE 802.15.4 น้อยลง ซึ่งจะทำให้การแทรกสอดจากโนด W1 ไม่ทำให้ PER=1 อีกต่อไป ดังนั้น ผลการจำลองเครือข่ายจะมีแนวโน้มเช่นเดียวกับกรณีการแทรกสอดจากโนด W1 เป็น Scenario 1 (PER=0.5) และโนด W2 เป็น Scenario 3 โดยที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 ในหัวข้อที่ 4.2.1.5 แต่สมรรถนะของเครือข่าย IEEE 802.15.4 ในกรณีนี้จะต่ำกว่ากรณีหัวข้อ 4.2.1.5 ทั้งนี้เนื่องจากในกรณีนี้โนด W1 ทำให้เกิดการแทรกสอด scenario 1 ที่ PER=0.99 ในขณะที่หัวข้อ 4.2.1.5 การแทรกสอดจากโนด W1 จะเป็น Scenario 1 ที่ PER=0.5

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

เครือข่าย IEEE 802.15.4 กำลังเป็นที่สนใจในวงกว้างทั้งในการประยุกต์ใช้งานโดยเฉพาะกับระบบเครือข่ายเซ็นเซอร์ไร้สายต่างๆ เช่น ระบบอัตโนมัติภายในบ้าน ระบบการอ่านหน่วยมิเตอร์อัตโนมัติ ระบบควบคุมไฟแสงสว่าง หรือแม้กระทั่งระบบควบคุมอัตโนมัติในโรงงานอุตสาหกรรม อย่างไรก็ตาม เนื่องจากเครือข่าย IEEE 802.15.4 ทำงานบนแถบความถี่ 2.4 GHz ซึ่งเป็นแถบความถี่สาธารณะจึงมีเทคโนโลยีอื่นๆจำนวนมากที่ทำงานบนแถบความถี่นี้ โดยเฉพาะเครือข่าย IEEE 802.11b/g ที่มีการใช้งานกันอย่างแพร่หลายแทบทุกพื้นที่ ทำให้มีโอกาสสูงที่จะเกิดการแทรกสอดกับเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 ซึ่งด้วยลักษณะเฉพาะต่างๆของเครือข่าย IEEE 802.11b/g มีโอกาสทำให้สมรรถนะของเครือข่าย IEEE 802.15.4 ลดลงอย่างมากและทำให้ระบบต่างๆเหล่านี้มีโอกาสทำงานผิดพลาดได้ ปัญหาดังกล่าวได้มีงานวิจัยจำนวนมากที่ได้พัฒนาแนวทางการลดผลกระทบจากการแทรกสอดระหว่างเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b/g ซึ่งงานวิจัยส่วนใหญ่ได้เลือกใช้วิธีย้ายช่องสัญญาณของเครือข่าย IEEE 802.15.4 ไปยังช่องสัญญาณที่ไม่ได้รับผลกระทบจากการแทรกสอดไม่ว่าจะเป็นการย้ายช่องสัญญาณของทั้งเครือข่าย หรือการย้ายช่องสัญญาณเฉพาะโนดที่ได้รับผลกระทบจากการแทรกสอด ซึ่งทุกงานวิจัยที่เสนอให้แก้ปัญหาโดยการย้ายช่องสัญญาณนั้นจำเป็นต้องมีการส่งข้อมูลข่าวสารระหว่างโนดทั้งสิ้น ซึ่งในสภาวะที่มีการแทรกสอดหนาแน่นนั้น มีความเป็นไปได้ที่ข้อมูลข่าวสารเหล่านี้จะส่งไม่สำเร็จ ซึ่งอาจทำให้บางโนดไม่สามารถย้ายช่องสัญญาณได้เช่นเดียวกับโนดอื่นๆ ทำให้โนดดังกล่าวอาจเสมือนถูกตัดออกจากเครือข่าย นอกจากนี้ การย้ายช่องสัญญาณของทั้งเครือข่ายอาจไม่เหมาะสมนักกับเครือข่ายขนาดใหญ่ เนื่องจากต้องใช้เวลา ในการ scan หาช่องสัญญาณใหม่ รวมถึงการรับส่งข้อมูลข่าวสรเพื่อแจ้งให้แต่ละโนดย้ายเครือข่ายค่อนข้างนาน ซึ่งในช่วงเวลานี้เครือข่ายเซ็นเซอร์ไร้สายจะไม่สามารถรับส่งข้อมูลตามปกติได้เลย แม้จะมีงานวิจัยที่เสนอให้ย้ายช่องสัญญาณเฉพาะโนดที่ได้รับผลกระทบจากการแทรกสอด ซึ่งจะทำให้เครือข่าย IEEE 802.15.4 ทำงานแบบ Multi-channel ซึ่งในทางปฏิบัติแล้วการทำให้เครือข่าย IEEE 802.15.4 ทำงานแบบ Multi-channel นั้นค่อนข้างทำได้ยาก

