

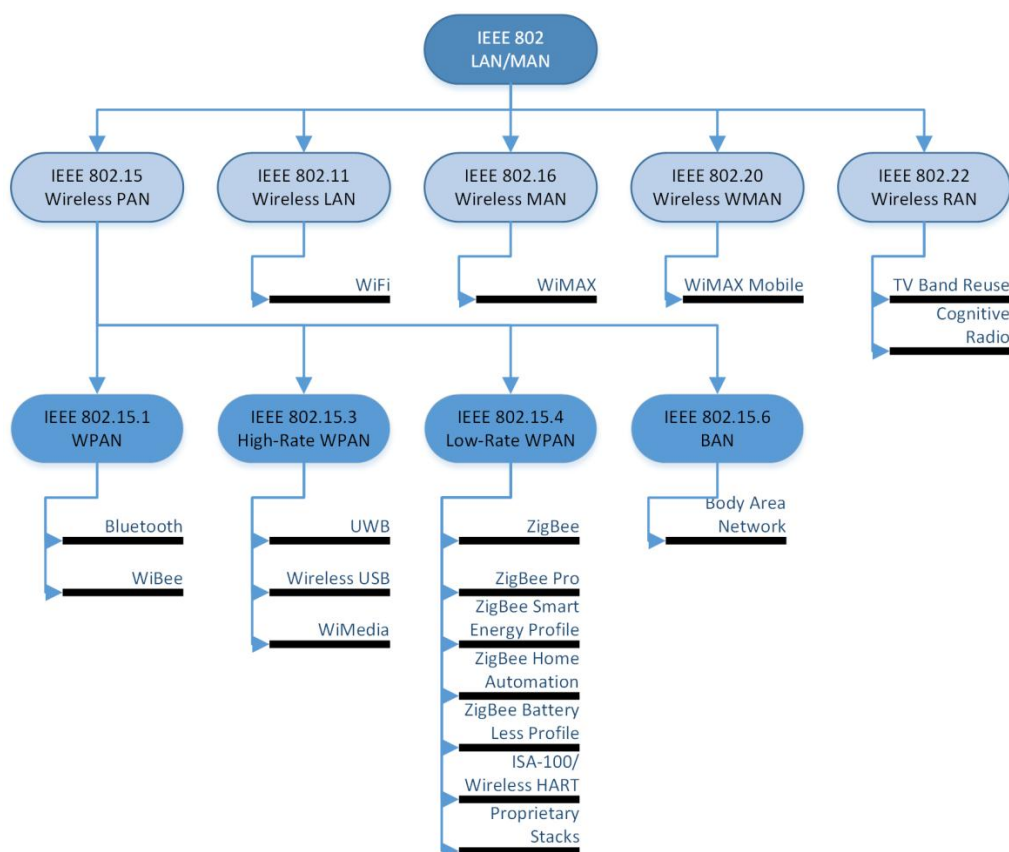
บทที่ 2

ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

ทฤษฎีที่เกี่ยวข้อง

2.1 เครือข่ายไร้สาย

ปัจจุบันเครือข่ายไร้สายมีการประยุกต์ใช้งานกันมากขึ้น และมีการแบ่งแยกกลุ่มงานวิจัยและพัฒนาออกไปเป็นแต่ละด้านโดยอ้างอิงตามมาตรฐาน IEEE802 แล้ว สามารถแบ่งออกเป็นส่วนต่างๆ ได้ดังนี้



ภาพที่ 2.1 แผนผังแสดงมาตรฐาน IEEE802

ที่มา: http://www.eetasia.com/ART_8800590160_590626_NT_3e1932a3.HTM

งานวิจัยนี้จะมุ่งเน้นไปในส่วนของ IEEE802.15.4 LR-WPAN ซึ่งเป็นกลุ่มที่เน้นเรื่องของอัตราการส่งข้อมูลที่ต่ำ และการประหยัดพลังงาน ซึ่งเราจะลงไปในส่วนที่เป็นมาตรฐาน IEEE802.15.4 ซึ่งเป็นมาตรฐานที่มีการนำไปใช้งานใน WSN มากที่สุด ซึ่ง WSN คือเครือข่ายที่ประกอบไปด้วยโหนดเซนเซอร์ต่างๆ ที่กระจายตัวอยู่กันอย่างอิสระ เพื่อใช้ในการเฝ้าติดตามตัวแปรทางด้านฟิสิกส์ต่างๆ ในบริเวณหรือพื้นที่ที่สนใจ เช่น ความดัน ระดับเสียง อุณหภูมิ ความชื้น ความเข้มแสง แรง ความเค้น ความเครียดที่วัตถุ ฯลฯ โดยอาศัยเซนเซอร์ที่ตรงกับความต้องการในการวัด เช่น วัดอุณหภูมิ อาจจะใช้ อาร์ทีดี วัดแรงอาจใช้โซลิดเชลล์ และตัว WSN จะต้องสามารถส่งผ่านข้อมูลที่ไ่มายังส่วนกลางได้ ปัจจุบัน WSN สมัยใหม่ได้มีการเพิ่มความสามารถในการทำงานโดยสามารถที่จะควบคุมอุปกรณ์ปลายทางที่ต่ออยู่กับโหนดของเครือข่ายได้ ในการพัฒนาเครือข่ายเซนเซอร์ไร้สายตั้งแต่อดีตนั้นได้แรงจูงใจมาจากความต้องการใช้งานในทางการทหาร เช่น สนามรบ ตรวจจับการบุกรุก การเคลื่อนพล การใช้อาวุธเคมี จนถึงในปัจจุบัน ได้มีการนำมาประยุกต์ใช้ในหลากหลายอุตสาหกรรม เช่น การเฝ้าติดตามกระบวนการผลิต การติดตามและควบคุมการทำงานของเครื่องจักร การติดตามสุขภาพของผู้ป่วย

ใน WSN สามารถมีโหนดจากไม่กี่ร้อย จนกระทั่งเป็นหลักพันได้ โดยแต่ละโหนดสามารถต่อเข้ากับเซนเซอร์แต่ละชนิด ในแต่ละโหนดจะประกอบด้วยส่วนหลัก 3 ส่วน ดังนี้ ส่วนแรกภาคส่งสัญญาณวิทยุรวมถึงสายอากาศ (RF Transceiver And Antenna) ส่วนของสายอากาศนั้นมีทั้งแบบอยู่ที่ตัวโหนดหรือสายอากาศภายใน (Internal Antenna) และแบบที่ใช้ขั้วต่อสายจากภาคส่งสัญญาณวิทยุไปยังสายอากาศด้านนอก (External Antenna) ส่วนที่สอง เป็นส่วนของคอนโทรล ซึ่งโดยปกติจะใช้ไมโครคอนโทรลเลอร์ที่มีขนาดเล็กและใช้พลังงานต่ำ รวมถึงวงจรอินเตอร์เฟสที่เป็นตัวรับสัญญาณจากตัวเซนเซอร์มายังตัวไมโครคอนโทรลเลอร์ โดยปกติแล้วสัญญาณจากตัวตัวเซนเซอร์มีอยู่ 2 แบบคือสัญญาณที่เป็นแบบดิจิทัล กับสัญญาณที่เป็นแบบอนาล็อก ส่วนที่สามเป็นภาคจ่ายไฟ ซึ่งโดยปกติจะใช้แบตเตอรี่เนื่องจากโหนดต่างๆ จะถูกกระจายติดตั้งในพื้นที่ต่างๆ จึงยากที่จะใช้พลังงานจากแหล่งจ่ายไฟปกติ หรือจะใช้พลังงานไฟฟ้าจากการผลิตขึ้นที่โหนดเลยก็ได้เช่น จากไดนาโมขนาดเล็ก หรือแผงเซลล์พลังงานแสงอาทิตย์ โดยระดับแรงดันที่ใช้ในแต่ละโหนดนั้นจะขึ้นอยู่กับส่วนควบคุมว่าใช้แรงดันเท่าไร โดยปกติจะใช้อยู่ 3.3 โวลต์ดีซี

ตัวเซนเซอร์โหนดนั้นอาจจะมีขนาดที่แตกต่างกัน ซึ่งขึ้นอยู่กับงานที่ใช้ โดยต้นทุนของแต่ละโหนดมีตั้งแต่ราคาถูกจนกระทั่งราคาแพง ซึ่งตัวแปรด้านต้นทุนที่สำคัญนั้นก็คือ ความซับซ้อนของโหนด ฟังก์ชันในการทำงานของแต่ละโหนด ซึ่งปัจจัยต่างๆ เหล่านี้ไม่ว่าจะเป็น ต้นทุน หรือขนาด เป็นตัวกำหนดคุณสมบัติทางกายภาพของโหนดเซนเซอร์ เช่น อายุการใช้งาน

ของโหนดซึ่งโหนดที่ต้องการอายุการทำงานที่นาน ก็จะต้องการพลังงานในการทำงานที่สูงกว่า โหนดที่ไม่ต้องการอายุการทำงานที่ยาว ขนาดของหน่วยความจำ ความเร็วในการประมวลผล และ ความเร็วในการสื่อสารข้อมูล โดยโครงสร้าง WSN นั้น สามารถเป็นได้ทั้งแบบอย่างง่ายเช่น เครือข่ายแบบดาว (Star Network) จนกระทั่งถึงเป็นแบบที่ซับซ้อนมากๆ หรือเครือข่ายเมช (Mesh Network) โดยทั้งหมดนี้สามารถเริ่มการเชื่อมต่อระหว่างโหนดได้โดยการใช้เส้นทาง (Routing) หรือการกระจายข้อมูลออกไปทั้งหมด (Flooding)

2.2 การประยุกต์ใช้งาน WSN

การประยุกต์ใช้งานเครือข่าย WSN นั้น สามารถใช้งานได้หลากหลาย โดยขึ้นอยู่กับวัตถุประสงค์ในการใช้งาน และความต้องการพื้นฐานของระบบ ไม่ว่าจะเป็นการตรวจวัดเพื่อเก็บข้อมูลเพียงการเดียว หรือมีการควบคุมสั่งการจากระยะไกล หรือต้องการทั้งการตรวจวัดเพื่อเก็บข้อมูลและการควบคุมสั่งการจากระยะไกล ซึ่งในการตรวจวัดนั้นจะต้องหาเซนเซอร์ที่เหมาะสมกับงานที่ต้องการตรวจวัด หรือการควบคุมก็จะต้องการอุปกรณ์ควบคุมที่เหมาะสมกับงานมาใช้ โดยตัวอย่างการใช้งาน WSN ที่ได้ศึกษามามีอยู่หลากหลายซึ่งได้แสดงรายละเอียดไว้ดังนี้

2.2.1 การเฝ้าระวังพื้นที่ (Area Monitoring)

เป็นการประยุกต์ใช้งาน WSN โดยการกระจายตัวโหนดเซนเซอร์ไปยังพื้นที่ ที่เราสนใจ ตัวอย่างเช่นในงานด้านการทหาร จะมีการเฝ้าระวังพื้นที่จากการรุกรานของฝ่ายตรงข้าม เมื่อมีการรุกรานเข้ามาก็ส่งข้อมูลกลับมาที่ส่วนกลางเพื่อรอคำสั่งในการจุดฉนวนระเบิดที่ต่ออยู่กับตัวโหนดเซนเซอร์ แต่ในการใช้งานด้านการทหารจะต้องคำนึงถึงการรักษาความปลอดภัยข้อมูลที่ถูกส่งภายในเครือข่ายเซนเซอร์ไร้สาย เพื่อป้องกันไม่ให้มีการปลอมแปลงข้อมูลที่ใช้ในการทำงานได้ ในงานด้านการสำรวจแหล่งทรัพยากรธรรมชาติ เช่นก๊าซ หรือน้ำมัน หรือทรัพยากรธรรมชาติอื่นๆ

2.2.2 การเฝ้าระวังสิ่งแวดล้อม และการเปลี่ยนแปลงของโลก

การเฝ้าระวังสิ่งแวดล้อม และการเปลี่ยนแปลงของโลก เช่น การตรวจจับการเกิดภูเขาไฟระเบิด ตรวจจับกระแส น้ำ อุณหภูมิ น้ำในมหาสมุทร การติดตามการเจริญเติบโตของสัตว์หรือ ต้นไม้ในป่า การเคลื่อนที่ของธารน้ำแข็ง ในการเฝ้าระวังสิ่งแวดล้อม และการเปลี่ยนแปลงของโลก นั้น ทำให้นักวิทยาศาสตร์ สามารถเก็บข้อมูลตัวอย่างที่ต้องการใช้ในงานวิจัยโดยข้อมูลที่ได้เป็นข้อมูลแบบต่อเนื่องทางเวลา ทำให้สามารถนำข้อมูลเหล่านั้นมาใช้ในการประกอบการตัดสินใจต่างๆ ได้ อีกทั้งยังประหยัดงบประมาณในการเดินทางเพื่อเข้าไปเก็บข้อมูลในพื้นที่ห่างไกล และมีความยากลำบากในการเข้าถึง

2.2.3 การเฝ้าระวังคุณภาพของอากาศ

เนื่องจากมลพิษทางอากาศเริ่มมีปริมาณมากขึ้นในปัจจุบัน จึงต้องมีการตรวจวัดกันเป็นประจำ เพื่อปกป้องประชากรและสิ่งแวดล้อมอื่นๆ อันเนื่องมาจากมลพิษทางอากาศ ซึ่งเป็นภัยอันตรายที่อยู่รอบๆ ตัวเรา ดังนั้นการเฝ้าระวังแบบตลอด (Real time monitoring) นั้นมีความสำคัญมาก เนื่องจากสภาวะอากาศมีการเปลี่ยนแปลงที่รวดเร็วมาก

2.2.4 การเฝ้าระวังมลพิษทางอากาศ

ปัจจุบัน WSN มีการติดตั้งใช้งานในหลายๆ เมืองเช่น ลอนดอน เพื่อเฝ้าระวังแก๊สที่เป็นอันตรายต่อพลเมืองของเขา โหนดเซนเซอร์เหล่านี้ใช้ประโยชน์จากเครือข่ายไร้สาย แทนที่จะเป็นแบบสาย เนื่องจากสามารถเคลื่อนที่ไปเฝ้าระวังในจุดต่างๆ ได้

