บทที่ 2
ทฤษฎีพื้นฐานที่ใช้ในการวิจัย

เครือข่ายเคลื่อนที่เฉพาะกิจเป็นเครือข่ายที่สะดวกต่อการใช้งานของผู้ใช้ เนื่องจากผู้ใช้สามารถเชื่อมต่อเข้ากับเครือข่ายได้โดยไม่ต้องใช้โครงข่าย แต่ผู้ใช้จะต้องมีอุปกรณ์เครือข่ายสำหรับติดต่อกับเครือข่าย เช่น การ์ดแลนไร้สาย (Wireless LAN card 802.11) ซึ่งปัจจุบันการ์ดแลนชนิดนี้ได้รับความนิยมอย่างแพร่หลายและมักจะถูกติดตั้งมาพร้อมกับเครื่องคอมพิวเตอร์พกพา เช่น แล็ปท็อป หรือ พีดีเอ ทำให้ผู้ใช้สามารถเชื่อมต่อหรือสร้างเครือข่ายเคลื่อนที่เฉพาะกิจได้ง่าย โดยเครือข่ายเคลื่อนที่เฉพาะกิจเกิดจากการรวมตัวกันของโหนดไร้สายแต่ละโหนด และการการส่งข้อมูลบนเครือข่ายเคลื่อนที่เฉพาะกิจ เกิดจากความร่วมมือของผู้ใช้แต่ละคนบนเครือข่าย โดยการส่งต่อข้อมูลจากโหนดต้นทาง ไปยังโหนดข้างเคียงและส่งต่อไปเรื่อยๆ จนกระทั่งข้อมูลถึงโหนดปลายทาง

เครือข่ายเคลื่อนที่เฉพาะกิจมีคุณสมบัติหลายอย่างที่เป็นลักษณะเฉพาะ เช่น โหนดสามารถเคลื่อนที่ได้ในขณะที่เชื่อมต่อเข้ากับเครือข่าย ทรัพยากรของเครือข่ายมีอยู่อย่างจำกัด เป็นต้น ซึ่งลักษณะเหล่านี้ทำให้เครือข่ายเคลื่อนที่เฉพาะกิจ เป็นเครือข่ายที่น่าสนใจต่อการทำวิจัย

เนื้อหาในบทนี้กล่าวถึงประโยชน์และการนำเครือข่ายเคลื่อนที่เฉพาะกิจไปใช้งาน และทฤษฎีพื้นฐานของเครือข่ายเคลื่อนที่เฉพาะกิจ ความสำคัญและที่มาของงานวิจัยรวมถึงงานวิจัยที่เกี่ยวข้อง และซิมมูเลเตอร์ที่ใช้ในการทดลอง ซึ่งเนื้อหาทั้งหมดนี้จำเป็นสำหรับการศึกษาและประเมินประสิทธิภาพของระบบเครือข่ายเคลื่อนที่เฉพาะกิจ

2.1 เครือข่ายเคลื่อนที่เฉพาะกิจ

เครือข่ายเคลื่อนที่เฉพาะกิจเป็นเครือข่ายที่น่าสนใจ เพราะเป็นเครือข่ายที่สามารถนำไปประยุกต์ใช้ได้ในหลายสถานการณ์ เช่น ในสนามรบหรือการกู้ภัย เนื่องจากเครือข่ายเคลื่อนที่เฉพาะกิจมีคุณสมบัติพิเศษทางเครือข่ายหลายประการ ดังนั้นการวิจัยเกี่ยวกับเครือข่ายเคลื่อนที่เฉพาะกิจ ผู้วิจัยจำเป็นต้องศึกษาถึงหลักการทำงานพื้นฐานและลักษณะเฉพาะของเครือข่ายเคลื่อนที่เฉพาะกิจ เพื่อใช้ในการวิเคราะห์การทำงานของเครือข่ายเคลื่อนที่เฉพาะกิจได้อย่างถูกต้อง ลักษณะต่างๆ ของเครือข่ายเคลื่อนที่เฉพาะกิจมีดังต่อไปนี้

1. เครือข่ายแบบไม่มีโครงข่าย (No Infrastructure) เนื่องจากโหนดอย่างน้อย 2 โหนดสามารถสร้างเครือข่ายเคลื่อนที่เฉพาะกิจได้ โดยที่โหนดมีเพียงแค่อุปกรณ์เครือข่ายไร้สาย เช่น อินเทอร์เฟสไอทริปเปิ้ลอี 802.11 ติดตั้งมาด้วยเท่านั้นโดยไม่จำเป็นต้องมีอุปกรณ์เครือข่ายอื่นๆ เลย เช่น ฮับหรือสวิทช์ ทำให้เครือข่ายเคลื่อนที่เฉพาะกิจมีความยืดหยุ่นในการนำไปใช้งานสูง เรา

สามารถนำเครือข่ายเคลื่อนที่เฉพาะกิจไปใช้ในพื้นที่ที่ไม่มีโครงข่ายได้ โดยไม่ต้องจัดเตรียมอุปกรณ์ใดๆ ไว้ก่อน และนอกจากนี้โหนดยังสามารถเชื่อมต่อหรือยกเลิกการเชื่อมต่อกับเครือข่ายได้ตลอดเวลา

2. มีการส่งข้อมูลต่อกันเป็นทอดๆ (Multi-hop data transfer) โหนดบนเครือข่ายเคลื่อนที่เฉพาะกิจสามารถส่งข้อมูลไปให้โหนดอื่นบนเครือข่ายที่ไม่อยู่ในรัศมีการส่งข้อมูลของตนเองได้ โดยการที่โหนดต้นทางจะส่งข้อมูลไปให้โหนดข้างเคียงที่อยู่ในรัศมีการส่งข้อมูลของตัวเอง และโหนดนั้นจะทำหน้าที่ในการส่งต่อข้อมูลต่อไปให้กับโหนดถัดไปที่อยู่ในรัศมีการส่งของตัวเองไปเรื่อยๆ จนกระทั่งข้อมูลไปถึงโหนดปลายทาง

3. โหนดสามารถเคลื่อนที่ได้ในระหว่างการติดต่อสื่อสาร เนื่องจากพื้นที่การให้บริการของเครือข่ายเคลื่อนที่เฉพาะกิจคือ พื้นที่ที่สัญญาณวิทยุของโหนดในเครือข่ายครอบคลุมถึง ดังนั้นถ้าโหนดมีการเคลื่อนที่ไปกับโหนดข้างเคียงทำให้โหนดไม่หลุดจากการเชื่อมต่อ แต่การเคลื่อนที่ของโหนดส่งผลให้โทโปโลจี (Topology) ของเครือข่ายสามารถเปลี่ยนแปลงได้ตลอดเวลา การออกแบบโปรแกรมประยุกต์สำหรับเครือข่ายเคลื่อนที่เฉพาะกิจบางประเภทจำเป็นต้องคำนึงถึงคุณสมบัติข้อนี้ด้วย เช่น การออกแบบเราติ้งโปรโตคอล

4. ความปลอดภัยของข้อมูล เนื่องจากเครือข่ายเคลื่อนที่เฉพาะกิจใช้คลื่นวิทยุเป็นฟิสิกซ์คอลเลเยอร์ ทำให้โหนดสามารถเคลื่อนที่ได้อย่างอิสระภายในบริเวณที่สัญญาณวิทยุของโหนดอื่นเชื่อมถึง แต่สัญญาณวิทยุสามารถถูกรบกวนได้โดยสัญญาณวิทยุในช่วงความถี่ใกล้เคียงจึงทำให้ข้อมูลที่ส่งมาถูกรบกวนได้ ส่งผลให้ประสิทธิภาพของเครือข่ายลดลงหรือไม่สามารถส่งข้อมูลได้เลย และเนื่องจากสัญญาณมีการแพร่กระจายในวงกว้างจึงอาจส่งผลต่อความปลอดภัยของข้อมูลได้ เนื่องจากผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ส่งผ่านช่องสัญญาณได้ง่าย

5. ทรัพยากรที่จำกัดของเครือข่าย เพราะเครือข่ายเคลื่อนที่เฉพาะกิจเป็นเครือข่ายที่เกิดจากการรวมตัวของผู้ใช้งานเครือข่าย และเนื่องจากเป็นเครือข่ายที่ไม่มีโครงข่ายดังนั้นแต่ละโหนดที่อยู่ในเครือข่ายนอกจากจะทำหน้าที่เป็นผู้ใช้บริการแล้วยังต้องทำหน้าที่เป็นผู้ให้บริการในส่วนของโครงข่ายอีกด้วย ดังนั้นทรัพยากรที่มีอยู่ของเครือข่ายเคลื่อนที่เฉพาะกิจจึงเป็นทรัพยากรที่ได้มาจากทรัพยากรของโหนดแต่ละโหนดที่เข้าร่วมเครือข่าย ซึ่งโหนดเหล่านี้ล้วนมีทรัพยากรต่างๆ อยู่อย่างจำกัด เช่น หน่วยประมวลผล หน่วยความจำ นอกเหนือจากทรัพยากรเหล่านี้แล้วพลังงานยังเป็นทรัพยากรที่จำกัดที่สุดสำหรับอุปกรณ์เคลื่อนที่เหล่านี้เพราะอุปกรณ์เหล่านี้ใช้พลังงานจากแบตเตอร์รี่เป็นหลัก

6. แต่ละโหนดมีความสามารถในการทำงานที่เหมือนกัน (Homogeneous) เนื่องจากโหนดสามารถเป็นได้ทั้งผู้รับหรือผู้ส่งข้อมูล และยังสามารถทำหน้าที่ในการส่งต่อข้อมูลของโหนดอื่นได้ในขณะเดียวกัน ซึ่งแตกต่างจากเครือข่ายประเภทอื่นที่มีการแยกหน้าที่ของต้นทาง-ปลายทางและโหนดที่ส่งต่อข้อมูลอย่างชัดเจน

7. ไม่มีการจัดการแบบรวมศูนย์ (No centralize administration) โทโปโลจีของเครือข่ายมีการเปลี่ยนแปลงอยู่ตลอดเวลาเนื่องจากการเคลื่อนที่และการเข้าออกของโหนด จึงเป็นการยากที่จะจัดหาโหนดมาทำหน้าที่เป็นศูนย์กลางของเครือข่าย และนอกจากนี้โหนดบนเครือข่ายเคลื่อนที่เฉพาะกิจเป็นโหนดที่มีประสิทธิภาพประสิทธิภาพใกล้เคียงกันเนื่องจากข้อจำกัดของโหนดเคลื่อนที่ ดังนั้นจึงไม่มีโหนดใดโหนดหนึ่งที่เหมาะสมกับหน้าที่ในการจัดการเครือข่าย