โดยจำเป็นต้องมีการตั้ง schedule สำหรับโนดที่ทำหน้าที่สลับช่องสัญญาณให้ทำงานได้อย่างเหมาะสม

สำหรับวิธี Adaptive CCA ซึ่งเสนอแนวทางแก้ปัญหาในชั้น MAC และเป็นแบบ Distribute คือแต่ละโนดสามารถทำงานด้วยตนเองโดยไม่จำเป็นต้องมีการส่งข้อมูลข่าวสารระหว่างโนด ข้อด้อยของวิธี Adaptive CCA คือการพยายามลดค่า ED threshold ลงเรื่อยๆ จนกว่าโนดส่งจะตรวจสอบพบว่าช่องสัญญาณว่าง หรือ ค่า ED threshold ลดลงจนถึงค่าต่ำที่สุดที่ยินยอมให้ใช้ ซึ่งวิธีนี้จะพิจารณาเพียงการลด Inhibition Loss แต่อาจทำให้เกิด Collision Loss มากขึ้น ซึ่งแท้จริงแล้ว Collision Loss จะมีผลกระทบรุนแรงกว่า Inhibition Loss

งานวิจัยนี้ได้เสนอแบบแผนการทำงานเพื่อควบคุมการเข้าถึงช่องสัญญาณของเครือข่ายเซ็นเซอร์ไร้สายบนมาตรฐาน IEEE 802.15.4 เพื่อเพิ่มสมรรถนะโดยรวมของเครือข่ายเซ็นเซอร์ไร้สาย ในกรณีที่มีการแทรกสอดจากเครือข่าย IEEE 802.11b/g โดยเลือกแนวทางการแก้ปัญหาในชั้น MAC และเป็นแบบ Distribute โดยจะเสนอให้โนดส่งใช้วิธีที่ 3 *Carrier sense with energy above energy threshold* โดยใช้ตัวดำเนินการทางตรรกศาสตร์ OR ในการทำ CCA นั่นคือโนดส่งจะใช้ทั้งวิธี ED และวิธี CS ในการตรวจสอบช่องสัญญาณ โดยโนดส่งสามารถปรับเปลี่ยนค่า ED threshold ให้สอดคล้องกับสภาวะของการแทรกสอดในขณะนั้น โดยหากโนดส่งไม่สามารถส่งแพ็กเกตข้อมูลได้สำเร็จติดต่อกันเป็นจำนวนครั้งตามที่กำหนด โนดส่งจะทำ ED scan เพื่อตรวจวัดระดับพลังงานที่ใช้งานช่องสัญญาณอยู่ในขณะนั้น ซึ่งมีความเป็นไปได้สูงว่าจะเป็นสัญญาณแทรกสอดที่ทำให้เซ็นเซอร์โนดส่งแพ็กเกตข้อมูลล้มเหลวในตอนแรกนั่นเอง และโนดส่งจะนำค่า RSSI ที่วัดได้ดังกล่าวมาตั้งเป็นค่า ED threshold สำหรับการส่งแพ็กเกตข้อมูลไปยังโนดปลายทางนั้นๆ หรืออาจกล่าวได้ว่าโนดส่งจะจดจำสัญญาณแทรกสอดที่ส่งกระทบให้การส่งแพ็กเกตข้อมูลล้มเหลวจากค่า RSSI ที่วัดได้นั่นเอง ดังนั้น หากมีสัญญาณแทรกสอดที่มีพลังงานต่ำกว่าค่า ED threshold ดังกล่าว โนดส่งจะสามารถส่งแพ็กเกตข้อมูลได้ในช่วงนี้ ด้วยการทำงานในรูปแบบนี้จะทำให้เซ็นเซอร์โนดทุกตัวสามารถใช้งานช่องสัญญาณได้อย่างคุ้มค่าที่สุด

เมื่อพิจารณาผลการจำลองการทำงานตามรายละเอียดในบทที่ 4 สามารถสรุปความเหมาะสมของวิธีที่เสนอ วิธี ED และวิธี CS ตามการเกิดการแทรกสอด scenario ต่างๆได้ดังนี้

5.1.1 **เมื่อการแทรกสอดทั้งหมดเป็น** Scenario 1

กรณีที่การแทรกสอดทั้งหมดทำให้การส่งแพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 มี PER เท่ากับ 1 วิธีที่เสนอจะมีสมรรถนะโดยรวมต่ำที่สุด คือ มีค่า throughput ต่ำที่สุด ในขณะที่มี