นอกจากการประยุกต์ใช้งาน WSN ที่ได้กล่าวและยกตัวอย่างมาแล้ว ยังมีการใช้งานอื่นๆ อีกเช่น การเฝ้าระวังการเคลื่อนที่ของหน้าดิน (Landslide detection) การเฝ้าระวังคุณภาพของน้ำ (Water quality monitoring) การเฝ้าระวังภัยพิบัติทางธรรมชาติ (Natural disaster prevention) การเฝ้าระวังในภาคอุตสาหกรรม (Industrial monitoring) การเก็บข้อมูลต่าง (Data logging) การติดตามการทำงานของเครื่องจักร (Machine health monitoring) การเฝ้าระวังน้ำเสีย (Waste water monitoring) การเฝ้าระวังในภาคเกษตรกรรม (Agriculture monitoring) การเฝ้าระวังในบ้าน (Smart home monitoring) จะเห็นได้ว่า WSN เริ่มเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น จึงได้มีการศึกษาและพัฒนาขีดความสามารถของ WSN ให้สูงขึ้น เพื่อตอบสนองต่อความต้องการที่มากขึ้น

2.3 คุณลักษณะของ WSN

- 1) โหนดต่างๆ ในเครือข่ายจะใช้พลังงานจากแบตเตอรี่ หรือจากการผลิตขึ้นมาด้วยตัวเอง
- 2) มีการใช้ MAC ที่เน้นเรื่องการประหยัดพลังงาน
- 3) เครือข่ายยังสามารถทำงานได้เมื่อมีบางโหนดเสียหาย
- 4) โหนดจะต้องสามารถเคลื่อนย้ายได้
- 5) แต่ละโหนดมีลักษณะการทำงานเป็นลำดับขั้น
- 6) เครือข่ายต้องรองรับการขยาย หรือเพิ่มจำนวนของโหนด
- 7) สามารถทนอยู่ได้ภายในสภาพแวดล้อมที่เลวร้าย
- 8) สามารถต่อกับเซนเซอร์ต่างๆ ได้
- 9) ง่ายต่อการใช้งาน

ตัวโหนดภายใน WSN เปรียบเสมือนเครื่องคอมพิวเตอร์ขนาดเล็กที่สามารถรับสัญญาณอินพุตและส่งสัญญาณเอาต์พุตผ่านทางอินเทอร์เน็ตต่างๆ โดยในการติดต่อสื่อสารนั้นจะใช้สัญญาณวิทยุ และติดต่อกับตัวเกตเวย์ เมื่อต้องการส่งข้อมูลออกนอกเครือข่าย

2.4 มาตรฐานและคุณสมบัติของ WSN

ใน WSN มีหลายสถาบันที่ช่วยกันพัฒนา ซึ่ง IEEE เป็นสถาบันที่มุ่งเน้นที่ชั้นที่ 1 กายภาพ (Physical layer) และชั้นที่ 2 ชั้นสื่อสารข้อมูล (Data link) ส่วน IETF จะมุ่งเน้นไปที่ชั้นที่ 3 ชั้นเครือข่าย (Network layer) และชั้นที่สูงกว่าขึ้นไป ตามการจัดเรียงใน OSI model

มาตรฐาน IEEE802.15.4 เป็นมาตรฐานที่เกี่ยวกับโครงสร้างของเครือข่ายสำหรับเครือข่ายเซนเซอร์ไร้สาย ตัวมาตรฐานเน้นไปที่ชั้นของกายภาพ (Physical layer) และชั้นเครือข่าย (MAC layer) สำหรับการประยุกต์ใช้งานเครือข่ายเซนเซอร์ไร้สายนั้น หลักในการออกแบบนั้นต้องการให้ตอบโจทย์เรื่องของการใช้พลังงานในการทำงานให้น้อยที่สุด ต้นทุนที่ต่ำ โหนดแต่ละโหนดครอบคลุมพื้นที่ขนาดเล็ก แต่มีการใช้เครือข่ายเมช (Mesh network) ในกรณีที่ต้องการติดต่อสื่อสารเป็นบริเวณกว้างและครอบคลุมโหนดจำนวนมาก โครงสร้างของเครือข่าย IEEE802.15.4 จะเริ่มจากลักษณะของเครือข่าย เช่น แบบดวงดาว โดยโหนดในเครือข่ายจะมีอยู่ 1 โหนด ที่จะคอยทำหน้าที่เป็นโหนดประสานงาน (Node Coordinator) ซึ่งจะทำหน้าที่ระบุช่องการสื่อสารที่ไม่ทับซ้อนกันเพื่อป้องกันการกวนกันของคลื่นความถี่ (Interference) โดยการสแกนหาระดับของพลังงานแต่ละช่องที่รับได้ ซึ่งตัวโหนดใดๆ ที่อยู่ในช่องสัญญาณเดียวกันกับตัวโหนดประสานงาน (Node Coordinator) และต้องการจะเชื่อมต่อ ก็จะมีการส่งสัญญาณแจ้งเตือนออกมา ร้องขอ (Beacon request) เพื่อขอเข้าร่วมเครือข่าย มีเพียงตัวโหนดประสานงาน (Node coordinator) เท่านั้นที่จะตอบสนองต่อการร้องขอนั้นๆ ซึ่งเรียกกระบวนการนี้ว่า แอสโซซิเอชัน (Association) และมี PAN Coordinator เป็นตัวประสานงาน ในการคุยกับตัวโหนดประสานงานอื่นๆ ที่อยู่ใน PAN เดียวกัน ในกรณีที่มี โหนดประสานงานมากกว่า 1 โหนด ซึ่งโหนด PAN Coordinator นอกจากการทำหน้าที่คอยประสานงานแล้ว ยังทำหน้าที่เป็นเกตเวย์ เพื่อเชื่อมต่อกับเครือข่ายอื่นๆ เพื่อให้่ายต่อการทำความเข้าใจในงานวิจัยนี้ จึงขอแทนตัวโหนด PAN Coordinator ว่า เกตเวย์โหนด ในมาตรฐาน IEEE802.15.4 นั้น เมื่อมีโหนดใดๆ เกาะกับตัวโหนด แล้ว โหนดเหล่านั้นสามารถที่จะกลายเป็นตัวโหนดเราเตอร์ (Node router) ได้ด้วยตัวเอง และสามารถยอมให้โหนดอื่นๆ เกาะกับตัวมันได้ต่อ ผลที่ได้คือทำให้เกิดการทำแอสโซซิเอชัน (Association) แบบหลายลำดับชั้น

โครงสร้างของเครือข่าย ZigBee นั้นจะประกอบไปด้วยโหนดต่างๆ จำนวนมากแต่สามารถแบ่งออกเป็นสองแบบหลักคือ โหนดที่มีฟังก์ชันการทำงานแบบเต็ม Full-function device (FFD) และโหนดที่ถูกตัดฟังก์ชันที่ไม่จำเป็นออก Reduced-function device (RFD) ซึ่งในเครือข่ายจะต้องประกอบไปด้วย FFD อย่างน้อย 1 ตัว เพื่อทำหน้าที่เป็น PAN coordinator ตัวโหนดที่เป็น FFD สามารถทำงานได้ 3 รูปแบบ ดังนี้

- 1) PAN coordinator node
- 2) Coordinator node
- 3) Device node

ตัวโหนดที่เป็น RFD จะถูกกำหนดเพื่อทำหน้าที่ในการติดต่อกับส่วนที่เป็นเซนเซอร์ และมีการทำงานที่ไม่ซับซ้อน ซึ่งบางทีจะถูกเรียกว่าโหนดสุดท้าย และต้องการที่จะส่งข้อมูลที่มีขนาดไม่มากนัก เนื่องจากต้องการประหยัดพลังงานที่ตัวเองให้มากที่สุด โหนด FFD สามารถที่จะคุยกับโหนด RFD หรือ FFD ใดๆ ก็ได้ทั้งหมดในเครือข่ายเดียวกัน แต่โหนด RFD จะคุยกับโหนด FFD ได้เท่านั้น ไม่สามารถคุยกับ RFD ด้วยกันได้ ในบางครั้งตัวโหนด FFD ก็สามารถที่จะทำหน้าที่เป็นโหนดเซนเซอร์เพื่อใช้ในการเก็บข้อมูลก็ได้ขึ้นอยู่กับการออกแบบตัวเครือข่าย

2.5 โครงสร้างเครือข่ายเซนเซอร์ไร้สาย ZigBee

โครงสร้างเครือข่ายของ ZigBee จะแบ่งเป็น 3 แบบ คือแบบดาว (Star topology) แบบจุดต่อจุด (Peer-to-peer topology) และแบบกลุ่มต้นไม้ (Cluster tree topology)

2.5.1 โครงสร้างแบบดาว (Star topology)

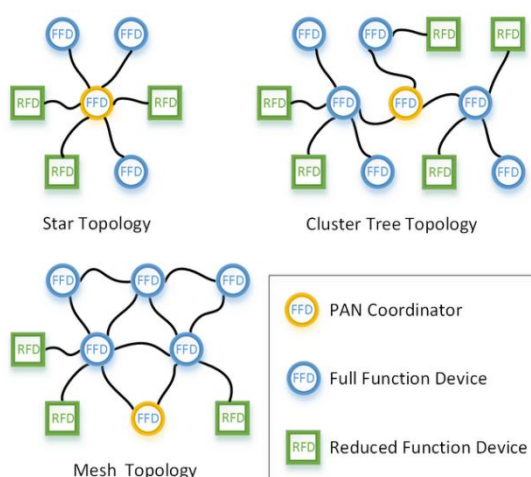
ในโครงสร้างแบบนี้การเริ่มการสื่อสารจะเริ่มขึ้นระหว่างโหนดโดยรอบกับโหนดควบคุมส่วนกลางหรือ (PAN coordinator) ตัวโหนดควบคุมส่วนกลางอาจจะจำเป็นต้องใช้พลังงานจากแหล่งพลังงานที่มากโหนดโดยรอบ เนื่องจากจะต้องติดต่อกับโหนดโดยรอบตลอดเวลา แต่โหนดโดยรอบอาจจะใช้เพียงแค่แบตเตอรี่อย่างเดียว การประยุกต์ใช้งานจากประโยชน์ที่ได้จากโครงสร้างแบบดาว คือการควบคุมระบบอัตโนมัติภายในครัวเรือน การทำงานของเครือข่ายเกิดขึ้นหลังจากโหนด FFD เริ่มต้นทำงานในครั้งแรก ตัวโหนด FFD ตัวนี้อาจจะทำหน้าที่เป็นโหนดควบคุมส่วนกลาง (PAN coordinator) ในแต่ละเครือข่ายดาว (Star Network) จะมีหมายเลขกำกับหรือ (PAN ID) ซึ่งจะไม่ซ้ำกับเครือข่ายอื่นๆ ภายในช่องสัญญาณสื่อสารเดียวกัน ซึ่งเป็นการทำให้เครือข่ายนี้ทำงานโดยอิสระกับเครือข่ายอื่นๆ

2.5.2 โครงสร้างแบบจุดต่อจุด (Peer-to-peer topology) หรือแบบตาข่าย (Mesh topology)

ในโครงสร้างแบบนี้ก็เช่นเดียวกับโครงสร้างแบบดาว คือ จะมีโหนดควบคุมส่วนกลาง (PAN coordinator) เพียงโหนดเดียวเท่านั้นในเครือข่าย แต่ตัวโหนดต่างๆ สามารถสื่อสารกับโหนดใดๆ ก็ได้เท่าที่อยู่ในย่านที่สามารถติดต่อกันกันได้ โครงสร้างแบบนี้เป็นเหมือนการทำงานในลักษณะของ Ad-Hoc คือสามารถที่จะสร้างโครงข่ายขึ้นมาด้วยตัวเองและดูแลรักษาโครงข่ายได้ด้วยตัวเอง ตัวอย่างการใช้งานเครือข่ายแบบนี้ เช่น ในการควบคุมในอุตสาหกรรม การเฝ้าติดตาม การเคลื่อนที่ต่างๆ เนื่องจากระบบเหล่านี้สามารถใช้ประโยชน์จากคุณสมบัติของโครงสร้างแบบนี้ได้เป็นอย่างดี ในโครงสร้างแบบนี้จะยอมให้มีการสร้างเส้นทางจากโหนดใดๆ ผ่าน ฮอปจำนวนมากได้ (Multiple hop) เพื่อไปยังโหนดใดๆ ในเครือข่าย อีกทั้งยังสามารถให้เส้นทางที่มีเสถียรภาพจากการทำการหาเส้นทางแบบหลายเส้น (Multipath routing)

2.5.3 โครงสร้างแบบกลุ่มต้นไม้ (Cluster tree topology)

เป็นโครงสร้างที่มีลักษณะจำเพาะหนึ่งของโครงสร้างแบบจุดต่อจุด (peer-to-peer topology) ซึ่งมีโหนดจำนวนมากเป็น FFD และมีโหนด RFD เชื่อมต่อเข้ากับโหนดเหล่านี้ ซึ่งมีลักษณะคล้ายกลุ่มของต้นไม้ โดยมีกิ่งก้านเป็นโหนด FFD และโหนด RFD เหมือนกับใบไม้ ซึ่งเป็นจุดปลายสุดของกิ่งก้านเหล่านั้น โหนด FFD ทุกๆ สามารถทำหน้าที่เป็นตัวประสานงานและคอยให้บริการกับโหนดอื่นๆ ที่เป็น FFD และ RFD ซึ่งในโครงสร้างแบบนี้จะมีเพียงโหนดเดียวที่ทำหน้าที่เป็นตัวประสานงานเครือข่าย (PAN coordinator)



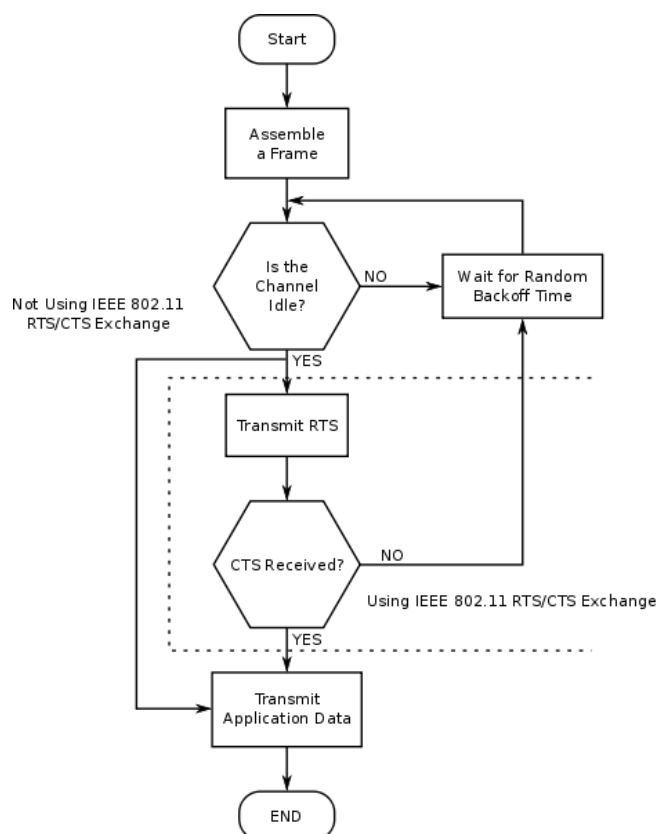
ภาพที่ 2.2 โครงสร้างเครือข่ายของ ZigBee

ที่มา: <http://www.pervcomconsulting.com/IEEE.html>

ตัวประสานงานเครือข่าย (PAN coordinator) ของกลุ่มแรกจะทำหน้าที่เป็นหัวหน้ากลุ่ม CLH และกำหนดตัวหมายเลขประจำกลุ่ม CL ID เป็น “0” หรือเลือกจาก PAN Identifier ที่ไม่ได้ใช้ จากนั้นก็จะกระจายเฟรมสัญญาณเตือน (frames broadcasting beacon) ไปยังตัวโหนดข้างเคียง