เครือข่ายเคลื่อนที่เฉพาะกิจที่ใช้ในงานวิจัยชิ้นนี้ ทำงานอยู่บนแอดฮ็อกโหมดของเครือข่ายแลนไร้สายมาตรฐาน 802.11 มาตรฐานแลนไร้สาย 802.11 ยังถูกพัฒนาเป็นมาตรฐานย่อยๆ อื่นอีก เช่น มาตรฐานแลนไร้สาย 802.11a, 802.11b, 802.11g และอื่นๆ

2.1.1 มาตรฐานไอทริปเปิลอี 802.11 (IEEE 802.11)

มาตรฐานแลนไร้สายไอทริปเปิลอี 802.11 เริ่มประกาศใช้โดยไอทริปเปิลอีในปี ค.ศ. 1997 ซึ่งในมาตรฐานนี้มีการใช้ฟิสิกซ์คอลเลเยอร์ (Physical Layer) และมีเดียมแอกเซสคอลโทร (Medium Access Control) แบบใหม่ และแบ่งการทำงานของอุปกรณ์ 802.11 ได้ 2 รูปแบบคือ 1) การติดต่อระหว่างอุปกรณ์ด้วยกันโดยไม่มีโครงข่าย ซึ่งเรียกว่าการติดต่อแบบเฉพาะกิจ (Ad hoc mode) 2) สามารถเชื่อมต่อเข้ากับโครงข่าย (Infrastructure mode) โดยเชื่อมต่อผ่านอุปกรณ์แอกเซสพอยท์ (Access point) เพื่อส่งข้อมูลไปยังระบบเครือข่ายแลนแบบอีเทอร์เน็ต (Ethernet) ได้ โดยมีอัตราการส่งข้อมูลอยู่ที่ 1 เม็กกะบิตต่อวินาที และอัตราการส่งข้อมูลสูงสุดอยู่ที่ 2 เม็กกะบิตต่อวินาที ซึ่งอัตราการส่งข้อมูลจะขึ้นอยู่กับชนิดของใช้ฟิสิกซ์คอลเลเยอร์ที่เลือกใช้

มาตรฐาน 802.11 มีตัวกลางในชั้นใช้ฟิสิกซ์คอลเลเยอร์ให้เลือกถึง 3 ชนิดด้วยกัน ประกอบด้วยตัวกลางที่เป็นคลื่นความถี่วิทยุ (Radio Wave) 2 ชนิด และอีกชนิดคือคลื่นอินฟราเรด (Infrared) เนื่องจากต้องการให้มาตรฐาน 802.11 สามารถใช้งานได้ในทุกๆ ประเทศทั่วโลก ดังนั้นจึงเลือกให้ตัวกลางที่เป็นความถี่วิทยุให้ทำงานที่ย่านความถี่สาธารณะสากล (Industrial, scientific and medical - ISM band) เป็นหนึ่งในตัวกลางประเภทความถี่วิทยุ แต่ช่วงของแบนวิดท์ (Bandwidth) จะแตกต่างกันขึ้นอยู่กับข้อกำหนดของแต่ละประเทศ เช่น ในสหภาพยุโรปใช้ในช่วงความถี่ 2.412 ถึง 2.472 จิกะเฮิร์ต ในประเทศญี่ปุ่นใช้ในช่วงความถี่ 2.412 ถึง 2.484 จิกะเฮิร์ต เป็นต้น

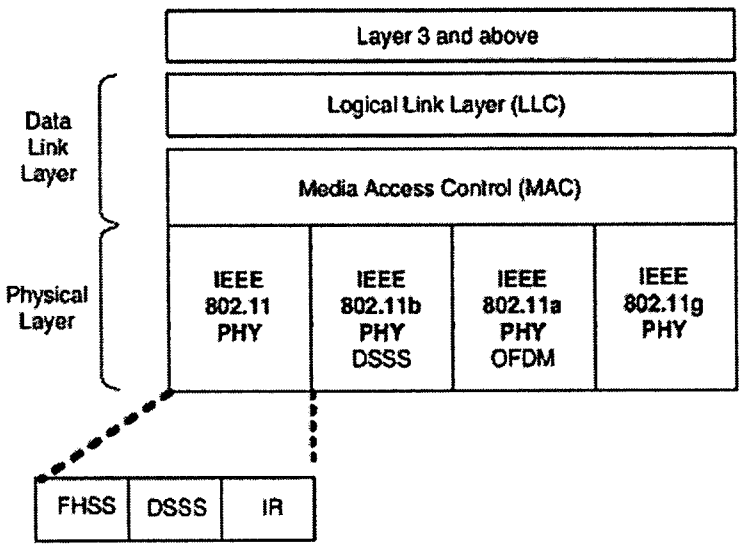
เนื่องจากอัตราการส่งข้อมูลสูงสุดของ 802.11 มีเพียง 2 เม็กกะบิตต่อวินาทีเท่านั้น ซึ่งถือว่าน้อยเกินไปสำหรับการส่งข้อมูลที่มีขนาดใหญ่และข้อมูลของโปรแกรมประยุกต์ ประเภทมัลติมีเดีย (multimedia application) ดังนั้นจึงมีการพัฒนามาตรฐานไอทริปเปิลอี 802.11 เพิ่มเติม ได้แก่ มาตรฐานไอทริปเปิลอี 802.11a และ 802.11b โดยมีการแก้ไขเพียงส่วนของฟิสิกซ์คอลเลเยอร์เท่านั้น

แต่ในประเทศไทยอนุญาตให้ใช้เฉพาะคลื่นวิทยุที่ความถี่สากลเท่านั้น ซึ่งก็คือมาตรฐานไอทริปเปิลอี 802.11b มีอัตราการส่งข้อมูลสูงสุดอยู่ที่ 11 เม็กกะบิตต่อวินาที และมีอัตรา

การส่งข้อมูลอื่นๆ อยู่ที่ 5.5, 2, 1 เม็กกะบิตต่อวินาที ตัวมาตรฐานมีกลไกสำหรับการรองรับอัตราการส่งข้อมูลจากอัตราการส่งข้อมูลที่แตกต่างกันนี้ ซึ่งในอัตราการส่งข้อมูลที่ 1, 2 เม็กกะบิตต่อวินาทีนั้นออกแบบตามอัตราการส่งข้อมูลจากมาตรฐานไอทริปเปิลอี 802.11 ให้ทำงานได้บนช่วงความถี่คลื่นวิทยุ

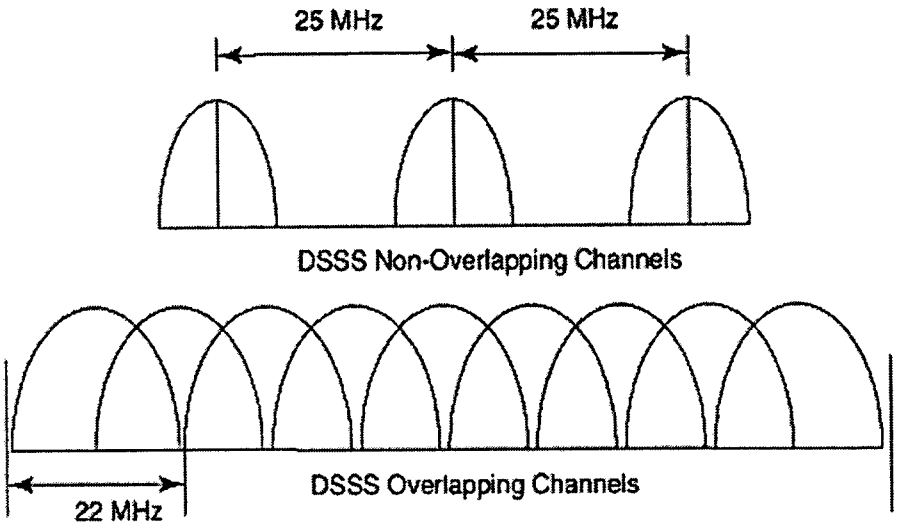
2.1.2 การทำงานของไอทริปเปิลอี 802.11 ในโอเอสไอโมเดล (OSI Model)

เราสามารถแบ่งการทำงานของมาตรฐานไอทริปเปิลอี 802.11 ตามโอเอสไอโมเดลได้เป็น 2 เลเยอร์ ได้แก่ ดาต้าลิงค์เลเยอร์ (Data Link Layer) และฟิสิกซ์คอลเลเยอร์ ซึ่งในแต่ละเลเยอร์จะกำหนดวิธีการทำงานตามหน้าที่ของแต่ละเลเยอร์ไว้



รูปที่ 2.1 มาตรฐานไอทริปเปิลอี 802.11 ในโอเอสไอโมเดล

2.1.2.1 การทำงานในชั้นฟิสิกซ์คอลเลเยอร์ ในชั้นนี้ได้กำหนดวิธีการทำงานของฟิสิกซ์คอลมีเดียม (Physical Medium) ให้สามารถรองรับอัตราการส่งข้อมูลที่ 5.5 เม็กกะบิตต่อวินาที และที่ 11 เม็กกะบิตต่อวินาที แต่ต้องใช้ตัวกลางเป็นคลื่นวิทยุและทำงานอยู่บนย่านความถี่สาธารณะสากลเท่านั้น ซึ่งใช้วิธีแบบไดเร็กซีเควนซ์สเปรดสเป็กตรัม (Direct Sequence Spread Spectrum - DSSS) ดังรูปที่ 2.2 เพื่อแบ่งช่วงความถี่ทั้งหมดออกเป็นช่วงความถี่ย่อยๆ และเลือกช่วงความถี่ย่อยนั้นมาใช้ส่งข้อมูลตามรูปที่ 2.1 อัตราการส่งข้อมูลบนมาตรฐานไอทริปเปิลอี 802.11 ขึ้นอยู่กับความแรงของสัญญาณคลื่นวิทยุ คือ ถ้าอยู่ในบริเวณที่มีคลื่นสัญญาณที่ดีก็สามารถส่งข้อมูลได้ที่ 5.5 หรือ 11 เม็กกะบิตต่อวินาที แต่ถ้าคลื่นสัญญาณไม่ดีก็จะส่งข้อมูล 1 หรือ 2 เม็กกะบิตต่อวินาที วิธีการที่ 802.11 ใช้ในการส่งข้อมูลที่อัตราต่างๆ ได้แสดงไว้ในตารางที่ 2.1