ค่า PER สูงที่สุดเท่ากับวิธี CS แต่หากพิจารณาสมรรถนะโดยรวมของทุกวิธีแล้วถือว่าไม่แตกต่างกันมากนัก คือ ทุกวิธีล้วนมีสมรรถนะต่ำมาก และไม่สามารถรองรับการประยุกต์ใช้งานของเครือข่ายเซ็นเซอร์ไร้สายได้ ซึ่งหากเกิดการแทรกสอดกรณีเช่นนี้ การเลือกใช้วิธีย้ายช่องสัญญาณน่าจะเหมาะสมที่สุด

เมื่อพิจารณาผลกระทบจากการแทรกสอดให้มีค่า PER ต่ำลงมา พบว่าวิธี CS มีแนวโน้มที่จะมีสมรรถนะสูงขึ้นมากที่สุด ในขณะที่วิธีที่เสนอจะมีสมรรถนะสูงกว่าวิธี ED เล็กน้อย โดยยิ่ง PER มีค่าต่ำลงมากขึ้น วิธี CS ก็จะมีสมรรถนะสูงกว่าวิธีอื่นๆมากขึ้น

ดังนั้นจึงพอสรุปได้ว่ากรณีที่การแทรกสอดทั้งหมดเป็น Scenario 1 หากการแทรกสอดทั้งหมดทำให้เกิด PER =1 ควรจะเลือกใช้วิธีย้ายช่องสัญญาณในการแก้ไขปัญหาการแทรกสอด แต่หากการแทรกสอดทั้งหมดทำให้เกิด PER ต่ำลงมา วิธี CS น่าจะเหมาะสมกว่าวิธีอื่นๆ อย่างไรก็ตามโอกาสที่การแทรกสอดทั้งหมดเป็น Scenario 1 มีน้อยมาก ดังตัวอย่างพื้นที่การเกิด scenario ต่างๆ สำหรับรูปแบบเครือข่ายที่ใช้ในงานวิจัยนี้ในรูปที่ 5.1

5.1.2 เมื่อการแทรกสอดเป็นทั้ง Scenario 1 และ Scenario 3

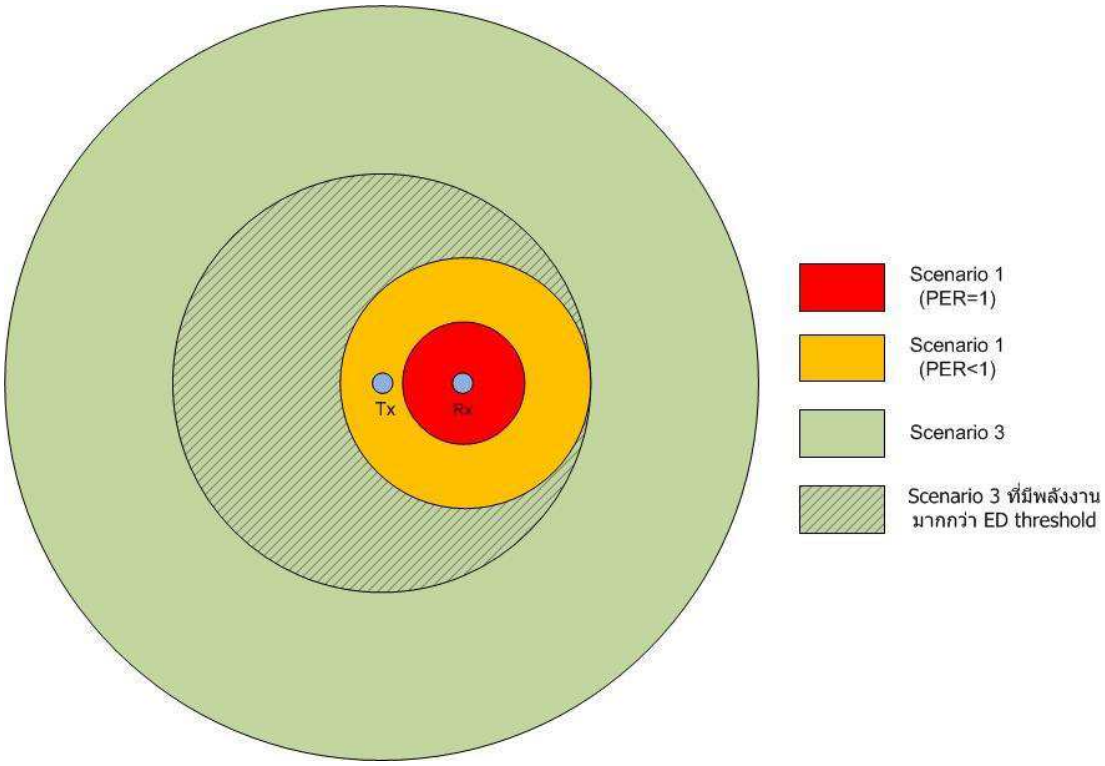
กรณีนี้เป็นเป้าหมายหลักของวิธีที่เสนอในงานวิจัยนี้ในการเพิ่มสมรรถนะของเครือข่าย IEEE 802.15.4 เนื่องจากเป็นรูปแบบการแทรกสอดที่สามารถปรับปรุงสมรรถนะเครือข่ายได้ หากโนดส่งรอการส่งแพ็กเกตข้อมูลในช่วงที่เกิดการแทรกสอด Scenario 1 และสามารถส่งแพ็กเกตข้อมูลได้ในช่วงที่เกิดการแทรกสอด Scenario 3 ซึ่งเป็นที่มาของวิธีที่เสนอ ซึ่งเมื่อพิจารณาผลการจำลองเครือข่ายจะเห็นว่าวิธีที่เสนอมีสมรรถนะโดยรวมดีกว่าวิธี ED และวิธี CS อย่างเห็นได้ชัด โดยเมื่อเปรียบเทียบกับวิธี ED จะเห็นว่าวิธีที่เสนอมีค่า throughput สูงกว่ามาก และยังมีค่า PER และ Channel Access Failure ratio ต่ำกว่าวิธี ED อีกด้วย ในขณะที่การเปรียบเทียบกับวิธี CS แม้วิธีที่เสนอจะมีค่า throughput ต่ำกว่าเล็กน้อย แต่วิธีที่เสนอมีค่า PER ต่ำกว่าวิธี CS อยู่มาก ซึ่งค่า throughput ของวิธี CS ที่สูงกว่าวิธีที่เสนอเล็กน้อย อาจไม่คุ้มค่ากับค่า PER ที่สูงกว่ามาก เนื่องจากการส่งแพ็กเกตข้อมูลล้มเหลวบ่อยครั้งจะทำให้สิ้นเปลืองพลังงานและอาจนำไปสู่การสูญหายของข้อมูลสำคัญได้