2.6 โครงสร้าง Low Rate Wireless Personal Area Network (LR-WPAN)

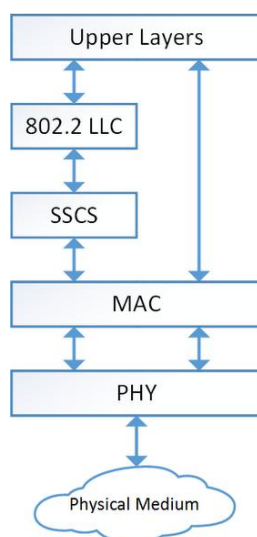
โครงสร้างของอุปกรณ์ที่เป็นแบบ LR-WPAN เนื่องจาก WSN มีจุดประสงค์หลักคือการส่งผ่านสัญญาณจากโหนดเซนเซอร์เพื่อมาประมวลผล โดยมีการส่งข้อมูลที่มีขนาดไม่ใหญ่มาก แต่จะเน้นที่การใช้พลังงานของตัวโหนดเซนเซอร์ให้น้อยที่สุด จึงต้องมีการออกแบบส่วนของ MAC เพื่อควบคุมการเข้าถึงสื่อกลางในการสื่อสารข้อมูล ระหว่างส่วนของ Upper Layers ไปยัง Physical Layers ในที่นี้คือคลื่นความถี่ โดยมีการใช้งานคลื่นความถี่ร่วมกันระหว่างโหนดเซนเซอร์ต่างๆ



ภาพที่ 2.3 กลไกการทำงาน CSMA/CA

ที่มา: http://en.wikipedia.org/wiki/File:Csma_ca.svg

ในกระบวนการติดต่อกับชั้นกายภาพของ WSN นั้นจะอาศัยกลไก ของ CSMA/CA ซึ่ง เป็นกระบวนการในการขอใช้ตัวกลางร่วมกัน และใช้กลไกของการตรวจจับว่าช่องสัญญาณว่างอยู่หรือไม่ ถ้าว่างก็จะมีการใช้ช่องสัญญาณนั้นๆ แต่ถ้าไม่ว่างก็จะจับเวลาถอยหลังเป็นเวลาเท่ากับ Backoff time จึงเริ่มทำการขอใช้ช่องสัญญาณใหม่



ภาพที่ 2.4 โครงสร้างของ LR-WPAN

ที่มา: <http://zigbeevsmbus.blogspot.com/2012/06/fossil-energy-crisis-havealways-lead-to.html>

โดยจะมีกลไกของตัว MAC เป็นตัวควบคุมการทำงานของตัวโหนด ว่าต้องการให้ตื่นหรือหลับ เมื่อไร โดยเน้นไปที่การใช้พลังงานให้ต่ำที่สุด เพื่อให้โหนดเซนเซอร์อยู่ได้นานที่สุด การทำงานของ MAC จะใช้การปรับเรื่องของค่า Duty Cycles โดยถ้าช่วงเวลาในการหลับมีมากกว่าช่วงเวลาตื่นมากๆ ก็จะทำให้ประหยัดพลังงานในการส่งข้อมูลได้ แต่ก็ต้องระวังเรื่องของช่วงเวลาในการตื่นเพื่อส่งข้อมูลนั้น จะต้องทำให้พร้อมกันกับตัว FFD ถ้าไม่ตรงอาจทำให้เกิดการส่งข้อมูลผิดพลาด หรือไม่ได้ส่งเลยก็ได้

2.7 พลังงานที่ใช้ใน WSN

ใน WSN สิ่งที่สำคัญคือเรื่องพลังงาน ในการทำงานของโหนดแต่ละโหนดนั้น จะต้องมีการใช้พลังงานไปในการทำงาน โดยรูปแบบของพลังงานที่ถูกใช้ไปใน WSN นั้น สามารถแบ่งได้เป็นได้เป็น 2 แบบ คือ

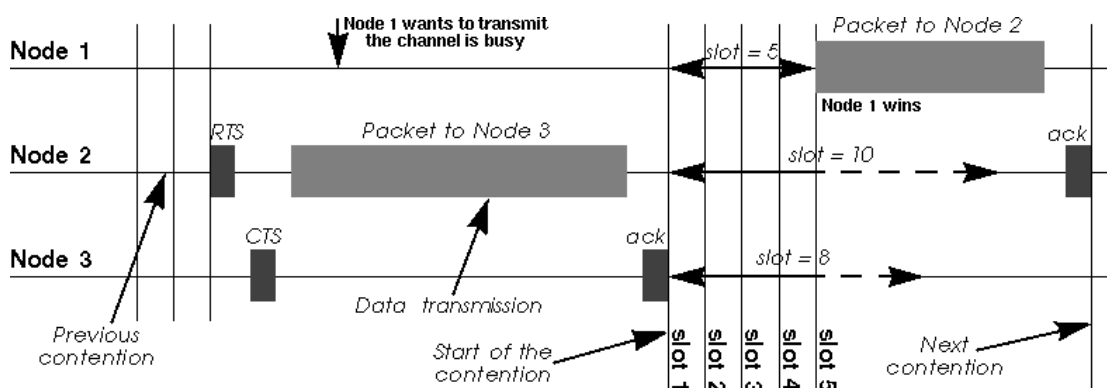
1) พลังงานที่ต้องใช้ (Useful power consumption) เป็นความต้องการใช้พลังงานสำหรับการส่ง หรือรับข้อมูล กระบวนการร้องขอการส่งข้อมูล การส่งต่อกระบวนการร้องขอต่างๆ หรือการส่งข้อมูลไปยังโหนดข้างเคียง (Node Neighbors)

2) พลังงานสูญเสีย (Wasteful power consumption) เป็นพลังงานที่สูญเสียไปจากกระบวนการต่างๆ เช่น การรอช่องสัญญาณว่าง เพื่อจะส่งข้อมูล การส่งข้อมูลใหม่ ในกรณีที่ข้อมูลเดิมที่ถูกส่งมีการชนกันของข้อมูล กระบวนการที่เซนเซอร์ได้รับแพ็คเกจที่ไม่ใช่ของมัน

2.8 กระบวนการเข้าถึงช่องสัญญาณสื่อสารใน WSN

ใน WSN กระบวนการหรือกลไก ที่ตัวโหนดต่างๆ จะเข้าถึงช่องสัญญาณสื่อสาร หรือสื่อกลางที่ใช้ในการสื่อสารร่วมกันนั้น ล้วนแล้วแต่เป็นกระบวนการที่เกิดขึ้นในส่วนของ MAC ซึ่งสามารถแบ่งออกเป็นกลุ่มต่างๆ ได้ 3 วิธีการ คือ

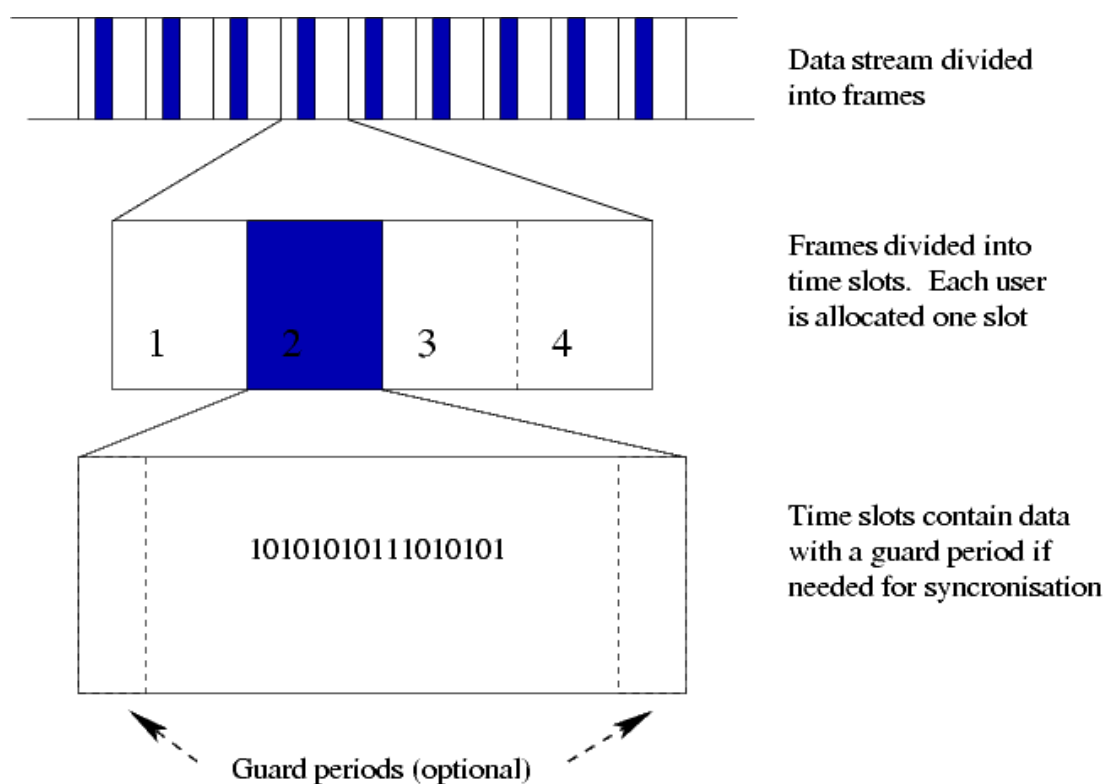
1) CSMA เป็นรูปแบบการเข้าถึงสื่อกลางแบบแย่งชิง (Contention based) คือจะไม่มี การจองสื่อกลางไว้ เหมือนแบบ TDMA ทำให้มีการใช้งานสื่อกลางได้อย่างมีประสิทธิภาพ แต่จะมีการเกิดการแข่งขันเวลาบ้างในกรณีที่สื่อกลางมีการใช้หนาแน่น ตัวอย่างรูปแบบของ MAC ที่ทำงานในลักษณะนี้ ได้แก่ S-MAC, T-MAC, PCS-MAC, B-MAC, Wise-MAC, D-MAC, U-MAC, X-MAC, P-MAC, C-MAC, etc.



ภาพที่ 2.5 การเข้าถึงช่องสัญญาณของ CSMA/CA

ที่มา: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.mac.html

2) TDMA เป็นรูปแบบการเข้าถึงสื่อกลางแบบมีการจองช่วงเวลาไว้ก่อน (Time slot) หรือ (Reservation based) เมื่อต้องการส่งข้อมูลก็สามารถส่งได้เลย ทำให้มีประสิทธิภาพในการส่งข้อมูลสูง และเกิดการหน่วงเวลาในการรอการส่งน้อยเนื่องจากไม่ต้องแย่งสื่อกลางกัน ตัวอย่างรูปแบบของ MAC ที่ทำงานในลักษณะนี้ ได้แก่ ER-MAC, TRAMA, E-MACS, DE-MAC, BMA, SS-TDMA, L-MAC, etc.



ภาพที่ 2.6 โครงสร้างเฟรมของ TDMA

ที่มา: <http://en.wikipedia.org/wiki/File:Tdma-frame-structure.png>

3) Hybrid (CSMA/TDMA) เป็นรูปแบบการเข้าถึงสื่อกลาง โดยมีการประยุกต์เอาข้อดีของทั้ง CSMA และ TDMA เข้าด้วยกัน เช่นการปรับค่า Duty Cycle ในมีค่าเปลี่ยนแปลงตามความหนาแน่นของข้อมูล โดยการเพิ่มจำนวนช่องของ TDMA ตัวอย่างรูปแบบของ MAC ที่ทำงานในลักษณะนี้ ได้แก่ IEEE802.15.4, PTDMA, DEE-MAC, μ -MAC, SCP-MAC, R-MAC, A-MAC, SPARE-MAC, Y-MAC, Z-MAC, H-MAC, etc.