รูปที่ 2.2 ช่วงความถี่ไดเร็กซีเควนซ์สเปรดสเป็กตรัม

ตารางที่ 2.1 วิธีการทำงานของไอทริปเปิลอี 802.11 ที่อัตราการส่งข้อมูลต่างๆ

Data Rate	Code	Modulation	Symbol Rate	Bit / Symbol
1 Mbps	11 bit Braker	DBPSK	1 Msps	1
2 Mbps	11 bit Braker	DBPSK	1 Msps	2
5.5 Mbps	8 bit CCK or PBCC	DQPSK	1.375 Msps	4
11 Mbps	8 bit CCK or PBCC	DQPSK	1.375 Msps	8

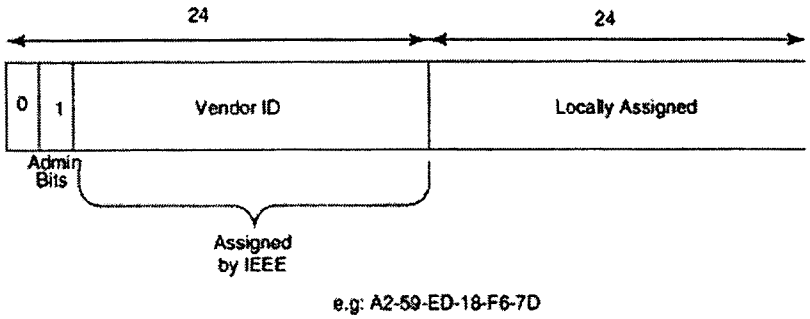
CCK : complementary code keying

PBCC : packet binary convolutional keying

2.1.2.2 การทำงานในชั้นดาต้าลิงค์เลเยอร์ การออกแบบในเลเยอร์นี้สำหรับมาตรฐานไอทริปเปิลอี 802.11 เตรียมไว้เพื่อรองรับความสามารถที่ผู้ใช้หลายคนสามารถใช้ตัวกลางร่วมกันได้ (Multiple users share a medium) ความน่าเชื่อถือของข้อมูลที่ส่ง (Reliable) และรวมถึงคุณสมบัติอื่นๆ ที่มีในชั้นมีเดียมแอกเซสคอนโทลเลเยอร์ (Medium Access Control Layer) เช่น ไซคลิกรีดันแดนซีเช็กซัม (Cyclic Redundancy Checksum - CRC) การแยกส่วนเพ็กเก็จ (Packet fragmentation) และเพิ่มความสามารถในด้านความปลอดภัย ซึ่งในเลเยอร์นี้แบ่งออกเป็นอีก 2 เลเยอร์ย่อย ได้แก่ โลจิคอลลิงค์เลเยอร์ (Logical Link Layer - LLC) และมีเดียแอ็กเซสคอนโทล (Media Access Control - MAC) สำหรับชั้นโลจิคอลลิงค์เลเยอร์ การทำงานในชั้นนี้เหมือนกับมาตรฐานแลนอื่นๆ คือ ทำหน้าที่เป็นตัวกลางการเชื่อมต่อการทำงานระหว่างเน็ตเวิร์คเลเยอร์ (Network Layer) และฟิซิกส์คอลเลเยอร์ แต่ในชั้นมีเดียแอ็กเซสคอนโทลเลเยอร์มาตรฐานไอทริปเปิลอี 802.11 ได้จัดเตรียมวิธีการต่างๆ ที่เหมาะสมกับเครือข่ายไร้สายไว้มากมาย

เช่น การจัดการแอดเดรส (Addressing) ฟิสิกซ์คอลแคเรียเซนซ์ (Physical Carrier Sense) ความน่าเชื่อถือและความคงทนของข้อมูล (Reliability and Robustness) การจัดการพลังงาน (Power management) และด้านความปลอดภัย (Security)

1) การจัดการแอดเดรสมีการใช้รูปแบบแม็กแอดเดรส (MAC Address) แบบเดียวกับมาตรฐานไอทริปเปิลอี 802.3 ดังรูปที่ 2.3 โดยมีแอดเดรสต้นทาง (Source Address) และแอดเดรสปลายทาง (Destination Address) และมีส่วนที่เพิ่มเติมขึ้นมาสำหรับมาตรฐานไอทริปเปิลอี 802.11 เพื่อใช้เป็นแอดเดรสของผู้ส่ง (Transmitter Address - TA) และแอดเดรสของผู้รับ (Receiver Address - RA) และค่าเบสิกเซ็ตไอเด็นติไฟเอร์ (Basic Set Identifier - BBS ID)

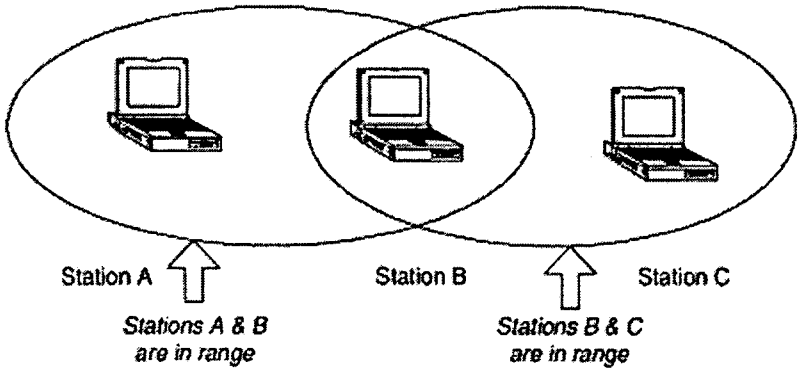


รูปที่ 2.3 ค่าแม็กแอดเดรสของอุปกรณ์ไอทริปเปิลอี 802.11

2) ฟิสิกซ์คอลแคเรียเซนซ์ อุปกรณ์เครือข่ายใน 802.11 เป็นแบบใช้ตัวกลางร่วมกัน (Shared medium) และอุปกรณ์แต่ละชิ้นสามารถตรวจสอบได้ว่ามีอุปกรณ์อื่นๆ กำลังส่งข้อมูลผ่านตัวกลางนี้อยู่หรือไม่ ดังนั้นวิธีการซีเอสเอ็มเอ (Carrier Sense Multiple Access – CSMA) จึงสามารถนำมาใช้กับ 802.11 ได้ แต่อุปกรณ์ใน 802.11 สามารถตรวจสอบการชน (Collision Detection) กันของข้อมูลได้ยาก ดังนั้นจึงไม่สามารถนำวิธีการตรวจสอบการชนกันของข้อมูลจาก 802.3 มาใช้ได้จึงได้พัฒนาวิธีการป้องกันการชนของข้อมูล (collision avoidance) ขึ้นมา โดยกำหนดให้ เมื่อผู้รับได้รับข้อมูลและตรวจสอบแล้วว่าข้อมูลที่ได้รับมาถูกต้องก็จะส่งค่าแอ็กโนวเลจเม้นต์ (Acknowledge) กลับไป ถึงแม้ว่าวิธีการนี้จะเป็นการเพิ่มโอ่เวอร์เฮด (Overhead) ให้กับการส่งข้อมูลแต่ก็มีส่วนช่วยในการสร้างความน่าเชื่อถือในการส่งข้อมูลให้แก่ตัวกลางแบบไร้สาย แต่ในการใช้งานจริงยังคงมีปัญหา เนื่องจากแต่ละโหนดสามารถตรวจสอบการใช้งานของตัวกลางได้แค่ในรัศมีของตนเองเท่านี้ ซึ่งเป็นที่มีของปัญหาโหนดที่มองไม่เห็น (Hidden Node Problem)

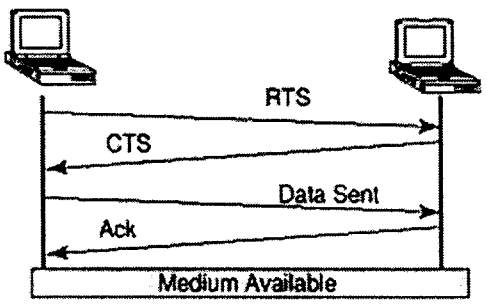
ปัญหาโหนดที่มองไม่เห็น จากรูปที่ 2.4 มีโหนดไร้สายอยู่ 3 โหนดเชื่อมต่อกันด้วยไอทริปเปิลอี 802.11 ซึ่งโหนด A และ B สามารถเชื่อมต่อกัน และเป็นเช่นเดียวกันในโหนด B และโหนด C แต่โหนด A และโหนด C ไม่สามารถเชื่อมต่อกันได้ ดังนั้นเมื่อโหนด A และโหนด

C ส่งข้อมูลมายัง โหนด B พร้อมๆ กันแล้วโหนด B จะไม่สามารถรับข้อมูลที่ถูกต้องได้เลย เนื่องจากข้อมูลจากโหนด A ชนกับข้อมูลจากโหนด C



รูปที่ 2.4 ปัญหาโหนดที่มองไม่เห็น

วิธีการแก้ปัญหาโหนดที่มองไม่เห็น สามารถทำได้โดยเพิ่มข้อความอีก 2 แบบ ได้แก่ รีเควสทูเซ้นต์ (RTS - Request to Send) และเคลียร์ทูเซ้นต์ (CTS - Clear to Send) การใช้งาน 2 ข้อความนี้คือนี้คือ เมื่อเครื่อง A ต้องการจะส่งข้อมูลไปยังเครื่อง B จะเริ่มโดยการส่งรีเควสทูเซ้นต์ไปก่อน เพื่อบอกให้เครื่อง B ทราบว่าโหนด A ต้องการส่งข้อมูลหา B และให้โหนด B เตรียมตัวรับข้อมูล เมื่อโหนด B ได้รับรีเควสทูเซ้นต์อย่างถูกต้องก็จะส่งเคลียร์ทูเซ้นต์ออกมา เพื่อที่จะบอกโหนด A ว่าพร้อมที่จะรับข้อมูลแล้ว ซึ่งเคลียร์ทูเซ้นต์นี้ทั้งโหนด A และ C จะได้รับทั้งคู่ แต่จะมีเพียงโหนด A เท่านั้นที่สามารถส่งข้อมูลได้เพราะเคลียร์ทูเซ้นต์เป็นการตอบรับต่อรีเควสทูเซ้นต์ของโหนด A ตามรูปที่ 2.5