อย่างไรก็ตาม ยังมีความเป็นไปได้ที่จะมีระดับพลังงานที่สูงกว่าค่า ED threshold ที่ไม่ทำให้การส่งแพ็กเกตข้อมูลล้มเหลว ซึ่งเป็นที่มาของการแบ่งกรณีการทดสอบออกเป็น 2 กรณี คือ กรณีที่โนด W2 อยู่ห่างจากโนด A มากกว่าโนด W1 และกรณีที่โนด W2 อยู่ใกล้โนด A มากกว่าโนด W1 ดังรายละเอียดในบทที่ 4 ซึ่งหากเกิดกรณีดังกล่าวขึ้น วิธีที่เสนอจะมีลักษณะคล้ายกับวิธี

ED ซ้ำยังมีสมรรถนะโดยรวมต่ำกว่าวิธี ED เล็กน้อย เนื่องจากวิธีที่เสนอมีช่วงเวลา ED scan ซึ่งใช้เวลาประมาณ 128 μs ต่อครั้ง และในช่วงที่ทำ ED scan ยังมีโอกาสทำให้เกิดการวัดพลังงานผิดพลาดในกรณีที่โนดที่ทำให้เกิดการแทรกสอด Scenario 1 และโนดที่ทำให้เกิดการแทรกสอด Scenario 3 สลับการทำงานกันพอดีอีกด้วย ส่งผลให้โนดส่งใช้ค่าพลังงานจากโนดที่ทำให้เกิดการแทรกสอด Scenario 3 มาตั้งเป็นค่า ED threshold แทน ซึ่งจะทำให้โนดส่งสามารถส่งแพ็กเกตข้อมูลในช่วงที่เกิดการแทรกสอด Scenario 1 โอกาสเกิดการล้มเหลวสูงมาก

5.1.3 เมื่อการแทรกสอดทั้งหมดเป็น Scenario 3

กรณีการแทรกสอดทั้งหมดเป็น Scenario 3 วิธีที่เสนอจะมีสมรรถนะเช่นเดียวกับวิธี CS ซึ่งเป็นวิธีที่เหมาะสมที่สุดสำหรับการแทรกสอด Scenario 3 ซึ่งโนดส่งสามารถตรวจจับสัญญาณแทรกสอดได้ แต่สัญญาณแทรกสอดดังกล่าวไม่ทำให้การส่งแพ็กเกตข้อมูลล้มเหลว ในขณะที่การใช้วิธี ED โนดส่งจะตรวจพบว่าช่องสัญญาณไม่ว่างและจะไม่ส่งแพ็กเกตข้อมูลในช่วงที่มีสัญญาณแทรกสอดดังกล่าว ทำให้เสียโอกาสในการใช้งานช่องสัญญาณไป เนื่องจากสัญญาณแทรกสอดดังกล่าวไม่ได้ส่งผลกระทบต่อการส่งแพ็กเกตข้อมูลนั่นเอง