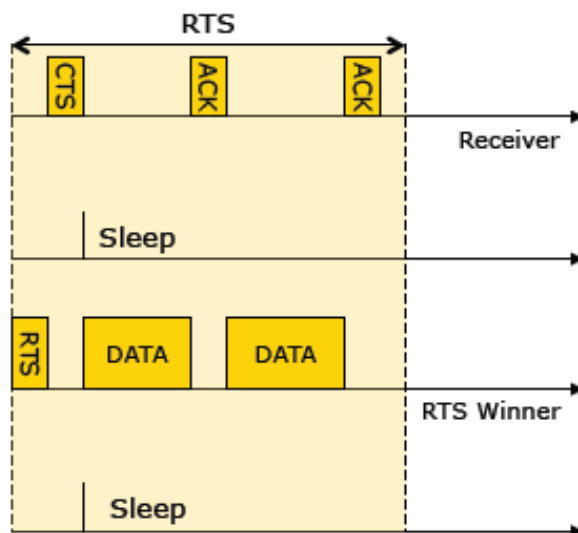
2.9 Media Access Control (MAC) ใน WSN

ใน WSN นั้น MAC มีความสำคัญ เนื่องจากการเลือกใช้ MAC ไม่เหมาะสมกับการใช้งาน ก็จะทำให้ไม่สามารถใช้งาน WSN ได้อย่างมีประสิทธิภาพ เพราะตัว MAC เป็นตัวแปรที่สำคัญที่จะทำให้โหนดต่างๆ ใน WSN สามารถประหยัดพลังงานในการส่งและรับข้อมูล (Energy efficiency) หรือมีประสิทธิภาพในแง่ของการส่งข้อมูลสำเร็จมากหรือน้อย (Throughput) การหลีกเลี่ยงการชนกันของข้อมูล (Collision avoidance) การเพิ่มจำนวนหรือลดจำนวนโหนดในเครือข่าย (Scalability) การหน่วงเวลาหรือการเข้าถึงข้อมูล (Delay and Latency) การใช้งานช่องสัญญาณอย่างมีประสิทธิภาพ (Bandwidth utilization) ดังนั้นส่วนใหญ่ MAC ต่างๆ ที่ใช้ใน WSN จะมุ่งเน้นไปในเรื่องของการ ประหยัดพลังงานในการส่งและรับข้อมูล โดยตัวอย่างการทำงานของ MAC แบบพื้นฐาน ที่ถูกใช้บ่อยใน WSN มีดังนี้

2.9.1 S-MAC

S-MAC เป็น MAC ที่มีการทำงานบนพื้นฐาน Contention based โดยจะมีช่วงเวลาหลับที่คงที่ (Regulates sleep periods) เพื่อประโยชน์ในเรื่องของการยืดอายุการใช้งานเครือข่ายเซนเซอร์ไร้สายให้นานขึ้น โดยอาศัยปัจจัย 4 อย่าง ในการบริหารจัดการพลังงาน

- 1) avoiding idle listening หลีกเลี่ยงการรับข้อมูลเข้ามา ในขณะที่ข้อมูลนั้นไม่ใช่ของตัวเอง
- 2) static sleep scheduling กำหนดช่วงเวลาในการหลับเป็นแบบคงที่
- 3) preamble sampling เมื่อตัวโหนดอยู่ในสถานะหลับ จะมีการตื่นขึ้นมาเป็นช่วงเวลานั้นๆ เพื่อคอยดูว่ามีโหนดใดส่งข้อมูลมาให้หรือไม่ ถ้าไม่มีก็จะหลับต่อ ในขณะที่ตื่นขึ้นมานั้น ถ้ามีโหนดใดส่งข้อมูลให้ ก็จะตื่นมารับข้อมูล
- 4) off-line scheduling จะทำงานเมื่อตัวโหนดอยู่ในสถานะหลับ โดยจะทำการปิดภาคส่ง และภาครับสัญญาณวิทยุ

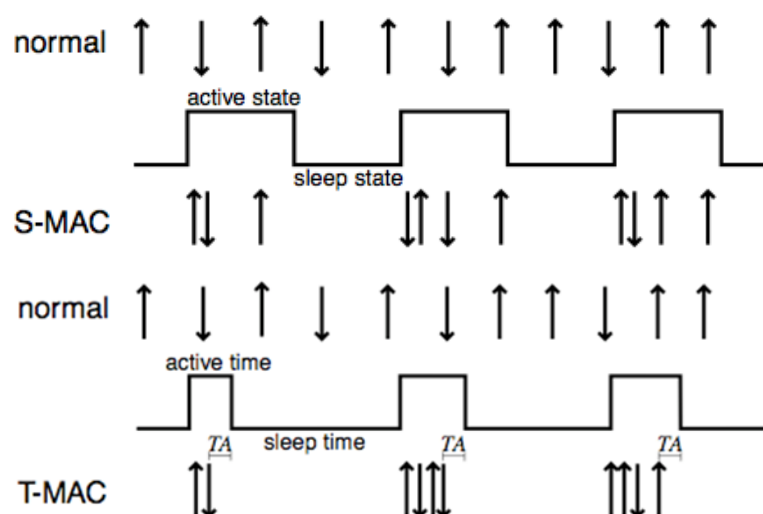


ภาพที่ 2.7 การทำงานของ S-MAC

ที่มา: http://www.cs.binghamton.edu/~kang/teaching/cs526/cs526_lect05_mac.ppt

2.9.2 T-MAC

T-MAC เป็น MAC ที่มีการทำงานบนพื้นฐาน Contention based โดยจะมีการทำงานคล้ายกับตัว S-MAC แต่จะมีการปรับเปลี่ยนวิธีการในการเข้าสู่โหมดการหลับ จากเดิมตัว S-MAC จะเป็นแบบ static sleep scheduling จะถูกปรับเปลี่ยนมาเป็น dynamic sleep scheduling โดยจะมีการปรับเปลี่ยนเวลาในการหลับ ตามปริมาณความหนาแน่นของการส่งและรับข้อมูล และให้ตัวจับเวลา TA เป็นตัวควบคุมการเข้าสู่โหมดหลับ เมื่อไม่การส่งหรือรับข้อมูลเป็นระยะเวลา $> TA$ ตัวโหนดนั้นก็จะเข้าสู่โหมดหลับ ทำให้เพิ่มเวลาในการหลับได้มากขึ้นและประหยัดพลังงานมากขึ้น จากภาพที่ 2.8 แสดงให้เห็นว่า ค่าเวลา TA ยิ่งน้อย ยิ่งทำให้เข้าสู่ Sleep mode เร็วขึ้น ทำให้ T-MAC ประหยัดพลังงานมากกว่า S-MAC



ภาพที่ 2.8 การเปรียบเทียบการทำงานของ S-MAC และ T-MAC

ที่มา: perso.ens-lyon.fr/eric.fleury/CPS/ART/Projet/MACPresentation.ppt

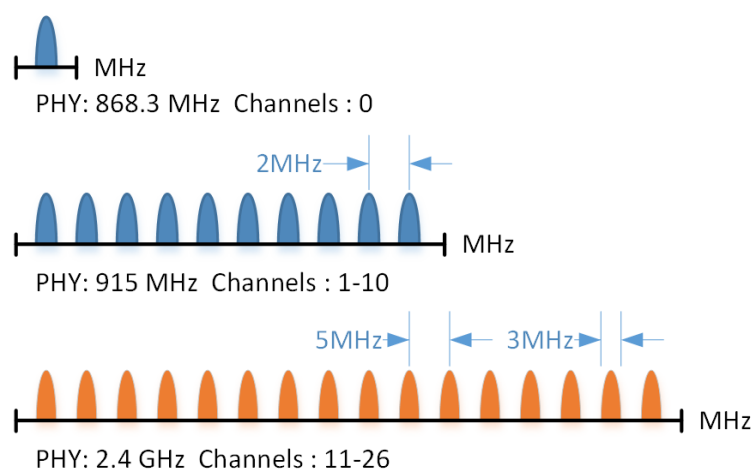
2.10 ย่านความถี่ที่ใช้งานใน IEEE802.15.4

ย่านความถี่และช่องสัญญาณข้อมูลที่ใช้ใน WSN จะมีอยู่ 3 ย่านความถี่ ซึ่งในแต่ละย่านความถี่ก็จะมีจำนวนช่องสัญญาณในการสื่อสารที่แตกต่างกัน

PHY (MHz)	Frequency Band (MHz)	Modulation	Channels	Channel spacing	Bit rate (kbps)	Symbol rate (ksymbol/s)	Symbols
868	868-868.6	BPSK	1	-	20	20	binary
868	868-868.6	ASK	1	-	250	12.5	20-bit PSSS
868	868-868.6	O-QPSK	1	-	100	25	16-ary orthogonal
915	902-928	BPSK	10	2MHz	40	40	binary
915	902-928	ASK	10	2MHz	250	50	5-bit PSSS
915	902-928	O-QPSK	10	2MHz	250	62.5	16-ary orthogonal
2450	2400-2483.5	O-QPSK	16	5MHz	250	62.5	16-ary orthogonal

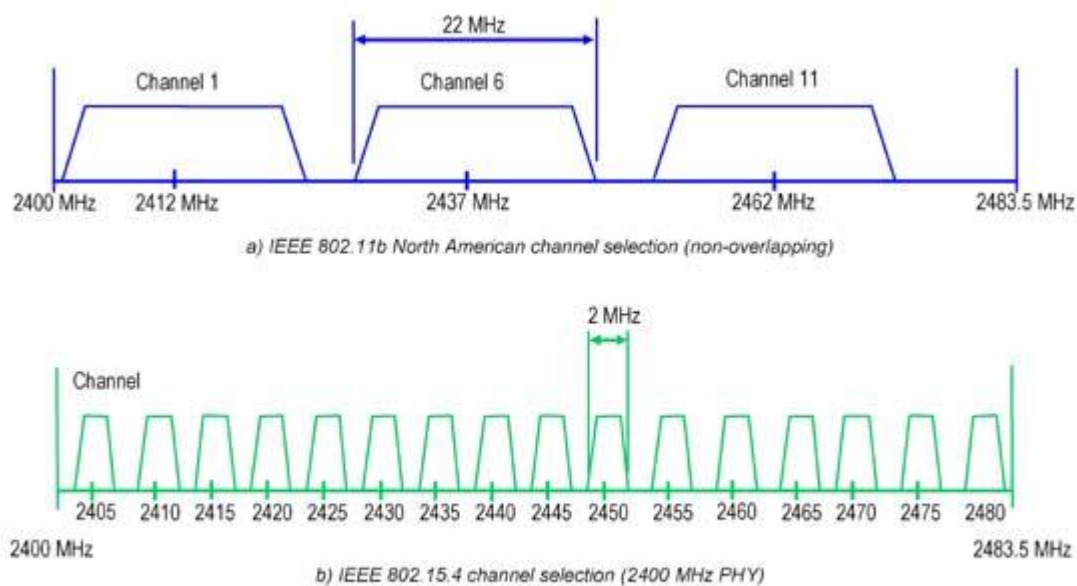
ภาพที่ 2.9 ค่าย่านความถี่ที่ใช้ใน IEEE802.15.4-2006

ที่มา: http://www.techonlineindia.com/techonline/design_centers/171033/introduction-wireless-sensor-network-concepts



ภาพที่ 2.10 ค่าความถี่มูลฐานของแต่ละช่องสัญญาณ

ที่มา: <http://thaieasyelec.com/article-wiki/basic-electronics/what-is-zigbee.html>



Source: IEEE 802.15.4 specification

ภาพที่ 2.11 ค่าความถี่ 2.4GHz ที่ทับซ้อนกันของ IEEE802.15.4 กับ IEEE802.11

ที่มา: http://www.eetasia.com/ART_8800550485_499488_NT_4a9289f5.HTM

จะเห็นได้ว่าในย่านความถี่ 2400MHz นั้นจะมีใช้ในส่วนของ IEEE802.15.4 กับ IEEE802.11b แต่มีส่วนของ Bandwidth ที่ต่างกัน ดังนั้นจึงอาจเกิดการกวนกันของสัญญาณได้

2.11 โพรโทคอลการค้นหาเส้นทางใน WSN

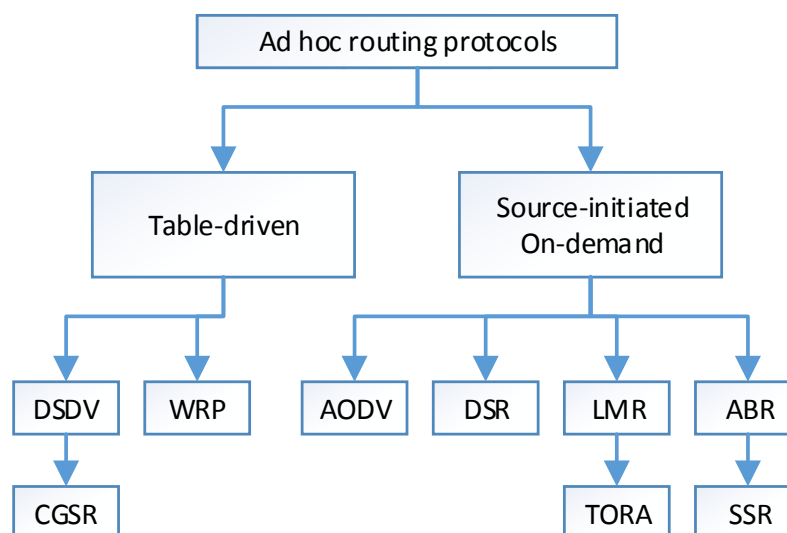
ใน WSN มีการเชื่อมกันแบบ Ad-Hoc mobile network ซึ่งเป็นวิธีการเชื่อมต่อเครือข่ายแบบหนึ่ง ในระบบการสื่อสารไร้สาย ที่โหนดนั้นมีการเคลื่อนที่อยู่ตลอดเวลา ดังนั้นเพื่อช่วยให้การติดต่อสื่อสารเป็นไปได้อย่างราบรื่นจึงได้มีการพัฒนาตัวโพรโทคอลในการค้นหาเส้นทาง ซึ่งถูกใช้ในการค้นหาเส้นทางระหว่างโหนดต้นทางไปยังโหนดปลายทาง ซึ่งเป้าหมายหลักของโพรโทคอลการค้นหาเส้นทางใน Ad-Hoc mobile network ก็เพื่อค้นหาเส้นทางที่ถูกต้องและมีประสิทธิภาพระหว่างคู่ของโหนดเพื่อให้ส่งข้อมูลไปยังเป้าหมายได้ตามเวลาที่เหมาะสม การสร้างเส้นทางนั้นควรจะทำให้เกิด Overhead และใช้ช่องสัญญาณ Bandwidth ให้น้อยที่สุด

ตั้งแต่โครงการวิจัย DARPA เกี่ยวกับเครือข่ายวิทยุแพ็คเกจ ในช่วงต้นปี 1970 มีโพรโทคอลจำนวนมากได้รับการพัฒนาเพื่อใช้งานบน Ad-Hoc mobile network หรือ MANET โพรโทคอลที่ถูกพัฒนาขึ้นมามีจุดประสงค์เพื่อจัดการกับข้อจำกัดต่างๆ เช่น การใช้พลังงานสูงในการทำงาน การได้ช่องสัญญาณที่ต่ำ และมีอัตราความผิดพลาดในการส่งข้อมูลที่สูง ซึ่งปัจจุบันโพรโทคอลการค้นหาเส้นทางที่ถูกออกแบบมาเพื่อใช้ใน Ad-Hoc mobile network สามารถแบ่งออกเป็น 3 กลุ่ม คือ

1) Table-driven protocols (Proactive) ประกอบไปด้วยโพรโทคอลที่ใช้วิธีการแบบ Distance Vector เช่น DSDV, WRP และ โพรโทคอลที่ใช้วิธีการแบบ Link State เช่น OLSR, GSR, TBRPF

2) Source-initiated or Demand-driven protocols (Reactive) ประกอบไปด้วยโพรโทคอลที่ใช้วิธีการแบบ Distance Vector เช่น AODV, ABR และ โพรโทคอลที่ใช้วิธีการแบบ Link State เช่น DSR