รูปที่ 2.5 ขั้นตอนการส่งข้อมูลบนไอทริปเปิลอี 802.11

3) ความน่าเชื่อถือและความคงทนของข้อมูล มาตรฐานไอทริปเปิลอี 802.11 ใช้วิธีแฟรกเม้นเทชั่น และไซคลิกรีดันแดนซีเช็กซัม (Cyclic Redundancy Checksum - CRC) การทำแฟรกเม้นเทชั่นคือการแยกข้อมูลที่ต้องการส่งออกเป็นส่วนเล็กๆ แล้วส่งออกไป เมื่อผู้รับได้รับ

ข้อมูลก็จะนำข้อมูลส่วนเล็กๆ นำมาประกอบกันเป็นข้อมูลเดิมก่อนที่จะแตกออกมา การทำแบบนี้มีข้อดีในสภาวะที่มีการส่งข้อมูลจำนวนมาก (congested environment) หรือสภาวะที่มีการรบกวนมาก (interference) เพราะถ้าข้อมูลเกิดการเสียหายจนต้องส่งข้อมูลซ้ำก็จะส่งเป็นข้อมูลขนาดเล็กๆ ส่วนการทำไซคลิกรีดันแดนซีเช็กซัมนั้นใช้เพื่อให้ฝั่งรับสามารถตรวจสอบได้ว่าข้อมูลที่ได้รับมานั้นถูกต้องหรือไม่

4) การจัดการพลังงาน (Power management) เพื่อเป็นการประหยัดพลังงาน อุปกรณ์ 802.11 สามารถยกเลิกการทำงานของตัวรับส่งสัญญาณของตัวเองได้ โดยใช้กลไกที่เรียกว่าพาวเวอร์เซฟโหมด (Power Save Mode) ในการแจ้งแก่เครื่องอื่นๆ ว่าต้องการจะทำงานแบบต่อเนื่อง (aware mode) หรือแบบไม่ต่อเนื่อง (power save mode) การทำงานในพาวเวอร์เซฟโหมดเครื่องไวร์เลสโอสต์จะแจ้งแก่เครื่องอื่นๆ ว่าจะหยุดการทำงานเป็นระยะเวลาเท่าไร จึงจะมาตรวจสอบว่ามีข้อมูลส่งมาหรือไม่ ถ้าตรวจสอบแล้วมีข้อความมาเครื่องผู้รับจะได้รับแจ้งด้วยวิธีการบรอดคาส (broadcast)

2.2 เราติ้งโปรโตคอลบนเครือข่ายเคลื่อนที่เฉพาะกิจ

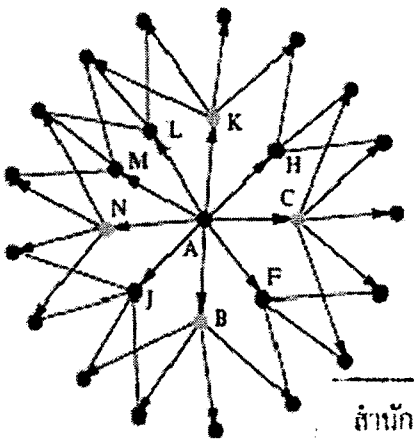
ก่อนการส่งข้อมูลจากต้นทางไปยังปลายทางในเครือข่าย โหนดจะต้องรู้ว่าจะต้องส่งข้อมูลไปตามเส้นทางใดในเครือข่าย โดยเราติ้งโปรโตคอลจะทำหน้าที่ในการค้นหาเส้นทางที่เหมาะสมที่สุดในการส่งข้อมูล เราแบ่งประเภทของเราติ้งโปรโตคอลสำหรับเครือข่ายเคลื่อนที่เฉพาะกิจไว้ 2 ประเภทหลักๆ คือ

2.2.1 โปรแอ็กทีฟเราติ้งโปรโตคอลหรือเทเบิ้ลไดร์เว่น (Pro-active Routing Protocol or Table-driven) เราติ้งโปรโตคอลในกลุ่มนี้จะค้นหาเส้นทางระหว่างโหนดไปยังทุกโหนดปลายทางที่อยู่ในเครือข่ายเป็นระยะๆ อยู่ตลอดเวลาไม่ว่าโทโปโลจีจะเปลี่ยนแปลงหรือไม่ก็ตาม ข้อแตกต่างระหว่างแต่ละเราติ้งโปรโตคอลประเภทนี้คือ วิธีการอัพเดทเราติ้ง การตรวจสอบเราติ้ง และข้อมูลที่เก็บไว้ในตารางเราติ้ง (Routing Table) ตัวอย่างของเราติ้งโปรโตคอลประเภทนี้ได้แก่

2.2.1.1 ดีเอสดีวี (Highly Dynamic Destination-Sequenced Distance Vector routing protocol – DSDV) [1] ใช้วิธีดิสแทนซ์เว็กเตอร์ (Distance Vector) ในการหาเส้นทางที่สั้นที่สุดเพียงเส้นทางเดียว เส้นทางที่ได้จากดีเอสดีวีสามารถรับประกันได้ว่าไม่มีโหนดซ้ำในเส้นทาง (No loop) มีการอัพเดทข้อมูลเส้นทาง 2 วิธีคือ 1) อัพเดทข้อมูลทั้งหมด (Full dump update) วิธีการนี้จะส่งข้อมูลเราติ้ง (Routing Information) ทั้งหมดออกไป และอีกวิธีคือ 2) อัพเดทเฉพาะข้อมูลที่เปลี่ยนแปลง (Incremental) จะส่งเฉพาะข้อมูลที่เปลี่ยนแปลงหลังจากการส่งข้อมูลทั้งหมดไป แต่ดีเอสดีวียังคงทำให้เกิดโอเวอร์เฮด (Overhead) จำนวนมากกับเครือข่าย เนื่องจากดีเอสดีวีต้องมีการอัพเดทข้อมูล

เราติ้งตามระยะเวลาที่กำหนด โดยมีโอเวอร์เฮดเป็น $O(N^2)$ ทำให้ดีเอสดีวีไม่เหมาะกับเครือข่ายเคลื่อนที่เฉพาะกิจที่มีโหนดจำนวนมาก เพราะต้องใช้แบนวิดท์ในการอัพเดทมาก

2.2.1.2 โอแอลเอสอาร์ (Optimized Link State Routing Protocol - OLSR) [2] ใช้หลักการการหาเส้นทางด้วยวิธีลิงค์สเตท (Link State) แต่โอแอลเอสอาร์ปรับปรุงวิธีการประกาศลิงค์สเตทจากการที่เดิมทุกโหนดจะต้องประกาศลิงค์สเตทของตนเองให้กับโหนดอื่นๆ ในเครือข่ายทั้งหมด โดยการให้โหนดบางโหนดทำหน้าที่ในการบรอดแคสข้อมูลลิงค์สเตท เราเรียกโหนดเหล่านี้ว่ามัลติพอยท์ดีสทรีบิวชั่นรีเลย์หรือเรียกสั้นๆ ว่าแอ็มพีอาร์ (Multipoint Distribution Relays – MPRs) แอ็มพีอาร์เป็นโหนดที่ถูกเลือกโดยโหนดเพื่อนบ้านที่อยู่ในระยะ 2 ฮ็อป ว่าทุกๆ โหนดสามารถรับข้อความที่บรอดแคสโดยโหนดนี้ได้ ซึ่งวิธีการนี้จะช่วยลดโอเวอร์เฮดลงเป็นอย่างมาก ตัวอย่างเช่น ในรูป โหนด A สามารถเลือกโหนด B, C, K และ N เป็นแอ็มพีอาร์เนื่องจากโหนดเหล่านี้ครอบคลุมทุกโหนดที่อยู่ 2 ฮ็อปถัดไป แต่ละโหนดจะเลือกเส้นทางที่มีจำนวนฮ็อปน้อยที่สุดเป็นเส้นทางที่ดีที่สุด ไปยังปลายทางแต่ละจุด โดยใช้ข้อมูลโทโปโลจีที่มีอยู่



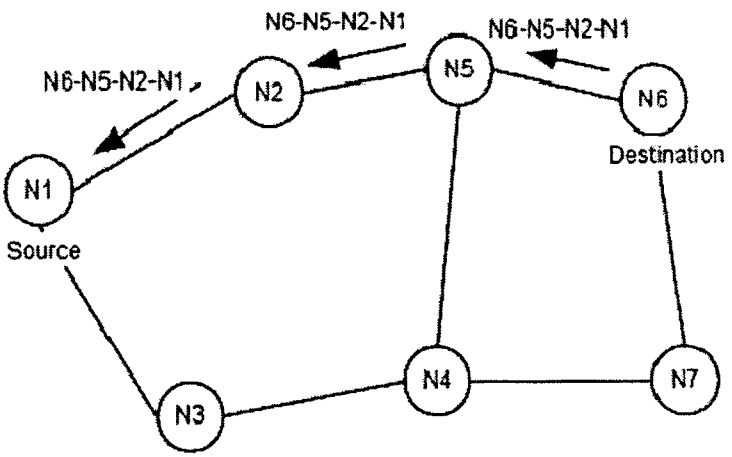
รูปที่ 2.6 มัลติพอยท์รีเลย์โหนด

2.2.2 Reactive Routing Protocol (On-demand) เราติ้งโปรโตคอลประเภทนี้จะค้นหาเส้นทาง เมื่อโหนดต้องการจะส่งข้อมูลเท่านั้น ข้อเสียของเราติ้งโปรโตคอลประเภทนี้ คือ โหนดจะต้องรอให้เราติ้งโปรโตคอลค้นหาเส้นทางเสร็จก่อนจึงจะสามารถส่งข้อมูลออกไปได้ ตัวอย่างของเราติ้งโปรโตคอลประเภทนี้ได้แก่

2.2.2.1 ดีเอสอาร์ (Dynamic Source Routing – DSR) ใช้หลักการของซอร์สเราติ้งในการค้นหาเส้นทาง โดยที่แต่ละแพ็กเกจจะมีข้อมูลของเส้นทางไปยังปลายทางที่สมบูรณ์ และในดีเอสอาร์แต่ละโหนดจะมีทำแคชเพื่อเก็บรักษาเส้นทางที่ได้เรียนรู้มาด้วย การหาเส้นทางของดีเอสอาร์แบ่งการทำงานออกเป็น 2 ช่วง 1) เราดิสโควเวอร์รี่ (Route Discovery) และ 2) เราแมน