รูปที่ 5.1 พื้นที่การเกิด scenario ต่างๆ สำหรับรูปแบบเครือข่ายที่ใช้ในงานวิจัยนี้

รูปที่ 5.1 แสดงตัวอย่างพื้นที่การเกิด scenario ต่างๆ สำหรับรูปแบบเครือข่ายที่ใช้ทดสอบในงานวิจัยนี้ คือ กำหนดให้โนดส่งและโนดรับของเครือข่าย IEEE 802.15.4 อยู่ห่างกัน 5 เมตร สามารถอธิบายรูปที่ 5.1 ได้ดังนี้

1. หากโนดส่งของเครือข่าย IEEE 802.11b อยู่ในพื้นที่วงกลมสีแดง จะส่งผลให้เกิดการแทรกสอด Scenario 1 ที่มี PER=1 ซึ่งพื้นที่ในกรณีนี้จะมีรัศมีประมาณ 4 เมตรรอบโนดรับของเครือข่าย IEEE 802.15.4

2. หากโนดส่งของเครือข่าย IEEE 802.11b อยู่ในพื้นที่วงกลมสีส้มจะทำให้เกิดการแทรกสอด Scenario 1 ที่มี PER < 1 โดยยิ่งโนดส่งของเครือข่าย IEEE 802.11b อยู่ห่างจากพื้นที่วงกลมสีแดงมากขึ้น ค่า PER ก็จะลดลงมากขึ้น ซึ่งพื้นที่ในกรณีนี้จะมีรัศมีประมาณ 7 เมตร จากโนดรับของเครือข่าย IEEE 802.15.4

3. หากโนดส่งของเครือข่าย IEEE 802.11b อยู่ในพื้นที่วงกลมสีเขียวไม่มีลายจะทำให้เกิดการแทรกสอด Scenario 3 ซึ่งพื้นที่ในกรณีนี้จะมีรัศมีประมาณ 22.8 เมตร จากโนดส่งของเครือข่าย IEEE 802.15.4

4. หากโนดส่งของเครือข่าย IEEE 802.11b อยู่ในพื้นที่วงกลมสีเขียวมีลายจะทำให้เกิดการแทรกสอด Scenario 3 ที่ทำให้ค่าพลังงานของสัญญาณแทรกสอดสูงกว่าค่า ED threshold ของวิธีที่เสนอ ซึ่งจะทำให้วิธีที่เสนอมีสมรรถนะต่ำกว่าวิธีอื่น อย่างไรก็ตาม โอกาสที่ทำให้เกิดการแทรกสอดกรณีนี้จะมีน้อยกว่าโอกาสที่จะเกิดการแทรกสอดในข้อที่ 3 อยู่มาก ซึ่งพื้นที่สีเขียวมีลายในรูปที่ 4.1 ถือเป็นกรณีเลวร้ายที่สุดที่มีโอกาสเกิดขึ้นได้แล้ว โดยจะมีรัศมีประมาณ 12 เมตร จากโนดส่งของเครือข่าย IEEE 802.15.4 (รัศมี 12 เมตร คิดมาจากระยะทางระหว่างโนดส่งและโนดรับของเครือข่าย IEEE 802.15.4 ซึ่งเท่ากับ 5 เมตร บวกกับ รัศมีพื้นที่สีส้มซึ่งเป็นรัศมีสูงสุดที่ทำให้เกิดการแทรกสอด Scenario 1 ซึ่งเท่ากับ 7 เมตร) แต่ในความเป็นจริงแล้วที่ระยะรัศมี 7 เมตรของพื้นที่สีส้มทำให้เกิด PER = 0.0075 เท่านั้น หากพิจารณารัศมีของพื้นที่สีส้มซึ่งทำให้เกิด PER ในระดับที่พอจะส่งผลกระทบต่อเครือข่าย IEEE 802.15.4 จะอยู่ที่ประมาณ 5-6 เมตร ซึ่งจะทำให้กรณีเลวร้ายที่สุดสำหรับรัศมีของพื้นที่สีเขียวมีลายนี้ลดลงเหลือประมาณ 10-11 เมตร

5.1.4 ผลกระทบจากปัจจัยอื่น ๆ

การวิเคราะห์ผลกระทบจากปัจจัยอื่นๆพบว่าวิธีที่เสนอยังสามารถทำงานได้ดีกว่าวิธีอื่นๆ เมื่อปรับเปลี่ยนรูปแบบการส่งแพ็กเกตข้อมูลของเครือข่าย IEEE 802.15.4 ให้มีความถี่ลดลง