3) Hybrid protocols ประกอบไปด้วยโพรโทคอลต่างๆ เช่น ARPAM, ZRP, OORP



ภาพที่ 2.12 โพรโทคอลการค้นหาเส้นทางที่ใช้ในเครือข่ายเฉพาะกิจ

ที่มา: <http://www.eexploria.com/routing-protocols-in-manets/>

2.11.1 Table-driven protocols (Proactive)

Table-driven protocols (Proactive) เป็นโพรโทคอลประเภท Table-Driven เป็นโพรโทคอลที่จะพยายามรักษาและอัปเดตข้อมูลเส้นทางจากโหนดหนึ่งไปยังทุกๆ โหนดในเครือข่ายให้เป็นปัจจุบัน โพรโทคอลเหล่านี้จำเป็นต้องใช้ในแต่ละโหนดเพื่อรักษาตารางเส้นทาง หนึ่งหรือมากกว่าในการจัดเก็บข้อมูลเส้นทาง และโพรโทคอลเหล่านี้จะมีตอบสนองต่อการเปลี่ยนแปลงต่างๆ ในโครงสร้างของเครือข่ายโดยการปรับปรุงข้อมูลเส้นทางในตาราง โดยการกระจายไปให้ทั่วเครือข่าย เพื่อให้เครือข่ายยังคงมีตารางที่สอดคล้องกัน จำนวนโหนดที่มีจำนวนมากมีความเกี่ยวข้องกับขนาดของตารางเส้นทาง และมีความจำเป็นที่จะใช้วิธีการกระจายแบบ Broadcast เมื่อมีการเปลี่ยนแปลงของโครงสร้างของเครือข่าย

2.11.2 Source-initiated or Demand-driven protocols (Reactive)

Source-initiated or Demand-driven protocols (Reactive) เป็นโพรโทคอลประเภท Demand-Driven จะเริ่มทำการค้นหาเส้นทาง หรือจะสร้างเส้นทางก็ต่อเมื่อมีความต้องการที่จะส่งข้อมูลจากโหนดต้นทางเท่านั้น เมื่อโหนดต้นทางต้องการเส้นทางไปยังโหนดปลายทาง กระบวนการสำรวจเส้นทางจะเกิดขึ้นภายในเครือข่าย กระบวนการนี้จะเสร็จสิ้นก็ต่อเมื่อพบเส้นทางทั้งหมดที่เป็นไปได้และได้รับการตรวจสอบแล้ว เมื่อเส้นทางได้ถูกสร้างขึ้น เส้นทางจะถูกดูแลรักษาโดยกระบวนการซ่อมบำรุงเส้นทาง จนกระทั่งเส้นทางที่ไปยังปลายทางไม่สามารถเข้าถึง

ได้ทุกๆ เส้นทาง หรือจนกว่าเส้นทางนั้นจะไม่ใช่ที่ต้องการอีกต่อไป เส้นทางนั้นๆ ก็จะถูกกำจัดออกไป

2.12 โพรโทคอล AODV

โพรโทคอลการค้นหาเส้นทาง AODV เป็นโพรโทคอลแบบ Source Initiated On-Demand Driven/Reactive ซึ่งจะทำให้การค้นหาเส้นทางก็ต่อเมื่อจุดเริ่มต้นต้องการหาเส้นทางโดยหาเส้นทางไปจนถึงปลายทาง ซึ่งจะเป็นการค้นหาเส้นทางตามเส้นทางที่เป็นไปได้จนถึงปลายทางแล้ว จึงหยุดค้นหาหาเส้นทาง โพรโทคอล AODV ได้ปรับปรุงมาจาก DSDV เนื่องจากมีความคล้ายคลึงกันมาก แต่ AODV จะลดจำนวนครั้งในการที่จะค้นหาเส้นทางลง โดยจะทำการค้นหาเส้นทางเมื่อมีโนดที่ต้องการที่จะส่งข้อมูล หรือมีการเคลื่อนที่ของโนดเท่านั้น ทำให้ไม่เปลือง Bandwidth ในช่องสัญญาณ

โพรโทคอล AODV เป็นโพรโทคอลค้นหาเส้นทางตามมาตรฐาน RFC3561 ที่ถูกใช้งานกันอย่างแพร่หลายในเครือข่ายการสื่อสารเคลื่อนที่แบบไร้สาย ที่มีเป็นแบบ ad hoc ซึ่งจะตอบสนองต่อการเปลี่ยนแปลงเส้นทางที่เกิดขึ้นอยู่บ่อยๆ ได้อย่างรวดเร็ว กินทรัพยากรในการประมวลผล และหน่วยความจำน้อย รองรับการสร้างเส้นทางแบบหลายฮอป (Multi Hop) มีการกำหนดเส้นทางแบบ Unicast เพื่อไปยังปลายทาง และปรับปรุงเส้นทาง ภายในเครือข่ายเฉพาะกิจ โดยจะใช้ลำดับเลขหมาย (Destination sequence numbers) คอยกำกับเส้นทางไปยังปลายทาง เพื่อให้มั่นใจได้ว่าจะไม่เกิดลูปตลอดเวลาและหลีกเลี่ยงการเกิดปัญหาการนับลำดับหมายเลขจนถึงค่าอนันต์ โดยใช้หลักการแบบ distance vector ของ Bellman-Ford โพรโทคอล AODV จะพยายามหาโนดได้รับเส้นทางโดยเร็วที่สุดเมื่อมีการกำหนดโนดปลายทางใหม่ และจะไม่ใช้โนดที่ไม่ได้ทำงานอยู่เพื่อไปยังโนดปลายทาง โพรโทคอล AODV จะแจ้งให้โนดรับรู้ถึงการเชื่อมโยงที่ถูกตัดขาด และเมื่อมีการเปลี่ยนแปลงโครงสร้างของเครือข่าย เพื่อให้โนดนั้นยกเลิกการใช้เส้นทางที่ถูกตัดขาดไป คุณลักษณะเด่นของโพรโทคอล AODV คือการใช้งานของลำดับหมายเลขเพื่อไปยังโนดปลายทาง (Destination sequence numbers) สำหรับแต่ละเส้นทาง ซึ่งจะเป็นหมายเลขที่ไม่ซ้ำกัน และจะใส่ไปในแพ็คเกจข้อมูลที่ถูกส่งออกไป การใช้ลำดับหมายเลขปลายทางนี้จะเป็นวิธีการป้องกันการเกิดลูปในเครือข่าย และทำให้ง่ายต่อการเขียนโปรแกรม ในการเลือกเส้นทางไปยังโนดปลายทางระหว่างสองเส้นทางที่มีนั้น โหนดปลายทางจะเลือกเพียงหนึ่งลำดับหมายเลขเท่านั้น

2.12.1 ความหมายของคำศัพท์ในโพรโทคอล AODV

ในตัวโพรโทคอล AODV มีการกำหนดความหมายของชื่อเรียกในตัวโพรโทคอลไว้ดังนี้

1) Active route เป็นเส้นทางที่สามารถไปยังโหนดปลายทางได้ ซึ่งมีรายการอยู่ในตารางเส้นทาง และมีการทำเครื่องหมายไว้ว่าสามารถใช้งานได้ ซึ่ง Active route จะเป็นเส้นทางที่ใช้ส่งข้อมูลได้

2) Broadcast เป็นการกระจายข้อมูลไปยังที่อยู่ไอพีที่ถูกกำหนดเป็น Broadcast address สำหรับไอพีเวอร์ชัน 4 ใช้ 255.255.255.255 โดยการกระจายแพ็กเก็ตนั้นจะช่วยให้ AODV สามารถกระจายข้อมูลไปได้ทั่วทั้งเครือข่ายเฉพาะกิจ

3) Destination เป็นโหนดปลายทางที่ต้องการส่งข้อมูลแพ็กเก็ต โดยข้อมูลนี้จะแสดงในส่วน IP Header การสร้างเส้นทางไปยังโหนดปลายทางนี้จะทำโดยโพรโทคอล AODV

4) Forwarding node เป็นโหนดที่ยอมให้มีการส่งผ่านแพ็กเก็ตไปยังโหนดปลายทาง โดยการส่งต่อแพ็กเก็ตเหล่านั้นไปยังโหนดข้างเคียงโดยใช้ Unicast ซึ่งเส้นทางนี้จะถูกใช้งานโดย Routing control message

5) Forward route เป็นเส้นทางที่จัดตั้งขึ้นเพื่อส่งแพ็กเก็ตข้อมูลจากโหนดต้นทางไปสู่โหนดปลายทางที่ต้องการ ซึ่งเกิดขึ้นในกระบวนการสำรวจเส้นทาง

6) Invalid route เป็นเส้นทางใดๆ ที่หมดอายุ และมีการทำเครื่องหมายยกเลิกไว้ในตารางเส้นทางแล้ว จะถูกนำมาใช้ในการจัดเก็บข้อมูลเส้นทางที่ถูกต้องก่อนหน้านี้ เส้นทางที่ถูกยกเลิกจะไม่สามารถใช้เพื่อส่งต่อแพ็กเก็ตข้อมูลได้ แต่ก็สามารถให้ข้อมูลที่เป็นประโยชน์ในการซ่อมแซมเส้นทางและเป็นข้อมูลให้ RREQ Message ในอนาคต

7) Originating node เป็นโหนดที่เป็นจุดเริ่มต้นของกระบวนการสำรวจเส้นทางใน AODV Message และอาจจะมีการส่งต่อข้อความนี้ไปยังโหนดอื่นๆ ภายในเครือข่ายเฉพาะกิจ ตัวอย่างเช่น โหนดที่เป็นโหนดเริ่มต้นในกระบวนการสำรวจเส้นทาง และทำการกระจาย RREQ Message นั้นจะถูกเรียกว่า “Originating node of the RREQ message”

8) Reverse route เป็นเส้นทางที่ถูกกำหนดขึ้นเพื่อการส่งต่อ RREP แพ็กเก็ต กลับไปยังโหนดเริ่มต้น จากโหนดปลายทาง หรือโหนดระหว่างทางที่มีเส้นทางไปยังโหนดปลายทาง

9) Sequence number เป็นจำนวนตัวเลขที่เพิ่มขึ้นโดยแต่ละโหนดต้นทาง ซึ่งเป็นกระบวนการสร้างเส้นทางใน AODV RREQ message ซึ่งจะถูกใช้โดยโหนดอื่นๆ เพื่อตรวจสอบความเป็นปัจจุบันของข้อมูลที่มาจากโหนดต้นทาง

10) Valid route เป็นเส้นทางที่มีการทำเครื่องหมายไว้ว่าสามารถใช้ในการส่งแพ็กเก็ตได้

โพรโทคอลสร้างเส้นทาง AODV ถูกออกแบบมาเพื่อใช้ในเครือข่ายเฉพาะกิจ (ad hoc network) โดยรองรับโหนดได้ถึงหลักพัน และรองรับการเคลื่อนที่ของโหนดจำนวนมากในเครือข่ายได้ดี อีกทั้งยังสามารถรองรับรูปแบบการส่งข้อมูลที่มีหลายระดับได้ AODV ถูกออกแบบมาเพื่อลดการแพร่กระจายแพ็กเก็ตเกิดในการปรับปรุงเส้นทาง และลด overhead ของข้อมูล เพื่อปรับปรุงประสิทธิภาพ และขยายขนาดของเครือข่ายให้ดีขึ้น

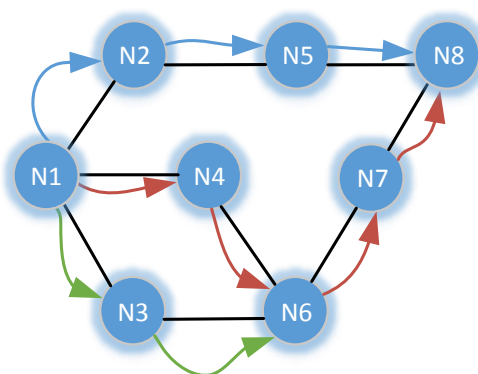
2.12.2 รูปแบบของข้อความ (Message Formats)

ในโพรโทคอลสร้างเส้นทาง AODV ได้มีการกำหนดรูปแบบของข้อความที่ส่งและรับระหว่างโหนดไว้ดังนี้

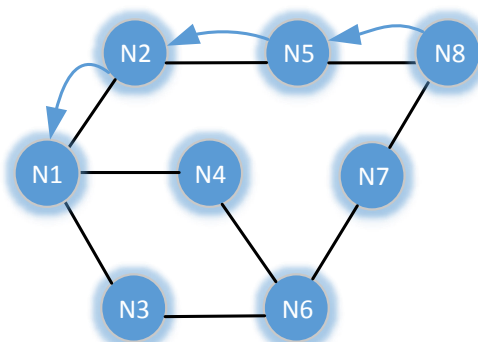
- 1) Route Request (RREQ) Message Format
- 2) Route Reply (RREP) Message Format
- 3) Route Error (RERR) Message Format
- 4) Route Reply Acknowledgment (RREP-ACK) Message Format

2.12.3 การทำงานของโพรโทคอล AODV

การทำงานของโพรโทคอล AODV จะเริ่มจากโหนดต้นทางมีการส่งร้องขอเส้นทาง (RREQ) มีการตอบ Route Reply (RREP) หรือ Route Error (RERR) สำหรับการสื่อสารแบบ Unicast ไปยังโหนดปลายทาง และเพื่อที่จะจัดการและประมวลผลข้อมูลเส้นทางเหล่านี้ได้ถูกต้อง จึงมีการจัดเก็บรักษข้อมูลไว้ในตารางเส้นทางที่ไปยังโหนดเป้าหมาย โดยปกติแล้วโพรโทคอล AODV จะใช้ UDP ในการส่งข้อมูลไปยังพอร์ต 654



ภาพที่ 2.13 กระบวนการค้นหาเส้นทางไปยังโหนดปลายทาง (RREQ)