เทนแนนซ์ (Route Maintenance) เมื่อโหนดต้องการที่จะส่งข้อมูล โหนดจะตรวจสอบแคชของตัวเองก่อน ถ้ามีเส้นทางที่ต้องการ โหนดต้นทางจะรวมข้อมูลของเส้นทาง (Routing Information) ไปไว้ในแพ็กเกจที่จะส่งก่อนที่จะส่งไป แต่ถ้าไม่มีเส้นทางที่ต้องการ โหนดต้นทางจะเริ่มทำเราดิสโควเวอร์รี่โดยการบรอดคาสเราร์เควสต์แพ็กเกจ ในเราร์เควสต์แพ็กเกจประกอบไปด้วยแอดเดรสของโหนดต้นทางและโหนดปลายทาง และยูนีคนัมเบอร์ของการรีเควสต์ โหนดที่ได้รับเราร์เควสต์จะตรวจสอบแคชของตนเอง ถ้าไม่มีเส้นทางไปยังปลายทาง โหนดจะต่อแอดเดรสของตัวเองไว้ในเราร์เควสต์แพ็กเกจแล้วจึงส่งต่อไปยังโหนดเพื่อนบ้าน เพื่อจำกัดโอเวอร์เฮดของการส่งเราร์เควสต์ โหนดจะทำอย่างนี้ก็ต่อเมื่อโหนดไม่เคยได้รับเราร์เควสต์นี้มาก่อนและไม่มีแอดเดรสของมันอยู่ในแพ็กเกจนั้น และเมื่อเราร์เควสต์ไปถึงปลายทางหรือโหนดที่มีเส้นทางไปยังโหนดปลายทาง โหนดจะส่งเราร์พายกลับไป ถ้าโหนดที่ตอบกลับเป็นโหนดปลายทางมันจะรวบรวมแอดเดรสของดหนดที่เราร์เควสต์ถูกส่งผ่านมา หรือถ้าโหนดที่ตอบกลับเป็นโหนดที่มีเส้นทางไปยังโหนดปลายทาง มันจะรวบรวมแอดเดรสที่เราร์เควสต์ถูกส่งผ่านมาเข้ากับเส้นทางที่มีอยู่ในเราแคช หลังจากที่สร้างเราร์พายแล้ว โหนดที่สร้างจำเป็นต้องส่งเราร์พายกลับไปให้โหนดต้นทางมี 3 วิธีที่จะส่งเราร์พายกลับไป คือ 1) โหนดมีเส้นทางไปยังต้นทางพร้อมอยู่แล้ว 2) เครือข่ายมีลิงค์เป็นแบบสมมาตร (Symmetric Link or bi-directional) เราร์พายจะถูกส่งกลับไปในเส้นทางที่เราร์เควสต์ถูกส่งมา 3) ถ้าลิงค์เป็นแบบไม่สมมาตร (Asymmetric Link or uni-directional) โหนดจะเริ่มทำเราดิสโควเวอร์รี่กลับไปหาโหนดต้นทาง โดยจะส่งเส้นทางที่ได้ค้นพบกลับไปในเราร์เควสต์ใหม่นี้

เมื่อดาต้าลิงค์เลเยอร์ตรวจพบการเชื่อมต่อที่ขาดหายไป เราเออเรอร์ (ROUTE_ERROR) จะถูกส่งกลับไปยังต้นทาง และเมื่อโหนดต้นทางได้รับเราเออเรอร์แล้ว โหนดต้นทางจะทำเราดิสโควเวอร์รี่อีกครั้ง และทุกเส้นทางที่มีลิงค์นี้อยู่จะถูกลบออกไปจากแคชของโหนดระหว่างทางทันทีที่เราเออเรอร์ถูกส่งไปยังต้นทาง



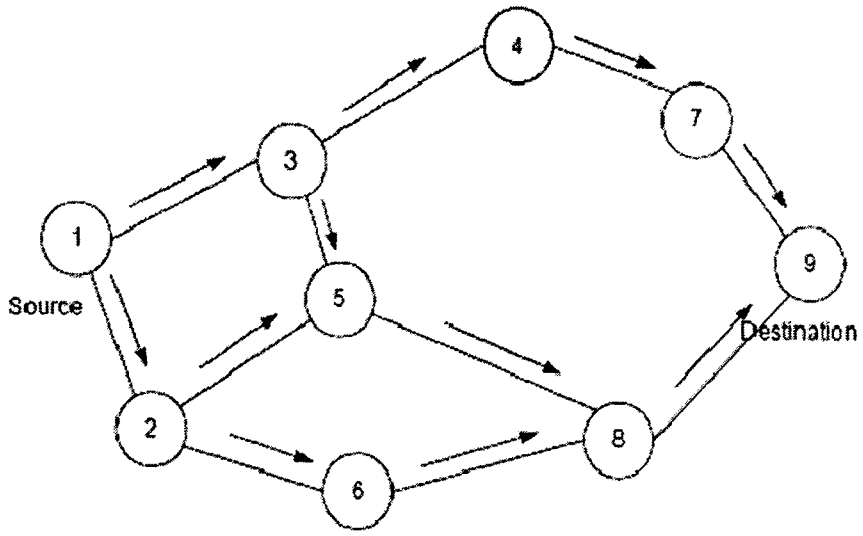
รูปที่ 2.7 เราร์พายที่ประกอบด้วยเส้นทางการส่งข้อมูลของดีเอสอาร์

2.2.2.2 เอโอดีวี (Ad-Hoc On-demand Distance Vector – AODV) [3] เป็นเราติ้งโปรโตคอลที่พัฒนามาจากดีเอสดีวี โดยลดจำนวนครั้งของการบรอดคาสลงจากเดิมที่เป็นการบรอดคาสตามคาบเวลา มาเป็นการบอรดคาสตามความต้องการ โหนดที่ไม่อยู่ในเส้นทางที่ถูกเลือกก็ไม่ต้องเข้าร่วมกับการแลกเปลี่ยนข้อมูลเราติ้ง เมื่อโหนดต้นทางต้องการที่จะส่งข้อมูลหาโหนดปลายทางและโหนดยังไม่มีเส้นทางในการส่งข้อมูล ข้อมูลเราติ้งที่แต่ละโหนดเก็บไว้คือค่าเน็กฮ็อป (Next Hop) ที่ไปยังปลายทางแต่ละจุด และข้อมูลนี้จะหมดอายุไม่ได้ใช้ภายในระยะเวลาที่กำหนด นอกจากนี้เอโอดีวียังปรับปรุงเดสทิเนชั่นซีเควนซ์นัมเบอร์ (Destination Sequence Number) ที่ใช้ในดีเอสดีวีให้เหมาะกับเราติ้งโปรโตคอลแบบออนดีมาน (On-demand)

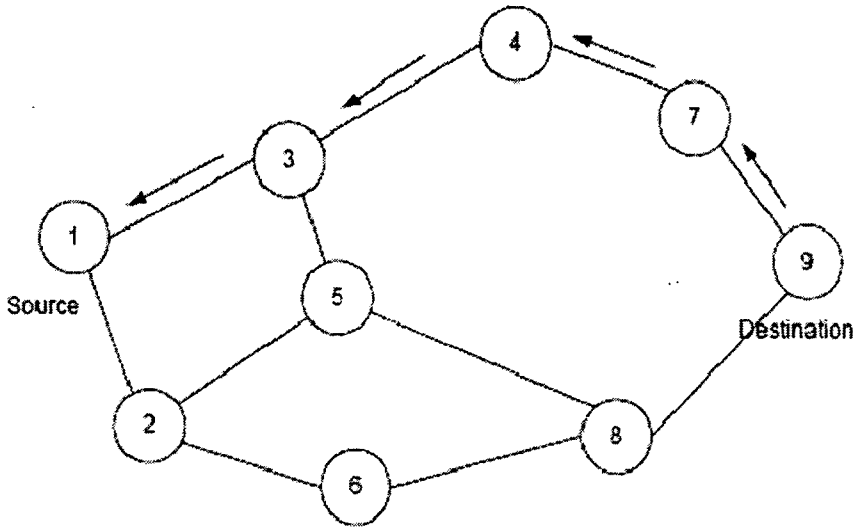
เมื่อโหนดต้นทางต้องการที่จะส่งข้อมูลไปหาโหนดปลายทาง แต่ยังไม่มีเส้นทางที่จะส่ง โหนดต้นทางจะเริ่มทำเราดิสคัฟเวอร์รี่ (Route Discovery) โดยการบรอดเคสเราติ้งเควสต์ (RREQ) ที่ประกอบไปด้วยที่อยู่ของโหนดต้นทางและโหนดปลายทาง บรอดคาสไอดี (Broadcast ID) และซีเควนซ์นันเบอร์ของปลายทางกับซีเควนซ์นัมเบอร์ของต้นทาง การใช้ซีเควนซ์นัมเบอร์เพื่อป้องกันเส้นทางที่วนซ้ำและเพื่อให้ได้เส้นทางที่ใหม่ที่สุดอยู่เสมอ เพื่อลดโอเวอร์เฮดในการฟลัดข้อมูล (Flooding overhead) โหนดจะยกเลิกเราติ้งเควสต์ที่เคยได้รับมาแล้ว ตอนเริ่มแรก RREQ จะมีค่าไทม์ทูลิฟ (Time to Live – TTL) ที่น้อย แต่ถ้ายังไม่สามารถหาปลายทางได้ค่า TTL จะเพิ่มขึ้นในเราติ้งเควสต์ต่อมา

ในเอโอดีวี แต่ละโหนดจะเก็บแคช (cache) ของเราติ้งเควสต์ที่ได้รับ และเก็บเส้นทางย้อนกลับไปหาต้นกำเนิดของเราติ้งเควสต์ เมื่อเราติ้งเควสต์ไปถึงโหนดปลายทางหรือถึงโหนดที่มีเส้นทางไปยังโหนดปลายทาง โหนดจะตรวจสอบว่าซีเควนซ์นัมเบอร์ของโหนดปลายทางที่ทราบอยู่แล้วกับที่ระบุมาในเราติ้งเควสต์ เพื่อที่ให้ได้เส้นทางที่ใหม่สุดอยู่เสมอ ถ้าซีเควนซ์นัมเบอร์ของปลายทางมีค่ามากกว่าหรือเท่ากับที่ได้รับในเราติ้งเควสซ์โหนดจะสร้างเราติ้งพาย (RREP) และส่งกลับไปตามเส้นทางเดิมไปยังโหนดต้นทาง เอโอดีวีจะใช้ได้กับลิงค์ที่สมมาตร (Symmetric links) เท่านั้น ในขณะที่โหนดระหว่างถามได้รับเราติ้งพายแต่ละโหนดจะอัพเดทตารางเน็กซ์ฮ็อปเกี่ยวกับโหนดปลายทางที่ได้รับ และเส้นทางที่ได้จากเราติ้งพายที่มีค่าซีเควนซ์นัมเบอร์ของโหนดปลายทางที่ต่ำกว่าจะถูกยกเลิกไป