รวมทั้งกรณีที่ค่า frequency offset ระหว่างความถี่กลางของเครือข่าย IEEE 802.15.4 กับเครือข่าย IEEE 802.11b มีค่าเพิ่มขึ้น แต่เมื่อปรับเปลี่ยนขนาดของแพ็กเกตข้อมูลให้มีขนาดใหญ่ขึ้น วิธี CS จะมีสมรรถนะสูงกว่าวิธีที่เสนอและวิธี ED ตามลำดับ แต่ทุกวิธีล้วนมีค่า PER สูงมาก เนื่องจากขนาดของแพ็กเกตข้อมูลที่ใหญ่ขึ้นทำให้โอกาสชนกับสัญญาณแทรกสอดมีมากขึ้นนั่นเอง

5.2 ข้อเสนอแนะ

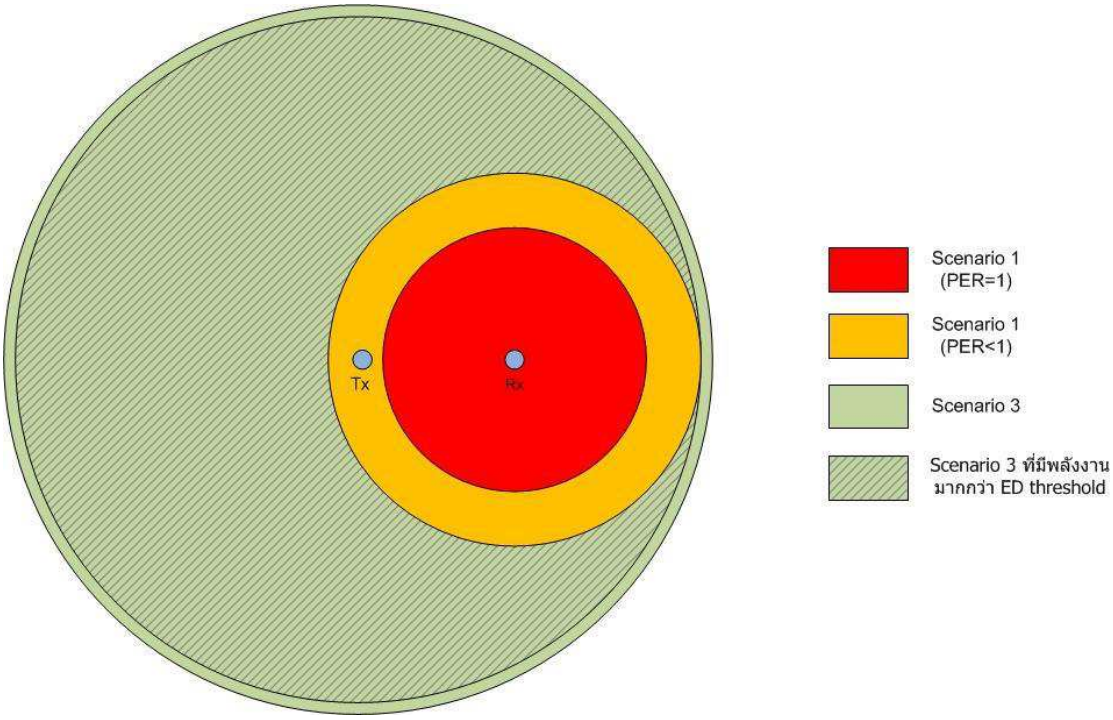
งานวิจัยนี้ได้เสนอวิธีปรับปรุงการทำงานของเครือข่ายเซ็นเซอร์ไร้บนมาตรฐาน IEEE 802.15.4 ในกรณีที่ใช้งานแถบความถี่ร่วมกันกับเครือข่าย IEEE 802.11b/g เพื่อบรรเทาปัญหาที่สมรรถนะการทำงานของเครือข่ายเซ็นเซอร์ไร้สายอาจลดลง อันเนื่องมาจากการแทรกสอดระหว่างสัญญาณของทั้ง 2 มาตรฐานข้างต้น โดยใช้การออกแบบวิธีตรวจสอบการเกิดการแทรกสอด และการปรับเปลี่ยนวิธีตรวจสอบเพื่อเข้าถึงช่องสัญญาณของโนดส่งในมาตรฐาน IEEE 802.15.4 ให้เหมาะสมกับสภาวะของการแทรกสอด แต่จากการศึกษาและทดสอบพบว่าวิธีที่เสนอยังมีจุดที่ควรจะได้รับการพัฒนาต่อไปเพื่อให้รองรับการแทรกสอดใน scenario ต่างๆได้ดีขึ้น รวมทั้งยังมีประเด็นหรือปัจจัยอื่นๆที่ส่งผลต่อประสิทธิภาพการทำงานของวิธีที่เสนอที่งานวิจัยนี้ยังไม่ได้พิจารณาหรือทำการทดสอบ ซึ่งสามารถสรุปเป็นข้อเสนอแนะสำหรับงานวิจัยในอนาคตดังนี้