ภาพที่ 2.14 การตอบข้อความกลับ (RREP) ไปยังโหนดต้นทาง

ในโพรโทคอล AODV จะประกอบไปด้วย Message Route Request (RREQ) Route Replies (RREP) และ Route Errors (RERR) ซึ่งเป็นการรับแบบ UDP และมีการใช้ IP header ยกตัวอย่าง การร้องขอจากโหนดจะถูกระบุ IP Address ที่เป็นต้นกำเนิดของ Messages สำหรับการ Broadcast Message นั้น จะใช้ IP address (255.255.255.255) โดยขนาดของการ Broadcast Message RREQ นั้น จะถูกแสดงและกำหนดเป็นค่า TTL ที่อยู่ในส่วนหัวของไอพี เมื่อมีโหนดเชื่อมต่อเข้ามา และไม่มีเส้นทางไปยังโหนดนั้น ถ้าต้องการไปยังโหนดปลายทางนั้น จะมีการ Broadcasts RREQ เพื่อค้นหาเส้นทางไปยังโหนดปลายทางนั้น เส้นทางจะถูกสร้างขึ้นเมื่อ RREQ Message ไปถึงยังโหนดปลายทางที่ระบุไว้ด้วยตัวเอง หรือโหนดระหว่างทางมีเส้นทางที่สามารถไปยังโหนดปลายทาง ถ้าเส้นทางใหม่เป็นเส้นทางที่ถูกต้องสามารถไปยังปลายทางที่อยู่ใน RREQ ได้และมีลำดับหมายเลข เส้นทางนี้จะเป็นเส้นทางที่ใช้สำหรับส่ง RREP กลับไปยังต้นทาง โดยการ Unicast แต่ละโหนดจะคอยเฝ้าติดตามสถานะของการเชื่อมโยงถัดไปยังโหนดที่ทำงานอยู่ เมื่อการเชื่อมโยงดังกล่าวขาดลง ในระหว่างการค้นหาเส้นทาง จะมี RERR message ถูกส่งออกไปเพื่อแจ้งเตือนโหนดต่างๆ ถึงการสูญเสียการเชื่อมโยงดังกล่าว RERR Message จะแสดงให้โหนดปลายทางเหล่านั้นที่อยู่ใน Subnets เดียวกันถึงการไม่สามารถใช้งานได้จากการเชื่อมโยงที่มีปัญหา ซึ่งกระบวนการนี้จะต้องเปิดใช้งาน กลไกการรายงาน ซึ่งในแต่ละโหนดจะเก็บ Precursor List ภายในรายการจะประกอบไปด้วย IP address ของโหนดข้างเคียง ที่เป็นโหนดเพื่อใช้เส้นทางนำไปสู่ปลายทาง ข้อมูลที่อยู่ในรายการนี้ส่วนใหญ่เกิดจากการประมวลผลในการสร้าง RREP message ซึ่งเป็นโหนดที่จะต้องผ่านไปยังโหนดต้นทาง โพรโทคอล AODV จะใช้ข้อมูลในการสร้างเส้นทางดังนี้

- 1) หมายเลขไอพีที่อยู่ปลายทาง Destination IP Address
- 2) หมายเลขลำดับปลายทาง Destination Sequence Number

3) เครื่องหมายแสดงหมายเลขลำดับปลายทางที่ใช้งานได้ Valid Destination Sequence Number flag

4) สถานะอื่นๆ Other state and routing flags (เช่น valid, invalid, repairable, being repaired)

5) อินเทอร์เฟซเครือข่าย Network Interface

6) จำนวนโหนด Hop Count (number of hops needed to reach destination)

7) รายการโหนดถัดไป Next Hop List of Precursors

8) อายุของแพ็กเก็ต Lifetime (expiration or deletion time of the route)

2.12.4 การดูแลรักษา Sequence Number

การจัดการหมายเลขลำดับเป็นสิ่งสำคัญเพื่อที่จะหลีกเลี่ยงการเกิดลูปในเส้นทาง เมื่อการเชื่อมโยงถูกตัดขาด ทำให้ไม่สามารถเข้าถึงโหนดได้ โหนดปลายทางไม่สามารถเข้าถึงการเชื่อมโยงในเครือข่ายได้ หรือเส้นทางถูกปิดการใช้งาน เมื่อเงื่อนไขเหล่านี้เกิดขึ้น เส้นทางนั้นก็จะถูกยกเลิกโดยการทำเครื่องหมายที่ลำดับหมายเลขในตารางเส้นทางไว้ โดยทุกๆ โหนดที่มีข้อมูลอยู่ในตารางเส้นทาง จะต้องต้องมีข้อมูลเกี่ยวกับ Sequence Number สำหรับไปยังหมายเลข IP address ของโหนดปลายทาง ซึ่ง Sequence Number นี้ถูกเรียกว่า destination sequence number โดยตัวเลขนี้จะถูกปรับปรุงอยู่เสมอเมื่อโหนดได้รับข้อมูล Sequence Number ใหม่จาก RREQ RREP หรือ RERR message ซึ่งเป็นรับข้อมูลเกี่ยวกับโหนดปลายทาง โดยโหนดปลายทางจะมีการเพิ่มค่า Sequence Number ของตัวเองใน 2 กรณี

1) เพิ่มทันทีก่อนที่โหนดเริ่มต้นจะค้นพบเส้นทาง มันจะทำการเพิ่มค่า Sequence Number ของตัวมันเอง เพื่อป้องกันไม่ให้เกิดความขัดแย้งกับ Sequence Number ที่สร้างขึ้นก่อนหน้านี้ ในขณะที่ส่งข้อมูลย้อนกลับไปสู่เส้นทางเริ่มต้นของโหนดเริ่มต้นที่กระจาย RREQ ออกมา

2) เพิ่มทันทีก่อนที่โหนดปลายทางจะส่ง RREP เพื่อตอบสนองต่อ RREQ โดยมันจะต้องปรับปรุงค่า Sequence Number ของมันให้เป็นค่าสูงสุดของหมายเลขปัจจุบันและ Destination sequence number ในแพ็กเก็ต RREQ

โหนดปลายทางสามารถเพิ่มค่าหมายเลขลำดับ โดยหมายเลขลำดับจะเป็นตัวเลขจำนวนเต็มขนาด 32 บิต ซึ่งมีค่าสูงสุดที่ 4294967295 เมื่อเพิ่มจนถึงค่านี้แล้วก็จะเริ่มต้นที่ศูนย์ใหม่ ในทางกลับกันถ้าคิดเป็นจำนวนเต็มแบบมีเครื่องหมายค่าจะเริ่มตั้งแต่ -2147483648 ถึง 2147483647 และเพื่อเป็นการตรวจสอบให้แน่ใจว่าข้อมูลเกี่ยวกับโหนดปลายทางไม่เป็นข้อมูลเดิมที่ค้างอยู่ โหนดจะทำการเปรียบเทียบค่าเลขหมายลำดับปัจจุบันของมันกับค่าเลขหมายลำดับที่ได้รับมาใหม่จาก AODV Message ในการเปรียบเทียบนี้จะต้องทำการเปรียบเทียบทางคณิตศาสตร์แบบคิด

เครื่องหมายขนาด 32 บิต ถ้าผลลัพธ์ของการลบหมายเลขลำดับระหว่างหมายเลขเดิมกับหมายเลขใหม่มีค่าน้อยกว่าศูนย์ หมายความว่าข้อมูลของโหนดใหม่ที่ส่งเข้าเก่ากว่าข้อมูลเดิมที่เก็บอยู่ในโหนด

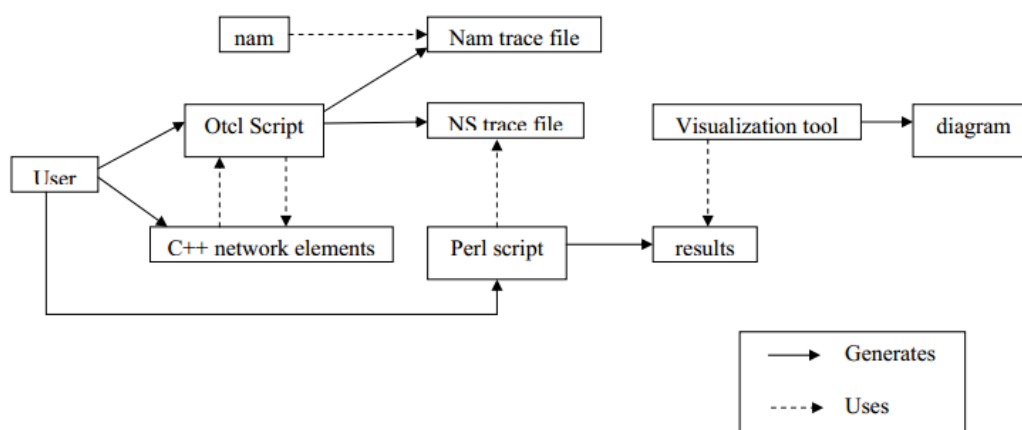
กรณีที่เส้นทางที่เชื่อมต่อระหว่างโหนดไปยังโหนดที่สามารถเชื่อมไปยังโหนดปลายทางได้มีการชำรุดหรือขาดลง โหนดนั้นอาจมีการเปลี่ยนแปลงค่าหมายเลขลำดับ โดยในกรณีนี้จะทำการเพิ่มค่าหมายเลขลำดับที่ไปยังโหนดปลายทางนี้ และทำการทำเครื่องหมาย “Invalid” เพื่อยกเลิกเส้นทางนี้ แต่เมื่อไรที่มีการรับข้อมูลใหม่เข้ามาและค่าหมายเลขลำดับน้อยกว่าหรือเท่ากับหมายเลขลำดับที่ถูกลบทิ้งไว้ นั่นหมายความว่าโหนดนั้นสมควรจะได้รับการปรับปรุง โหนดอาจจะมีการเปลี่ยนหมายเลขลำดับในตารางเส้นทางของโหนดปลายทางถ้าอยู่ในเงื่อนไขดังนี้

- 1) ถ้าโหนดนั้นเป็นโหนดปลายทางเอง และต้องการให้เส้นทางใหม่มายังตัวมัน
- 2) ถ้าได้รับ AODV message ที่เป็นข้อมูลใหม่เกี่ยวกับหมายเลขลำดับของโหนดปลายทาง
- 3) ถ้าได้รับ AODV message ที่เป็นข้อมูลว่าเส้นทางไปยังโหนดปลายทางนั้นชำรุดหรือเสียหาย

2.13 โปรแกรมจำลองการทำงานของเครือข่าย NS2

โปรแกรมการจำลองการทำงานของระบบเครือข่ายที่มีชื่อว่า NS2 เป็น discrete event simulator โดย NS2 ซึ่งสนับสนุนการทำงานแบบจำลองการทำงานของ UDP, TCP, Routing, Multicast protocols over wired และ wireless (local และ satellite) networks จากคุณสมบัติเหล่านี้เราสามารถจำลองการทำงานของเครือข่ายได้

NS2 มีภาษาที่ใช้อยู่ 2 ภาษาคือ ภาษา C++ และ Tcl โดย NS2 เป็น Open Source และสามารถที่จะทำงานได้ทั้งบน Linux , FreeBSD, SunOS, Solaris, Window ถูกพัฒนาขึ้นโดย ISI ซึ่ง NS2 เป็นโปรแกรมที่ใช้ในการจำลองการทำงานของ network ในแบบที่เป็น Discrete event simulator ซึ่งสนับสนุนการจำลองการเลือกเส้นทางในการขนส่ง packet สามารถจำลองการทำงานของ multicast protocol และ IP protocol เช่น UDP, TCP, RTP, SRM ที่อยู่บนเครือข่ายประเภทที่เป็น Wire และ Wireless (Local และ Satellite) ซึ่ง NS2 เป็นเครื่องมือที่มีประโยชน์มากทั้งยังสนับสนุน multiple protocol และยังสามารถในการแสดงรายละเอียดของ Network traffic ออกมาในรูปแบบของภาพเคลื่อนไหว รวมทั้งยังสนับสนุนขั้นตอนวิธีในการจัดเส้นทาง และ Queuing เช่น FIFO, Round-robin เป็นต้น



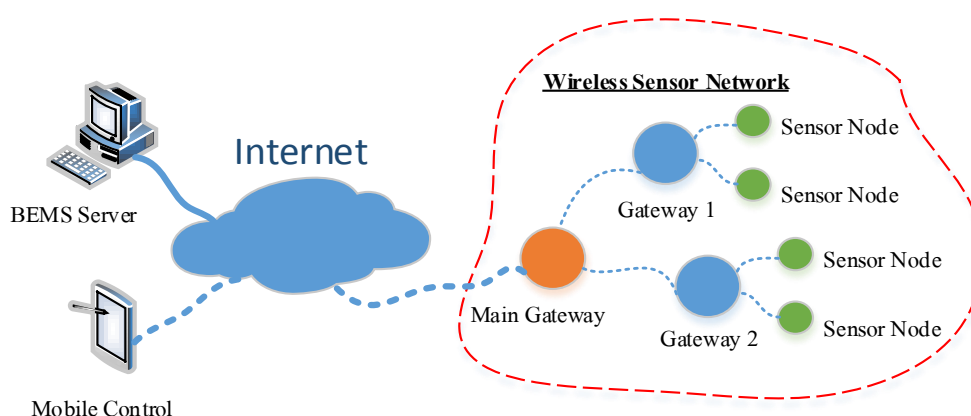
ภาพที่ 2.15 การทำงานของผู้ใช้งานผ่านโปรแกรม NS2

ที่มา: <http://wiki.nectec.or.th/ngiwiki/pub/Project/IntelligentNMS/bm-ns2.pdf>

2.14 งานวิจัยที่เกี่ยวข้อง

2.14.1 งานวิจัยเรื่อง Efficient Multiple Gateway System for WSN Management in BEMS
 จากงานวิจัยของ Xuan He, Yuanchen Ma และ Mika Mizutani

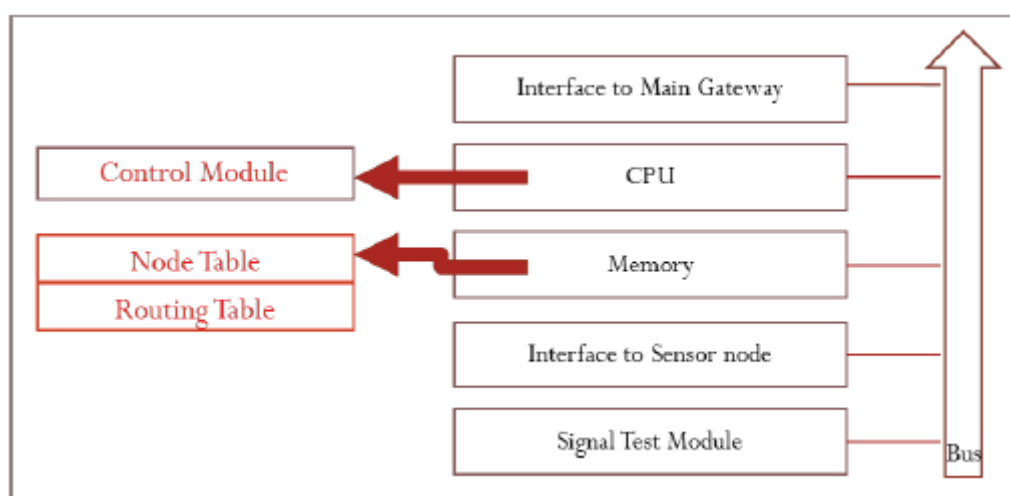
เป็นงานวิจัยเกี่ยวกับการใช้ระบบหลายเกตเวย์ ในเครือข่ายเซนเซอร์ไร้สาย เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการพลังงานในอาคาร BEMS โดยมีการออกแบบไว้ให้มีสถาปัตยกรรมที่มีเกตเวย์หลักอยู่หนึ่งตัว โดยเชื่อมต่อกับกับเครื่องแม่ข่าย BEMS และรวบรวมข้อมูลจากเทอร์มินอลเกตเวย์ตัวอื่นๆ ที่ต่อกับโหนดเซนเซอร์



ภาพที่ 2.16 โครงสร้างของ Multiple Gateway System

ที่มา: Xuan He and Yuanchen Ma, “Efficient Multiple Gateway System for WSN Management in BEMS” Networked Sensing Systems (INSS), Belgium, June 2012.