เอโอดีวีใช้วิธีของเฮลโหลเมสเสจ (Hello message) ในการบอกโหนดเพื่อนบ้านถึงการดำรงอยู่ของตนเอง ดังนั้นสถานะของลิงค์ไปยังโหนดถัดไปจะสามารถตรวจสอบได้เสมอ เมื่อไรที่โหนดพบว่าลิงค์ขาดหายไปมันจะบรอดเคสเราเออเรอร์ (RERR) ไปให้กับโหนดเพื่อนบ้าน และโหนดเพื่อนบ้านจะส่งเราเออเรอร์ไปให้กับโหนดที่ได้รับผลกระทบจากลิงค์ที่หายไปนี้ เมื่อโหนดต้นทางได้รับเราเออเรอร์และโหนดยังคงต้องการติดต่อกับโหนดปลายทางต่อไป โหนดจะเริ่มทำเราดิสโควเวอร์รี่อีกครั้ง



รูปที่ 2.8 การทำเรารีเควสต์ของเอโอดีวี



รูปที่ 2.9 เส้นทางการส่งเรารีพายของเอโอดีวี

2.3 แนวคิดของงานวิจัย

เราเปรียบเทียบลักษณะเฉพาะของเครือข่ายเคลื่อนที่เฉพาะกิจกับเครือข่ายอินเทอร์เน็ต เนื่องจากเครือข่ายอินเทอร์เน็ตเป็นเครือข่ายที่มีความแพร่หลายทั้งในด้านการใช้งานและในด้านการวิจัย ลักษณะที่เรานำมาเปรียบเทียบ ได้แก่ ความเป็นอิสระจากกันของแต่ละโหนด ทรัพยากรและพฤติกรรมของโหนดในเครือข่าย การส่งต่อข้อมูลจากต้นทางไปยังปลายทาง และนอกจากนี้เครือข่ายเคลื่อนที่เฉพาะกิจยังมีลักษณะเฉพาะของตัวเองที่จำเป็นต้องคำนึงถึงสำหรับการทำงานวิจัย เช่น โหนดสามารถเคลื่อนที่ได้อย่างอิสระ ไม่มีการจัดการแบบรวมศูนย์

2.3.1 ความเป็นอิสระจากกันของโหนด เนื่องจากเครือข่ายเคลื่อนที่เฉพาะกิจเกิดจากการรวมตัวกันของโหนด ซึ่งแต่ละโหนดสามารถทำการเปลี่ยนแปลงภายในโหนดได้โดยไม่ส่งผลกระทบกับเครือข่าย หรือถ้าโหนดบางโหนดออกหรือเข้ามาร่วมกับเครือข่ายก็ไม่ส่งผลกระทบกับโหนดที่มีอยู่แล้ว เราพิจารณาความเป็นอิสระของโหนดใน 2 แง่มุม ได้แก่

1) ความเป็นอิสระจากกันในด้านของการจัดการ เครือข่ายอินเตอร์เน็ตเป็นเครือข่ายที่มีขนาดใหญ่ จึงยากที่จะจัดการเครือข่ายแบบรวมศูนย์ ดังนั้นเครือข่ายอินเตอร์เน็ตจะแยกกลุ่มของการจัดการออกเป็นออโตโนมัสซิสเต็ม (Autonomous System - AS) ซึ่งแต่ละออโตโนมัสซิสเต็มจะมีการจัดการที่แตกต่างกันไปตามวิธีการของตนเอง แต่ละออโตโนมัสซิสเต็มจะจัดเตรียมทรัพยากรและการเชื่อมต่อไว้ให้กับผู้ใช้ของตัวเอง และยอมส่งต่อข้อมูลจากออโตโนมัสซิสเต็มหนึ่งไปยังอีกออโตโนมัสซิสเต็มอื่นได้โดยมีเงื่อนไข เช่น การจ่ายค่าเชื่อมต่อระหว่างผู้ให้บริการอินเตอร์เน็ต เส้นทางสำหรับการส่งข้อมูลผ่านออโตโนมัสซิสเต็มได้มาจากเราติ้งโปรโตคอลที่เรียกว่า บีจีพี (Border Gateway Routing Protocol – BGP) ซึ่งหลักการหาเส้นทางของบีจีพีคือ จะเลือกเส้นทางตามนโยบายของผู้ดูแล (Policy-based Routing Protocol) ซึ่งขึ้นอยู่กับเงื่อนไขที่ได้ตกลงกันไว้ก่อนระหว่างแต่ละออโตโนมัสซิสเต็ม การเปลี่ยนแปลงภายในออโตโนมัสซิสเต็มจะไม่ส่งผลกระทบกับออโตโนมัสซิสเต็มอื่นๆ

เราสามารถเปรียบเทียบโหนดบนเครือข่ายเคลื่อนที่เฉพาะกิจ ได้กับออโตโนมัสซิสเต็ม เนื่องจากโหนดบนเครือข่ายเคลื่อนที่เฉพาะกิจสามารถจัดการการทำงานและทรัพยากรของตนเองได้อย่างอิสระโดยไม่ส่งผลกระทบกับโหนดอื่นๆ ในเครือข่าย

2) ความเป็นอิสระจากกันในด้านการจัดสรรทรัพยากร เนื่องจากโหนดบนเครือข่ายเคลื่อนที่เป็นของผู้ใช้แต่ละคน ดังนั้นผู้ใช้จึงมีสิทธิในการเปลี่ยนแปลงสิ่งต่างๆ ของอุปกรณ์ของตนเองโดยไม่ส่งผลกระทบกับการส่งข้อมูลผ่านเครือข่ายเคลื่อนที่เฉพาะกิจ

2.3.2 บทบาทหน้าที่และทรัพยากรของโหนดบนเครือข่าย เครือข่ายอินเทอร์เน็ตให้บริการโดยผู้ให้บริการอินเทอร์เน็ตหรือไอเอสพี (ISP – Internet Service Provider) ถ้าผู้ใช้ต้องการเชื่อมต่อเข้ากับเครือข่ายอินเทอร์เน็ตผู้ใช้จะต้องจ่ายค่าเชื่อมต่อให้กับผู้ให้บริการ ซึ่งทางผู้ให้บริการจะจัดเตรียมการเชื่อมต่อและทรัพยากรเครือข่าย เช่น การประมวลผลเส้นทาง แบนวิดท์ เป็นต้น และผู้ใช้บริการจำเป็นต้องจ่ายค่าบริการเพื่อที่จะใช้ทรัพยากรเหล่านี้ แต่บนเครือข่ายเคลื่อนที่เฉพาะกิจได้รับทรัพยากรเครือข่ายมาจากความร่วมมือของผู้ใช้แต่ละคน ดังนั้นผู้ใช้บริการจะต้องทำหน้าที่เป็นผู้ให้บริการเครือข่ายในเวลาเดียวกัน โดยไม่มีการคิดค่าใช้จ่าย ทรัพยากรของอุปกรณ์คอมพิวเตอร์พกพา เช่น พีดีเอ หรือแล็ปท็อป อุปกรณ์เหล่านี้จะมีทรัพยากรสำหรับการประมวลผล แบนวิดท์ที่จำกัดเมื่อเทียบกับเครือข่ายอินเทอร์เน็ต และนอกจากนี้อุปกรณ์เหล่านี้ทำงานโดยใช้พลังงานจากแบตเตอร์รี่เป็นหลัก ดังนั้นพลังงานจึงเป็นทรัพยากรที่

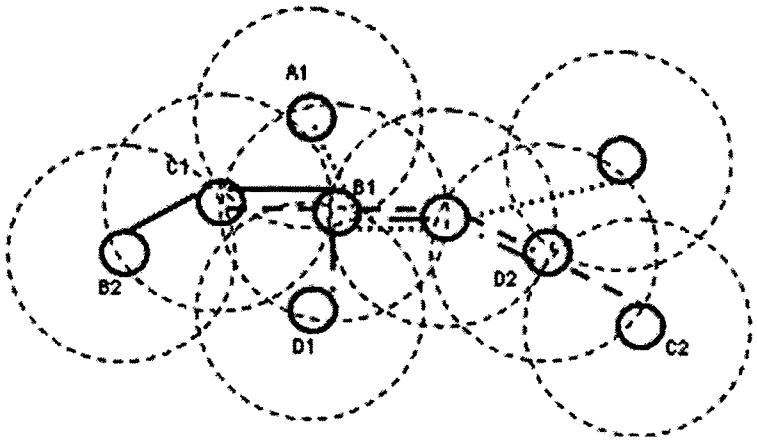
สำคัญที่สุดสำหรับเครือข่ายเคลื่อนที่เฉพาะกิจ โหนดจึงจำเป็นต้องจัดสรรทรัพยากรเหล่านี้อย่างมีประสิทธิภาพ

ดังนั้นการส่งข้อมูลบนเครือข่ายเคลื่อนที่เฉพาะกิจนอกจะคำนึงถึงลักษณะพิเศษของเครือข่ายแล้ว ยังควรจะคำนึงความเป็นอิสระจากกันของแต่ละโหนดด้วย เนื่องจากเราสามารถนำเครือข่ายเคลื่อนที่เฉพาะกิจมาให้บริการในสถาวะแวดล้อมที่ผู้ใช้มีความเป็นอิสระจากกันสูง เช่น การให้บริการในบริเวณสนามบิน เป็นต้น เนื่องจากการให้บริการในลักษณะนี้ผู้ใช้จะให้ความร่วมมือกับเครือข่ายอย่างไม่เต็มที่ เพราะต้องการที่จะสงวนทรัพยากรของตนเองไว้สำหรับการส่งข้อมูลของตนเองโดยไม่ยอมส่งต่อข้อมูลให้กับโหนดอื่นๆ ซึ่งแตกต่างกับการนำเครือข่ายเคลื่อนที่เฉพาะกิจมาใช้งานในบริเวณที่เกิดภัยพิบัติ หรือในหน่วยงานทางทหารที่ทุกโหนดร่วมมือร่วมใจกับอย่างเต็มที่