1. วิธีที่เสนอจะทำงานได้ดีในกรณีที่มีการแทรกสอดจากทั้ง Scenario 1 และ Scenario 3 สลับกันไปเท่านั้น ซึ่งหากเกิดการแทรกสอด Scenario 1 เพียงอย่างเดียว หรือ เกิดการแทรกสอดจากทั้ง Scenario 1 และ Scenario 3 สลับกันไป แต่การแทรกสอด Scenario 1 ทำให้เกิด PER ต่ำมาก วิธี CS อาจจะเหมาะสมกว่าวิธีที่เสนอ ดังนั้น การปรับปรุงวิธีที่เสนอให้นำค่า throughput และค่า PER มาใช้ในการพิจารณาเลือกวิธีแก้ปัญหาการแทรกสอดให้เหมาะสมไม่ว่าจะเป็นการย้ายช่องสัญญาณ การใช้วิธีที่เสนอ วิธี ED หรือวิธี CS น่าจะทำให้สามารถบรรเทาปัญหาจากการแทรกสอดได้ครอบคลุมมากขึ้นในทุกๆ scenario

2. ในการจำลองการทำงานของงานวิจัยนี้กำหนดคู่ของโนดส่งและโนดรับของเครือข่าย IEEE 802.15.4 ในการพิจารณา รวมถึงคู่ของโนดส่งและโนดรับของสัญญาณแทรกสอดภายในเครือข่าย IEEE 802.15.4 และสัญญาณแทรกสอดจากเครือข่าย IEEE 802.11b เพียงอย่างละ 1 คู่เท่านั้น ดังนั้น การจำลองการทำงานโดยเพิ่มจำนวนโนดของทั้งเครือข่าย IEEE 802.15.4 และเครือข่าย IEEE 802.11b/g น่าจะทำให้วิเคราะห์ผลได้ครอบคลุมมากขึ้น

3. วิธีที่เสนอจะเหมาะสำหรับกรณีที่โนดส่งและโนดรับของเครือข่าย IEEE 802.15.4 อยู่ห่างกันไม่มากนัก เพราะหากโนดส่งและโนดรับอยู่ห่างกันมาก การที่โนดส่งนำค่าพลังงานของสัญญาณ

แทรกสอดที่ส่งผลกระทบต่อโนดรับมาใช้เป็นค่า ED Threshold จะมีโอกาสเกิดกรณีการแทรกสอด Scenario 3 ที่ทำให้ค่าพลังงานของสัญญาณแทรกสอดสูงกว่าค่า ED threshold มากขึ้น ดังแสดงในรูปที่ 5.2 หากโนดส่งและโนดรับของเครือข่าย IEEE 802.15.4 อยู่ห่างกัน 10 เมตร โอกาสเกิดการแทรกสอด Scenario 3 ที่ค่าพลังงานของสัญญาณแทรกสอดมีโอกาสสูงกว่าค่า ED threshold (พื้นที่สีเขียวมีลาย) จะสูงเกือบเทียบเท่าโอกาสเกิด Scenario 3 ทั่วไป (พื้นที่สีเขียวไม่มีลาย) ทำให้วิธีที่เสนอจะมีสมรรถนะพอๆกับวิธี ED เท่านั้น



รูปที่ 5.2 พื้นที่การเกิด scenario ต่างๆ เมื่อโนดส่งและโนดรับของเครือข่าย IEEE 802.15.4 อยู่ห่างกัน 10 เมตร

3. งานวิจัยนี้พิจารณาสมรรถนะเครือข่ายเพียง 3 พารามิเตอร์ คือ ค่า throughput, PER และ Channel Access Failure ratio เท่านั้น เนื่องจากมุ่งเน้นไปที่การปรับปรุงสมรรถนะของเครือข่าย ซึ่งงานวิจัยต่อไปอาจศึกษาพารามิเตอร์อื่นๆนอกเหนือจากนี้เพื่อที่จะวิเคราะห์ความเหมาะสมของวิธีที่เสนอ รวมทั้งวิธี ED และวิธี CS ในหลายๆด้าน

4. งานวิจัยนี้จัดทำโดยใช้มาตรฐาน IEEE 802.15.4 ปี 2006 โดยในระหว่างการวิจัยพบว่ามาตรฐาน IEEE 802.15.4 ได้ถูกปรับปรุงใหม่เป็นฉบับปี 2011 ซึ่งรายละเอียดบางส่วนได้ถูกปรับปรุงใหม่จากฉบับปี 2006 ดังนั้น งานวิจัยต่อจากนี้ควรศึกษาโดยอ้างอิงจากมาตรฐาน IEEE 802.15.4 ฉบับปี 2011

รายการอ้างอิง

[1] Shahin farahani, Zigbee Wireless Networks and Transceivers, USA: Elsevier Ltd January, 2008, pp. 25-32.