ในกรณีที่ตัวเทอร์มินอลเกตเวย์ในระบบตัวใดตัวหนึ่งมีปัญหาตัวโหนดเซนเซอร์ที่ต่ออยู่กับเทอร์มินอลเกตเวย์ตัวนั้น ก็จะหาเส้นทางไปยังเทอร์มินอลเกตเวย์ตัวอื่นๆ ที่ยังทำงานอยู่ แล้วจึงส่งต่อข้อมูลออกไปยังเกตเวย์หลัก เพื่อส่งต่อไปยังเครื่องม้าย BEMS อีกที ตัวเทอร์มินอลเกตเวย์ในสถาปัตยกรรมนี้จะแตกต่างกับตัวเกตเวย์ปกติทั่วไป ตรงที่จะต้องให้ตัวโมดูลควบคุมและคอยส่งสัญญาณ ไปทดสอบแต่ละเกตเวย์ว่ายังทำงานอยู่หรือไม่ ซึ่งการส่งสัญญาณนี้ จะเป็นการกินทรัพยากรด้านช่องสัญญาณในเครือข่าย



ภาพที่ 2.17 โครงสร้างของ Terminal Gateway

ที่มา: Xuan He and Yuanchen Ma, “Efficient Multiple Gateway System for WSN Management in BEMS” Networked Sensing Systems (INSS), Belgium, June 2012.

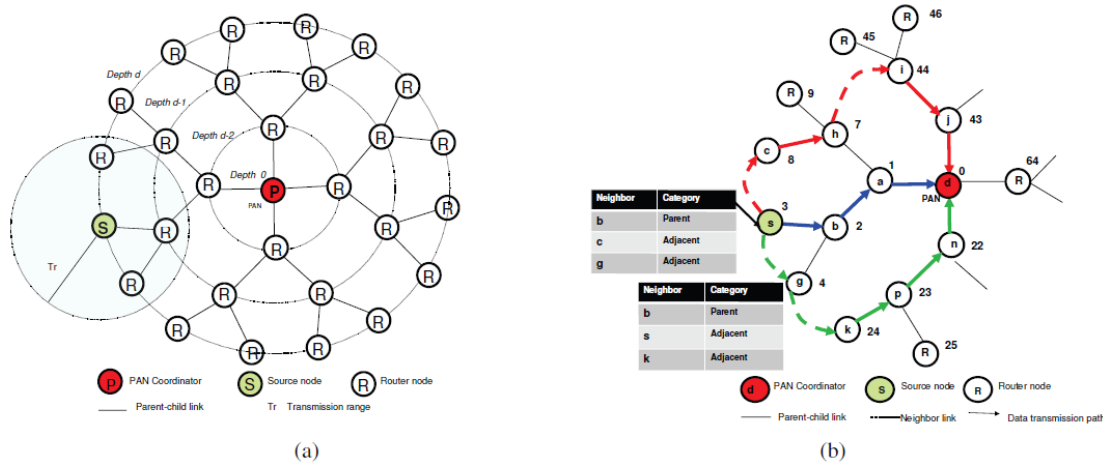
จากสถาปัตยกรรมแบบนี้ตัวกระบวนการหลัก (Main process) จะเริ่มต้นการทำงานโดยการสร้างตารางเส้นทางโดยมีเส้นทางทั้งหมดของเกตเวย์ข้างเคียง โดยตารางเส้นทางนี้จะมีพารามิเตอร์ของการหน่วงเวลา (delay time) การใช้พลังงาน (Power consumption) และสถานะของเส้นทาง ค่าการหน่วงเวลาจะหาจากขนาดของหน่วยความจำและสถานะของเส้นทาง ส่วนค่าการใช้พลังงาน จะคำนวณจากระยะทางของเกตเวย์ข้างเคียง หลังจากคำนวณทุกอย่างเสร็จแล้วเส้นทางที่ดีที่สุดจะถูกเลือก ซึ่งเป็นเส้นทางที่ประหยัดพลังงานและมีการหน่วงเวลาน้อยที่สุด ตัวสถานะของเส้นทางจะถูกระบุเป็น “ON” นอกนั้นจะระบุเป็น “OFF” ซึ่งตัวตารางเส้นทางนี้จะถูกปรับปรุงอยู่เป็นประจำ เมื่อเส้นทางที่ดีที่สุดขาด เส้นทางที่สองจะถูกเลือกขึ้นมาใช้แทน ตัวเกตเวย์หลัก จะทำ

หน้าที่เป็นเหมือนสะพานเพื่อเชื่อมระหว่างเครือข่ายเซนเซอร์ไร้สายกับเครือข่ายอินเทอร์เน็ต โดยจะรับข้อมูลจากเทอร์มินอลเกตเวย์ นอกจากนั้นยังทำหน้าที่ในการรับคำสั่งจากตัวผู้ใช้งานเพื่อส่งไปยังเทอร์มินอลเกตเวย์และโหนดเซนเซอร์ปลายทางที่ต้องการ ในงานวิจัยนี้ได้ประโยชน์ในการช่วยให้ตัวเซนเซอร์โหนดสามารถหาทางออกไปยังเกตเวย์หลักได้ง่ายขึ้นเนื่องจากมีหลายเกตเวย์ และใช้ตัวแปรเวลากับพลังงาน มาเป็นส่วนหนึ่งในการเลือกเส้นทางที่ดีที่สุด ซึ่งการใช้วิธีนี้สามารถที่จะลดเรื่องของการหน่วงเวลาและการใช้พลังงานได้ทั้งคู่

ในส่วนของงานวิจัยนี้ จะมีปัญหาอยู่ตรงส่วนที่เป็นตัวเกตเวย์หลัก เนื่องจากมีแค่เพียงตัวเดียว ดังนั้นถ้าเกตเวย์ตัวนี้มีปัญหา SPOF ก็จะทำให้เครือข่ายเซนเซอร์ไร้สายไม่สามารถติดต่อกับเครือข่ายอินเทอร์เน็ตได้ นั่นหมายความว่าเครือข่ายเซนเซอร์ไร้สายจะไม่สามารถส่งข้อมูลไปเก็บบน BEMS เครื่องแม่ข่ายได้

2.14.2 งานวิจัยเรื่อง Node disjoint multi-path routing for ZigBee cluster-tree Wireless Sensor Network จากงานวิจัยของ Zahia Bidai, Hafid Haffaf และ Moufida Maimour

เป็นงานวิจัยที่เกี่ยวกับการส่งข้อมูลในเครือข่ายเซนเซอร์ไร้สายแบบหลายเส้นทาง เนื่องจาก ZigBee เป็นเครือข่ายแบบ Ad-hoc ที่มีรากฐานการพัฒนามาจากมาตรฐาน IEEE802.15.4 ซึ่งมุ่งเน้นไปที่ชั้นกายภาพ (Physical layers) และชั้นการเชื่อมโยงข้อมูล (MAC layers) โดยมุ่งเน้นการใช้งานสำหรับงานที่ต้องการส่งผ่านข้อมูลที่มีขนาดต่ำ (Low data rate) และใช้พลังงานในการทำงานที่น้อย จากคุณลักษณะนี้ตัว ZigBee จึงถูกคาดหวังในการใช้งานเป็นเครือข่ายเซนเซอร์ไร้สายในอุตสาหกรรมเพื่อคอยวัดและควบคุมงานต่างๆ ดังนั้นการใช้งานที่ต้องการส่งผ่านข้อมูลที่มีขนาดสูง (High data rate) ผ่านเครือข่ายนี้ เช่น การส่งผ่านข้อมูลภาพเคลื่อนไหว จึงเป็นสิ่งที่น่าสนใจ จากงานวิจัยนี้ พวกเขาได้นำเสนอวิธีการที่จะส่งผ่านข้อมูลที่มีขนาดสูง (High data rate) ผ่านเครือข่ายนี้โดยใช้วิธีการส่งแบบหลายเส้นทาง โดยมีการจำลองการส่งข้อมูลจากต้นทางไปยังปลายทาง โดยใช้โปรโตคอล Z-MHTR ซึ่งเป็นโปรโตคอลที่สร้างขึ้นเพื่อใช้งานในการสร้างเส้นทางแบบหลายเส้นทางในการส่งข้อมูลบนเครือข่ายรูปแบบกลุ่มต้นไม้ (Cluster tree network) และทำการเปรียบเทียบกับโปรโตคอล AODV (Table driven or On-Demand) ซึ่งเป็นการสร้างเส้นทางแบบ Single-Path โดยใช้โปรแกรมจำลองการทำงานเครือข่าย NS2 ในการทดสอบ ทำการวัดประสิทธิภาพของเครือข่ายด้านการส่งผ่านข้อมูล (Throughput Data) การหน่วงเวลาในการส่งข้อมูลระหว่างต้นทางไปยังปลายทาง (Delay end to end) และระยะเวลาของการใช้งาน (Lifetime) ระหว่างการส่งผ่านข้อมูลที่มีขนาดสูง (High data rate) และ ส่งผ่านข้อมูลที่มีขนาดต่ำ (Low data rate)



ภาพที่ 2.18 ภาพ (a) Circular Topology ภาพ (b) An example of the multipath routing in subnet ZigBee cluster-tree

ที่มา: Zahia Bidai and Hafid Haffaf “Node disjoint multi-path routing for zigbee cluster-tree Wireless Sensor Networks”, Multimedia Computing and Systems (ICMCS), Ouarzazate, Morocco, April 2011.

จากภาพที่ 2.18 ภาพ a เป็นรูปแบบเครือข่ายที่จะนำมาจำลอง โดยการกำหนดให้โหนดปลายทางในที่นี้คือ โหนดประสานงานเครือข่าย (PAN Coordinator node) อยู่ที่ศูนย์กลางของเครือข่าย และมีการส่งข้อมูลจากโหนดต้นทาง (Source node) ผ่านไปยังเราเตอร์โหนดต่างๆ ภาพ b เป็นตัวอย่างของเส้นทางที่ถูกสร้างขึ้นซึ่งจะเห็นได้ว่ามีอยู่ 3 เส้นทางที่จะวิ่งไปยังโหนดปลายทางบนเครือข่ายแบบ กลุ่มต้นไม้ (Cluster tree)

ในการจำลองการทำงานของเครือข่ายเซนเซอร์ไร้สาย บนโปรแกรม NS2 มีการกำหนดค่าพารามิเตอร์ และตั้งค่าต่างๆ ดังนี้

ตารางที่ 2.1 ค่าการตั้งค่าพารามิเตอร์ในโปรแกรม NS2

พารามิเตอร์	ค่าที่กำหนด
Number of Nodes	29
Radio Transmission range (m)	17
Number of FFD	28
Number of Simulation Runs	(4*8) a total 32
Circle Radius R (m)	10
Number of Sources	1
Number of Sinks	1 (PAN Coordinator)
Sink Position	Center of the area
Node Mobility	None
ZigBee Parameters (Lm, Cm, Rm)	(3,4,4)
Initial Energy of Sensor nodes	1 j
Transmission Energy	0.3μ j/bit
Reception Energy	0.3μ j/bit
MAC Protocol	IEEE802.15.4 (Non-Beacon mode with unslotted CSMA/CA mechanism)
Propagation Model	Two Ray Ground Model
Queue Size	50
Data Transfer Model	Direct Data Transmission
Traffic Model	Poisson traffic
Packet Size (bytes)	80
Simulation Area (m*m)	70*70
Traffic load (pps)	200, 100, 50, 20, 10, 5, 2, 1
Simulation Time (sec)	100

ในการวัดผลของประสิทธิภาพของการทำงานของวิธี Z-MHTR นั้น พวกเขาพิจารณาตัวชี้วัดต่างๆ ดังนี้

1) Packet delivery fraction เป็นค่าความสำเร็จในการรับข้อมูลที่ปลายทางกับจำนวนข้อมูลที่ถูกส่งจากต้นทาง

2) Average end-to-end delay เป็นค่าการหน่วงเวลาโดยเฉลี่ย จากการส่งข้อมูลจากต้นทางไปยังปลายทาง

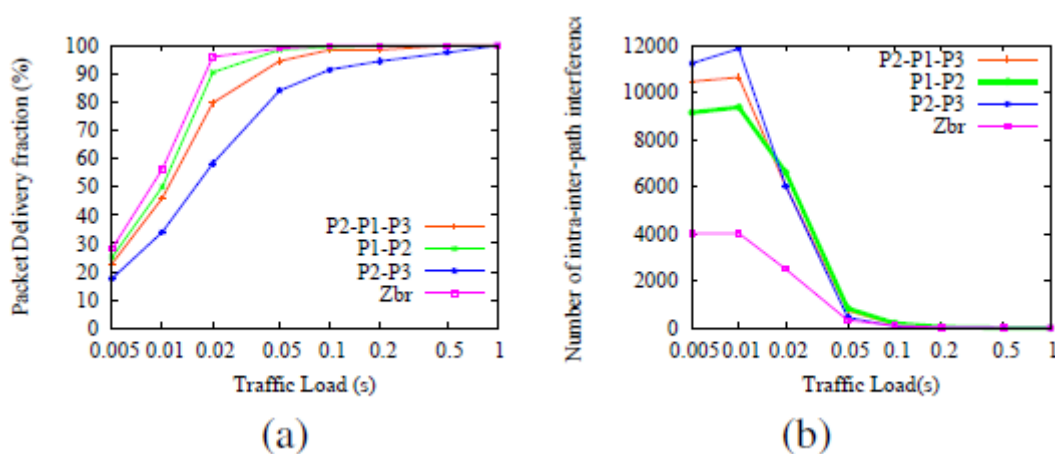
3) Network lifetime เป็นค่าเวลาทั้งหมดที่เครือข่ายทำงาน เมื่อปลายทางหยุดรับข้อมูลจากต้นทาง เครือข่ายก็จะหยุดทำงาน

จากตัวชี้วัดข้างต้นสามารถตีความหรือตั้งข้อสังเกตอื่นๆ ได้ดังนี้

1) เกิดการชนกันของข้อมูลที่โหนดปลายทาง ทำให้เกิดการหลุดของข้อมูลได้ ซึ่งเป็นปัจจัยที่เกี่ยวข้องกับจำนวนข้อมูลที่หลุดไป

2) เกิดการชนกันของข้อมูลภายในเส้นทางเดียวกัน ทำให้เกิดการหลุดของข้อมูลได้ ซึ่งเป็นปัจจัยที่เกี่ยวข้องกับจำนวนข้อมูลที่หลุดไป

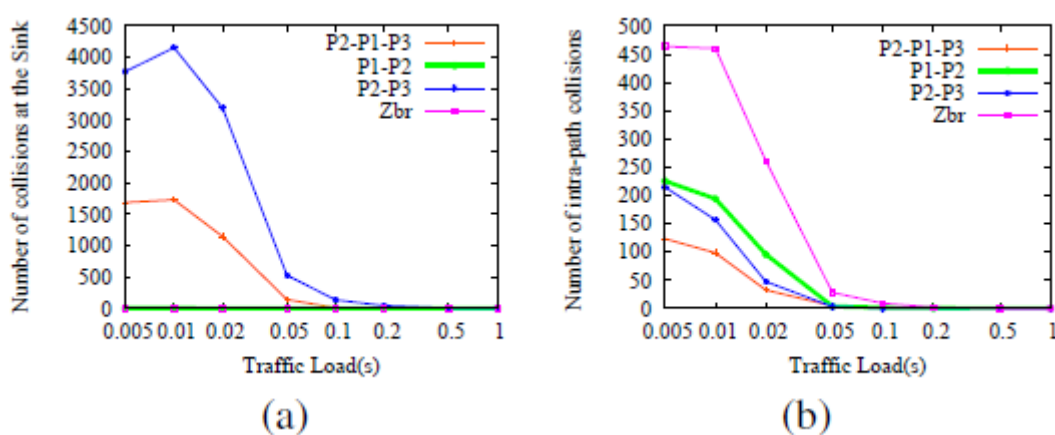
3) เกิดการรบกวนกันระหว่างเส้นทางภายใน กับเส้นทางภายนอก ทำให้เกิดการหลุดของข้อมูลได้ ซึ่งเป็นปัจจัยที่เกี่ยวข้องกับจำนวนข้อมูลที่หลุดไป



ภาพที่ 2.19 ภาพ (a) Packet delivery fraction ภาพ (b) Number of intra-path and inter-path interference in the different routing strategies

ที่มา: Zahia Bidai and Hafid Haffaf “Node disjoint multi-path routing for zigbee cluster-tree Wireless Sensor Networks”, Multimedia Computing and Systems (ICMCS), Ouarzazate, Morocco, April 2011.