2.4 พฤติกรรมการเห็นแก่ตัวของโหนดและการจูงใจโหนดที่เห็นแก่ตัว

เนื่องจากการส่งข้อมูลบนเครือข่ายเคลื่อนที่เฉพาะกิจ เป็นการส่งข้อมูลแบบมัลติฮ็อป (Multi-hop) ซึ่งโหนดระหว่างทางจะต้องส่งต่อข้อมูลไปเป็นทอดๆ จนกว่าข้อมูลจะไปถึงปลายทาง สำหรับโหนดที่ต้องการที่จะรักษาพลังงานของตัวเองไว้ โหนดจะปฏิเสธที่จะส่งต่อข้อมูลของโหนดอื่น โหนดเหล่านี้จะใช้พลังงานไปกับการรับ-ส่งข้อมูลของตัวเองเท่านั้น ซึ่งพฤติกรรมนี้เป็นพฤติกรรมที่เห็นแก่ตัว (Selfish Behavior) และส่งผลกระทบต่ออัตราการส่งข้อมูลสำเร็จของเครือข่าย ดังนั้นจึงมีงานวิจัยจำนวนมากศึกษาเกี่ยวกับวิธีการตรวจจับโหนดที่มีพฤติกรรมเห็นแก่ตัว และคิดค้นวิธีการจูงใจให้ทุกโหนดให้ความร่วมมือในการส่งต่อข้อมูล รวมทั้งกำหนดบทลงโทษแก่โหนดที่ไม่ให้ความร่วมมือ

แต่การไม่ให้ความร่วมมือในการส่งต่อข้อมูลในเครือข่าย มีด้วยกันหลายสาเหตุ เช่น จากรูปที่ 2.10 มีโหนดอยู่ทั้งหมด 9 โหนด มีการเชื่อมต่ออยู่ 4 คู่ คือ ระหว่างโหนด A1 กับ A2 โหนด B1 กับโหนด B2 โหนด C1 กับโหนด C2 และโหนด D1 กับโหนด D2 โหนด B1 จะต้องทำหน้าที่เป็นปลายทางการสื่อสารกับโหนด B2 และจะต้องส่งต่อข้อมูลให้กับการสื่อสารอีก 3 คู่ในเวลาเดียวกัน ส่งผลให้พลังงานของโหนด B1 สูญเสียพลังงานสูงกว่าโหนดอื่นในเครือข่าย ในขณะที่โหนดที่อยู่รอบนอกของเครือข่ายไม่ต้องใช้พลังงานในการส่งต่อข้อมูล แสดงให้เห็นถึงความไม่เท่าเทียมกันถึงโอกาสในการส่งต่อข้อมูล เนื่องจากโหนด B1 เสียพลังงานกับการส่งต่อข้อมูลของโหนดอื่นเป็นจำนวนมาก และโหนด B1 มีความต้องการที่จะส่งข้อมูลของตัวเองด้วย แต่โหนด B1 นั้นมีพลังงานอยู่จำนวนจำกัด ดังนั้นโหนด B1 อาจจะปฏิเสธการส่งข้อมูลของโหนดอื่นเพื่อเก็บพลังงานไว้ใช้ในการส่งข้อมูลของตนเอง ซึ่งพฤติกรรมแบบนี้ของโหนด B1 อาจทำให้อัตราการส่งข้อมูลสำเร็จ (Throughput) ของเครือข่ายลดลงได้ ในกรณีนี้เราไม่ควรเรียกโหนด B1 ว่าเป็นโหนดที่เห็นแก่ตัว



รูปที่ 2.10 โทโปโลจีที่แสดงถึงความไม่เท่าเทียมกันในการทำงานของโหนด

งานวิจัยที่ผ่านมา ยังไม่มีการศึกษาถึงการให้ความร่วมมือกับเครือข่ายของโหนดอย่างละเอียด เช่น การศึกษาถึงพลังงานที่โหนดใช้ไปกับกิจกรรมต่างๆ เมื่อให้ความร่วมมือกับเครือข่ายเคลื่อนที่เฉพาะกิจ ดังนั้นการศึกษาพฤติกรรมความร่วมมือในการส่งต่อข้อมูลของโหนดบนเครือข่ายเคลื่อนที่เฉพาะกิจจึงมีความจำเป็น งานวิจัยชิ้นนี้ศึกษาเกี่ยวกับผลกระทบต่อโหนดเนื่องจากการให้ความร่วมมือกับเครือข่าย และอัตราการส่งข้อมูลของเครือข่ายที่โหนดมีพฤติกรรมในการให้ความร่วมมือกับเครือข่ายในระดับที่ต่างกัน งานวิจัยนี้ใช้พลังงานเป็นตัวชี้วัดผลกระทบต่อโหนด เนื่องจากพลังงานเป็นทรัพยากรที่สำคัญที่สุดของเครือข่ายเคลื่อนที่เฉพาะกิจ

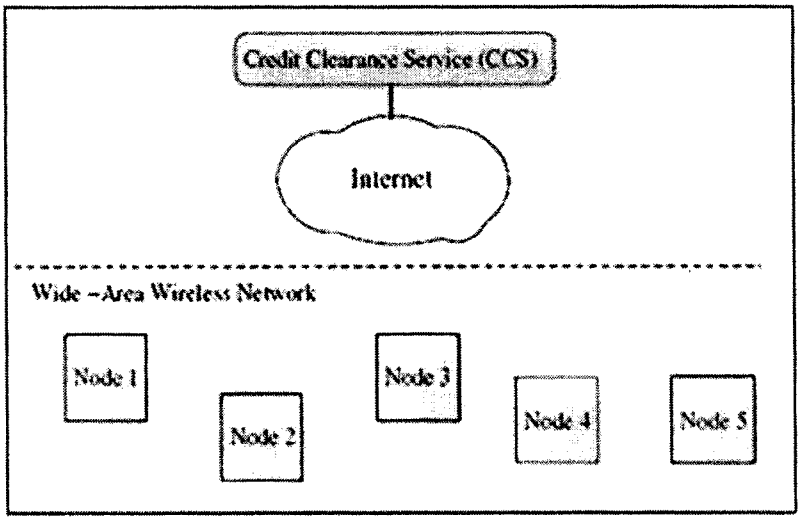
โหนดที่มีพฤติกรรมที่ไม่ดีต่อเครือข่าย (Misbehavior Node) บนเครือข่ายเคลื่อนที่เฉพาะกิจ สามารถแยกได้เป็น 2 ประเภท คือ 1) โหนดที่มีพฤติกรรมเห็นแก่ตัว (Selfish Node) โหนดจะไม่ให้ความร่วมมือกับเครือข่ายในการส่งต่อข้อมูลของโหนดอื่น และพยายามทำให้ตัวเองได้รับประโยชน์สูงสุดจากเครือข่ายอยู่เสมอ การที่โหนดไม่ให้ความร่วมมือในการส่งต่อข้อมูลเพราะโหนดต้องการที่จะรักษาพลังงานของตนเองไว้ แล้วใช้พลังงานนี้ไปกับการรับ-ส่งข้อมูลของตนเองเท่านั้น ถึงแม้ว่าพฤติกรรมของโหนดที่เห็นแก่ตัวเหล่านี้จะทำให้อัตราการส่งข้อมูลสำเร็จของเครือข่ายลดลง แต่โหนดไม่ได้มีเจตนาในการทำให้เครือข่ายมีประสิทธิภาพแย่ลง เพราะโหนดที่เห็นแก่ตัวนี้คำนึงถึงผลประโยชน์ของตัวเองเป็นหลักเท่านั้น ซึ่งแตกต่างจากโหนดประเภทที่ 2 คือโหนดที่ประสงค์ร้ายต่อเครือข่าย (Malicious Node) ที่ต้องการทำให้ประสิทธิภาพของเครือข่ายลดลงโดยตั้งใจ โดยมิได้คำนึงถึงประโยชน์ของตนเอง โหนดจะก่อกวนเครือข่ายในรูปแบบต่างๆ เช่น พยายามส่งข้อมูลออกมาเพื่อให้เกิดการชนกันของข้อมูล หรือการจำกัดรัศมีการส่งของโหนดตัวเอง เพื่อหลอกโหนดต้นทางว่าได้ส่งข้อมูลไปหาโหนดปลายทางแล้ว พฤติกรรมเหล่านี้บางพฤติกรรมเราสามารถสร้างกลไกในการป้องกันการจู่โจม แต่บางวิธีเราก็ไม่สามารถป้องกันได้ ดังนั้นจึงมีงานวิจัยจำนวนหนึ่งที่ต้องการจูงใจให้โหนดที่เห็นแก่ตัว ให้ความร่วมมือ

กับการส่งต่อข้อมูลของโหนดอื่นๆ และกำหนดบทลงโทษให้กับโหนดที่ไม่ให้ความร่วมมือกับเครือข่ายหรือโหนดที่มีพฤติกรรมประสงค์ร้ายบางพฤติกรรมเท่านั้น งานวิจัยเหล่านี้ออกเป็น