[2] IEEE 802.15.4 Specification, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), September 8, 2006.

[3] IEEE 802.11 Specification, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 12, 2007.

[4] S. Y. Shin, H. S. Park, S. Choi and W. H. Kwon, "Packet Error Rate Analysis of Zigbee under WLAN and Bluetooth Interference," IEEE Trans. on Wireless Communications, Vol. 6, pp. 2825-2830, August 2007.

[5] D. G. Yoon, S. Y. Shin , W. H. Kwon and H. S. Park, “Packet Error Rate Analysis of IEEE 802.11b under IEEE 802.15.4 Interference,” in IEEE Vehicular Technology Conference, Vol. 3, pp. 1186-1190, May 2006.

[6] W. Yuan, X. Wang, J. P. M. G. Linnartz and I. G. M. M. Niemegeers, “Experimental Validation of a Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g Networks,” IRA-DSN’09, 2009.

[7] ZigBee Specification, ZigBee Alliance, January 17, 2008.

[8] P. Yi, A. Iwayemi and C. Zhou, “Frequency Agility in a ZigBee Network for Smart Grid Application,” Innovative Smart Grid Technologies, pp. 1-5, January 2010.

[9] C. Won, J. H. Youn, H. Ali, H. Sharif and J. Deogun, “Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b,” in IEEE Vehicular Technology Conference, Vol. 4, pp. 2522-2526, September 2005.

[10] M. S. Kang, J. W. Chong, H. Hyun, S. M. Kim, B. H. Jung and D. K. Sung, “Adaptive Interference-Aware Multi-Channel Clustering Algorithm in a ZigBee Network in the Presence of WLAN Interference,” International Symposium on Wireless Pervasive Computing, pp. 200-205, February 2007.

[11] W. Yuan, X. Cui, and I. G. M. M. Niemegeers, Distributed Adaptive Interference-Avoidance Multi-channel MAC Protocol for Zigbee Networks, 10th IEEE International Conference on Computer and Information Technology, 2010.

[12] S. M. Kim, J. W. Chong, C. Y. Jung, T. H. Jeon, J. H. Park, Y. J. Kang,S. H. Jeong, M. J. Kim, and D. K. Sung, “Experiments on Interference and Coexistence between Zigbee and WLAN Devices Operating in the 2.4 GHz ISM Band,” in Proc. NGPC, pp. 15 - 19, Nov 2005.

[13] W. Yuan, J. P. M. G. Linnartz and I. G. M. M. Niemegeers, Adaptive CCA for IEEE 802.15.4 Wireless Sensor Networks to Mitigate Interference, Wireless Communications and Networking Conference, April 2010.

[14] IEEE 802.15.2 Specification, Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands, August 28, 2003.

[15] S. Y. Shin, S. Choi, H. S. Park, and W. H. Kwon, “Packet Error Rate Analysis of IEEE 802.15.4 Under IEEE 802.11b Interference,” Wired/Wireless Internet Communications, pp. 279–288, May 2005.

ภาคผนวก

ประวัติผู้เขียนวิทยานิพนธ์

นายวันทวัฒน์ วงศ์มาโนชญ์ เกิดเมื่อวันที่ 27 กันยายน พ.ศ. 2526 ที่จังหวัดสงขลา จบการศึกษาระดับมัธยมศึกษาจากโรงเรียนมหาวชิราวุธ จังหวัดสงขลา และสำเร็จการศึกษาระดับวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จากมหาวิทยาลัยธรรมศาสตร์ ในปีการศึกษา 2548 หลังจบการศึกษาได้เข้าทำงานตำแหน่งวิศวกรไฟฟ้า บริษัทเหล็กก่อสร้างสยาม จำกัด ตั้งแต่ปี 2549 ถึงปี 2552 จากนั้นได้เข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2552 และได้เข้าทำงานตำแหน่งวิศวกรไฟฟ้า การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ตั้งแต่ปี 2554 ถึงปัจจุบัน

บทความทางวิชาการเรื่อง ADAPTIVE ED THRESHOLD FOR IEEE 802.15.4 TO SUPPORT COEXISTENCE WITH IEEE 802.11B/G ซึ่งเป็นส่วนหนึ่งของวิทยานิพนธ์ฉบับนี้ ได้รับการตีพิมพ์ใน Proceedings of The 2013 International Electrical Engineering Congress (iEECON2013) ฉบับปี 2013 หน้า 292-295