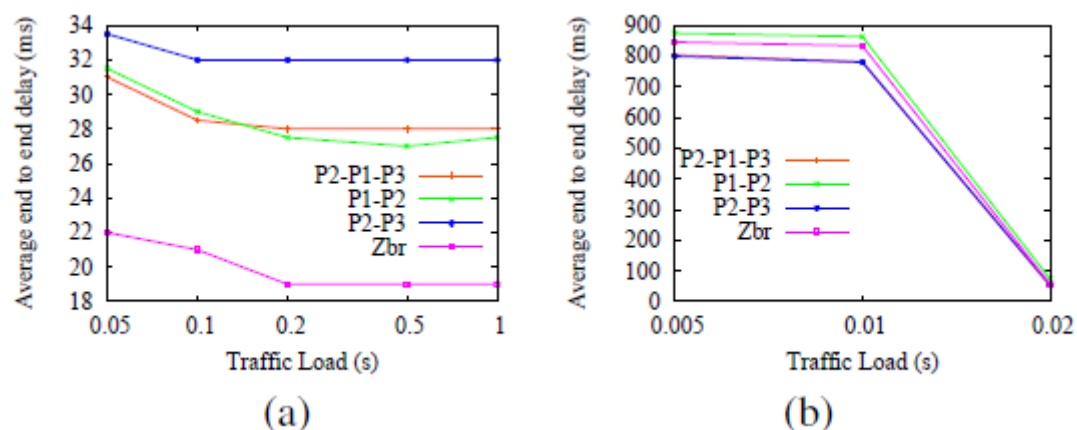
จากภาพที่ 2.19 ภาพ (a) จะเห็นได้ว่าเปอร์เซ็นต์ระหว่างการส่งและรับข้อมูลสำเร็จนั้นแบบที่เป็นเส้นทางเดียว (Zbr) จะมีค่าสูงกว่าการส่งข้อมูลแบบหลายๆ เส้นทางในทุกๆ ค่าภาระการจราจร (Traffic Load) ส่วนภาพ (b) แสดงถึงการรบกวนกันของเส้นทางระหว่างเส้นทางภายในกับเส้นทางภายนอก จะเห็นได้ว่าการรบกวนกันแบบที่เป็นเส้นทางเดียว (Zbr) มีค่าน้อยกว่าการส่งข้อมูลแบบหลายๆ เส้นทาง ตั้งแต่การส่งข้อมูลที่มีค่ามากกว่า 20 pps



ภาพที่ 2.20 ภาพ (a) Number of collisions at the sink ภาพ (b) Number of intra-path collisions in the different routing strategies

ที่มา: Zahia Bidai and Hafid Haffaf “Node disjoint multi-path routing for zigbee cluster-tree Wireless Sensor Networks”, Multimedia Computing and Systems (ICMCS), Ouarzazate, Morocco, April 2011.

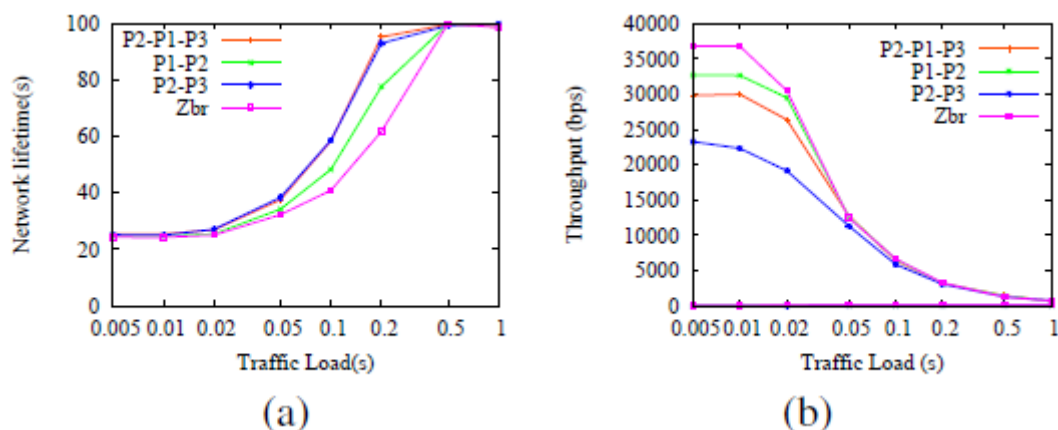
จากภาพที่ 2.20 ภาพ (a) จะแสดงให้เห็นถึงการชนกันของข้อมูลที่ตัวโหนดปลายทาง โดยการส่งข้อมูลแบบที่เป็นเส้นทางเดียว (Zbr) จะไม่เกิดการชนข้อมูลเลย แต่แบบการส่งข้อมูลแบบหลายๆ เส้นทางมีอยู่ 1 เส้นทางที่ไม่มีการชนกันของข้อมูล ส่วนอีก 2 เส้นทาง เริ่มมีการชนของข้อมูลมากขึ้นตั้งแต่การส่งข้อมูลที่มีค่ามากกว่า 20 pps ส่วนภาพ (b) แสดงถึงการชนกันของข้อมูลภายในเส้นทางเดียวกัน ซึ่งการส่งข้อมูลแบบหลายๆ เส้นทาง ทำได้ดีกว่าการส่งข้อมูลแบบเส้นทางเดียว แต่ก็เห็นได้ว่าเริ่มมีการชนกันเกิดขึ้นอย่างมากตั้งแต่การส่งข้อมูลที่มีค่ามากกว่า 20 pps



ภาพที่ 2.21 ภาพ (a) Average end to end delay in the different routing at time: 0.05s to 1s ภาพ (b) at time: 0.005s to 2s

ที่มา: Zahia Bidai and Hafid Haffaf “Node disjoint multi-path routing for zigbee cluster-tree Wireless Sensor Networks”, Multimedia Computing and Systems (ICMCS), Ouarzazate, Morocco, April 2011.

จากภาพที่ 2.21 ภาพ (a) จะแสดงให้เห็นถึงค่าเฉลี่ยของการหน่วงเวลาของข้อมูลจากต้นทางไปยังปลายทาง โดยพิจารณาข้อมูลที่มีขนาดตั้งแต่ 1pps ถึง 20pps โดยการส่งข้อมูลแบบที่เป็นเส้นทางเดียว (Zbr) จะมีการหน่วงเวลาน้อยกว่าแบบการส่งข้อมูลแบบหลายๆ เส้นทาง ซึ่งมีการหน่วงเวลามาก ภาพ (b) จะแสดงให้เห็นถึงค่าเฉลี่ยของการหน่วงเวลาของข้อมูลจากต้นทางไปยังปลายทาง โดยพิจารณาข้อมูลที่มีขนาดตั้งแต่ 50pps ถึง 200pps ซึ่งในกรณีนี้ ทั้งการส่งข้อมูลแบบเส้นทางเดียว แบบหลายเส้นทาง เริ่มมีการหน่วงเวลามากขึ้นเรื่อยๆ



ภาพที่ 2.22 ภาพ (a) Network lifetime ภาพ (b) Throughput in the different routing strategies

ที่มา: Zahia Bidai and Hafid Haffaf “Node disjoint multi-path routing for zigbee cluster-tree Wireless Sensor Networks”, Multimedia Computing and Systems (ICMCS), Ouarzazate, Morocco, April 2011.

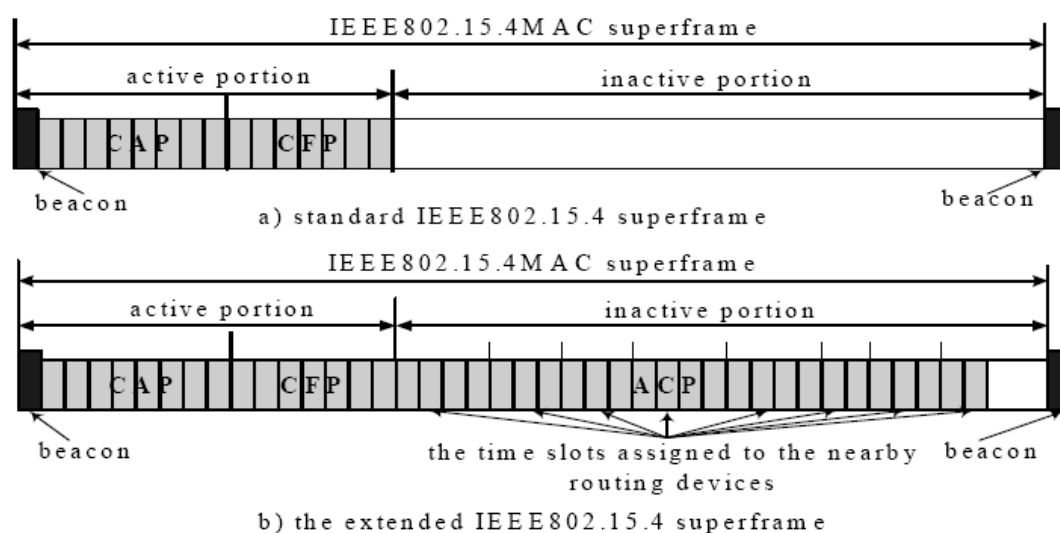
จากภาพที่ 2.22 ภาพ (a) จะแสดงให้เห็นถึงอายุการใช้งานเครือข่าย โดยแบบเส้นทางเดียว โหนดปลายทางจะหยุดรับข้อมูลก็เมื่อโหนดแรกที่เชื่อมต่อกับมันหยุดทำงาน ส่วนแบบหลายเส้นทาง ตัวโหนดปลายทางจะหยุดรับข้อมูลก็เมื่อโหนดแรกของทุกๆ เส้นทาง ที่เชื่อมต่อกับมันหยุดทำงาน ซึ่งที่ขนาดของข้อมูลที่มีการส่งเท่าๆ กันที่ 5pps ตัวการทำงานของเครือข่ายที่ใช้แบบเส้นทางเดียวจะทำงานน้อยกว่า ซึ่งทำให้อายุการใช้งานยาวนานกว่า ส่วนที่ $< 2\text{pps}$ และ $> 100\text{pps}$ การทำงานของเครือข่ายพอๆ กัน ในภาพ (b) จะแสดงให้เห็นถึงขนาดของข้อมูลที่ผ่านเครือข่ายโดยที่จราจรภายในเครือข่ายมากกว่า 20pps การใช้เส้นทางเดียว จะให้ข้อมูลผ่านได้มากที่สุด

ในส่วนของการงานวิจัยนี้ จะมีปัญหาอยู่ในเรื่องของการชนกันของข้อมูลภายในเส้นทางเดียวกัน และข้ามเส้นทาง จึงเป็นสาเหตุให้เกิดการหน่วงเวลาของข้อมูลและเป็นผลทำให้การส่งผ่านข้อมูลทำได้ช้าลง ดังนั้นจึงคิดว่าการส่งข้อมูลแบบเส้นทางเดียวน่าจะทำได้ดีกว่าการส่งหลายเส้นทาง เนื่องจากเกิดการชนกันของข้อมูลที่โหนดปลายทาง และระหว่างเส้นทางน้อยกว่า อีกทั้งยังทำให้การส่งข้อมูลสามารถทำได้มากกว่าแบบหลายเส้นทาง

2.14.3 งานวิจัยเรื่อง Congestion Control for Industrial Wireless Communication Gateway

จากงานวิจัยของ Tang Zhong, Mei Zhan

เป็นงานวิจัยเกี่ยวกับการลดความคับคั่งของข้อมูลที่เกตเวย์ โดยอาศัยการเพิ่มประสิทธิภาพของ IEEE802.15.4 MAC super frame ซึ่งโดยปกติแล้วที่ตัวเกตเวย์ การทำงานจะทำงานแบ่งเป็น 2 ส่วนคือส่วนที่ Active กับส่วนที่เป็น Inactive ดังภาพที่ 2.23



ภาพที่ 2.23 การทำงานของ IEEE802.15.4 MAC super frame

ที่มา: Tang Zhong, Mei Zhan “Congestion Control for Industrial Wireless Communication Gateway”

จากภาพที่ 2.23 (b) จะเห็นได้ว่าการเพิ่มการส่งข้อมูลในส่วนที่เป็น Inactive portion ซึ่งจะช่วยลดปัญหาความคับคั่งของข้อมูลที่ตัวเกตเวย์ได้ แต่อย่างไรก็ตามงานวิจัยนี้ ไม่ได้กล่าวถึงปัญหาในกรณีที่เกตเวย์เกิดการเสียหาย ดังนั้นจึงคิดว่าอาจเกิดปัญหา SPOF ที่ตัวเกตเวย์ได้