2.4.1 วิธีที่อิงตามชื่อเสียงของโหนด (Reputation Based) [6] นำเสนอวิธีการในการตรวจจับโหนดที่มีพฤติกรรมไม่ดีและกำหนดบทลงโทษ โดยใช้วอทช์ด็อก (watchdog) และพาธราเทอร์ (pathrater) วอทช์ด็อกมีหน้าที่ในการตรวจจับโหนดที่มีพฤติกรรมไม่ดี โดยหลังจากที่โหนดส่งข้อมูลออกไปแล้ว โหนดจะยังคงเก็บข้อมูลไว้ในบัฟเฟอร์ (buffer) ต่อไป และจะคอยฟังว่าโหนดที่รับข้อมูลต่อไปนั้นได้ส่งต่อข้อมูลไปให้โหนดถัดไปหรือไม่ ถ้ามีการส่งข้อมูล วอทช์ด็อกก็จะลบข้อมูลที่ส่งแล้วออกจากบัฟเฟอร์ แต่ถ้าไม่มีการส่งข้อมูลภายในระยะเวลาที่กำหนด (timeout) วอทช์ด็อกจะให้คะแนนความล้มเหลวของโหนดนี้เพิ่มขึ้น (failure) จนเมื่อค่าความล้มเหลวสูงขึ้นจนถึงระดับที่กำหนดไว้ วอทช์ด็อกจะส่งข้อความไปบอกโหนดต้นทางว่าโหนดที่ถูกจับตามองเป็นโหนดที่มีพฤติกรรมไม่ดี ทำให้โหนดอื่นๆ มีข้อมูลของโหนดที่ไม่ดีเหล่านี้อยู่ ส่วนพาธราเทอร์ทำหน้าที่ในการเลือกเส้นทางโดยหลีกเลี่ยงโหนดที่มีพฤติกรรมไม่ดี โดยใช้ข้อมูลจากวอทช์ด็อก และถ้าโหนดไม่ดีเหล่านี้ต้องการส่งข้อมูลไปในเครือข่าย พาธราเทอร์ของโหนดที่มีข้อมูลจะปฏิเสธในการส่งข้อมูลของโหนดไม่ดีเป็นการลงโทษโหนดที่ไม่ยอมส่งข้อมูลให้โหนดอื่น [7] ได้นำเสนอวิธีการค้นหาโหนดที่เห็นแก่ตัวโดยปรับปรุงข้อเสียหลายอย่างของวอทช์ด็อก เนื่องจากวอทช์ด็อกใช้โหนดเพียงโหนดเดียวในการจับตาดูโหนดข้างเคียงและการตัดสินความผิด แต่การจับตาดูเพียงโหนดเดียวอาจไม่ถูกต้องเนื่องจากการชนกันของคลื่นวิทยุในเครือข่ายไร้สาย วิธีการนี้จึงนำเสนอให้โหนดเพื่อนบ้านของโหนดที่ถูกจับตาดูช่วยกันจับตาดูและลงคะแนนตัดสินความผิด และถ้าโหนดถูกตัดสินว่ามีความผิดแล้วโหนดเพื่อนบ้านจะปฏิเสธการส่งต่อข้อมูลของโหนดนั้นในช่วงระยะเวลาหนึ่งเพื่อเป็นการลงโทษ และจูงใจให้โหนดนั้นเลิกพฤติกรรมที่เห็นแก่ตัว แต่ถ้าโหนดที่ถูกจับตามองยังคงมีพฤติกรรมที่เห็นแก่ตัวอยู่มันจะถูกปฏิเสธการต่อข้อมูลจากโหนดเพื่อนบ้านเป็นระยะเวลาที่ยาวนานกว่าเดิม และวิธีการนี้ได้นำเสนอวิธีการแก้ไขปัญหา เรื่องโหนดที่อยู่ตรงกลางเครือข่ายจะต้องทำหน้าที่ในการส่งต่อข้อมูลของโหนดอื่นมากกว่าโหนดที่อยู่รอบนอก โหนดที่อยู่ตรงกลางนี้จะเสียพลังงานมากกว่าโหนดที่อยู่รอบนอก โดยการให้โหนดประกาศระดับพลังงานที่เหลืออยู่ให้โหนดข้างเคียงทราบ โหนดข้างเคียงจะประเมินระยะเวลาที่เหลืออยู่ของโหนดนั้น และจะยอมส่งต่อข้อมูลให้โหนดนั้นตามระยะเวลาที่ได้ประเมินไว้

2.4.2 วิธีการจูงใจโหนดหรือการใช้เงินจำลอง หลักการคือระบบจะสมมติเงินจำลองขึ้นมา และกำหนดว่าโหนดจะต้องจ่ายเงินเป็นค่าจ้างในการส่งต่อข้อมูล สำหรับโหนดที่ส่งต่อข้อมูลของโหนดอื่นจะได้รับเงินมาไว้สำหรับใช้จ่ายในการส่งข้อมูลของตัวเอง และโหนดจะพยายามสร้างเครดิตให้มากที่สุดโดยที่ยังรักษาระดับพลังงานให้อยู่ในเกณฑ์ที่ยังสามารถส่งข้อมูล

ได้ ซึ่งแต่ละวิธีมีข้อกำหนดเกี่ยวกับเครดิตที่แตกต่างกัน เช่น [8] นำเสนอสไปรท์ เป็นวิธีการที่จูงใจผู้ใช้ให้ความร่วมมือในการส่งต่อข้อมูล และรายงานการกระทำของตนเองอย่างซื่อสัตย์ วิธีการคือ เมื่อโหนดได้รับเมสเสจ โหนดจะหาเมสเสจไดเจสท์ (Message Digest) ของเมสเสจนั้นเพื่อใช้เป็นในรับของ (receipt) และนำใบรับของนี้ไปขึ้นเงินกับเครดิตเคลียร์แรนซ์เซอร์วิส (Credit Clearance Service – CCS) สไปรท์กำหนดว่าโหนดที่ส่งข้อมูลได้สำเร็จจะได้รับค่าตอบแทนที่สูงกว่าโหนดที่ไม่สำเร็จ และผู้ส่งจะเป็นผู้จ่ายให้กับโหนดระหว่างทางทั้งหมด ซึ่งค่าใช้จ่ายที่ผู้ส่งต้องจ่ายจะสูงกว่าค่าใช้จ่ายที่โหนดระหว่างทางทั้งหมดได้รับรวมกัน เพื่อป้องกันการร่วมมือกันโกงของโหนดระหว่างทาง สไปรท์เป็นวิธีแรกที่แต่ละโหนดไม่จำเป็นจะต้องมีฮาร์ดแวร์ที่สามารถทนต่อการติดสินบนได้ และระบบทั้งหมดทำงานบนซอฟต์แวร์



รูปที่ 2.11 สถาปัตยกรรมของสไปรท์

การจูงใจโหนดเพื่อให้ความร่วมมือกับเครือข่ายมากขึ้น ยังมีอีกหลายประเด็นที่จำเป็นต้องคำนึง ดังต่อไปนี้

2.4.1.1 การใช้เซอร์ติฟิเคต (certificate) เนื่องจากโหนดในเครือข่ายเคลื่อนที่เฉพาะกิจ สามารถเชื่อมต่อหรือยกเลิกการเชื่อมต่อกับเครือข่ายได้ตลอดเวลา รวมทั้งโหนดสามารถเคลื่อนที่ภายในเครือข่ายได้อย่างอิสระ และเป็นเครือข่ายที่ไม่มีการจัดการแบบรวมศูนย์ จึงทำให้ไม่เหมาะที่จะมีเซอร์ติฟิเคตออโธริตี้ (Certificate Authority - CA) ที่ต้องทำหน้าที่เป็นศูนย์กลางอยู่ตลอดเวลา ดังนั้นจึงไม่มีโหนดใดเหมาะสมที่จะทำหน้าที่เป็นเซอร์ติฟิเคตออโธริตี้เซอร์เวอร์

2.4.1.2 การใช้เครดิต (Credit-based) ในระบบการจูงใจ โหนดจะต้องส่งต่อข้อมูลของโหนดอื่นเพื่อให้ได้รับเครดิตไว้ใช้สำหรับการส่งข้อมูลของตัวเอง การจัดการเครดิตในเครือข่ายเคลื่อนที่เฉพาะกิจให้ถูกต้องและน่าเชื่อถือเป็นเรื่องที่ยุ่งยากเนื่องจากการที่เครือข่าย

เคลื่อนที่เฉพาะกิจไม่มีการจัดการแบบรวมศูนย์ และโหนดในเครือข่ายไร้สายสามารถเชื่อมต่อและยกเลิกการเชื่อมต่อได้ตลอดเวลา การที่เครือข่ายจะจดจำค่าเครดิตของทุกโหนดไว้ตลอดเวลานั้นเป็นเรื่องยาก และพฤติกรรมของโหนดคือจะส่งต่อข้อมูลของโหนดอื่นเพื่อเพิ่มเครดิตให้ตัวเองให้ได้มากที่สุด จนกระทั่งพลังงานของโหนดเหลืออยู่ในระดับที่กำหนดโหนดจึงหยุดการส่งต่อข้อมูล ซึ่งวิธีการนี้อาจจะไม่ได้ผลอย่างดีที่สุดในหลายๆ กรณี เช่น โหนดที่ต้องการจะส่งข้อมูลแต่ไม่มีเครดิต และไม่อยู่ในตำแหน่งที่สามารถส่งต่อข้อมูลให้โหนดได้ การนำเครดิตมาใช้จะทำให้โหนดนี้ไม่สามารถส่งข้อมูลได้เลย

2.4.1.3 การจูงใจบางวิธีการ เช่น [8] เครือข่ายไร้สายแบบเฉพาะกิจจำเป็นต้องเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตเพื่อจัดการกับเครดิตของแต่ละโหนด ซึ่งการส่งข้อมูลบนเครือข่ายเฉพาะกิจไม่จำเป็นจะต้องติดต่อกับเครือข่ายอินเตอร์เน็ตเสมอไป อาจจะเป็นส่งข้อมูลกันระหว่างโหนดก็ได้ ดังนั้นถ้าส่วนการตรวจสอบเครดิตทำอยู่บนเครือข่ายอินเตอร์เน็ตแล้วจะเป็นการบังคับให้ทุกครั้งที่ใช้เครือข่ายเคลื่อนที่เฉพาะกิจ จะต้องติดต่อกับเครืออินเตอร์เน็ต หรือบางวิธีการ [6] [7] โหนดจำเป็นจะต้องจับตาดูการทำงานของโหนดข้างเคียง ดังนั้นโหนดจะต้องมีอินเทอร์เฟสการ์ดที่สามารถจับตาดูการทำงานของโหนดอื่นได้ (Promiscuous mode) ซึ่งการทำงานในโหมดนี้โหนดจะต้องเสียพลังงานส่วนนึงไปกับการจับตาดู

สำหรับงานวิจัยประเภทที่กำหนดบทลงโทษโดยการตัดโหนดที่ไม่ให้ความร่วมมือออกจากเครือข่ายเลย ทำให้โหนดเหล่านี้ไม่มีโอกาสที่จะกลับมาให้ความร่วมมือกับเครือข่ายอีกแล้ว ดังนั้นการแก้ปัญหาด้วยการจูงใจให้โหนดเหล่านี้หันมาให้ความร่วมกับเครือข่ายจึงเป็นเรื่องที่ดีกว่า และวิธีการจูงใจที่ได้รับความนิยมมากวิธีหนึ่งคือการใช้เงินจำลอง โดยโหนดจะได้รับเงินเมื่อส่งต่อข้อมูลของโหนดอื่นๆ โดยมีโหนดที่ได้รับประโยชน์จากการส่งต่อข้อมูลนี้เป็นผู้จ่ายเงิน ซึ่งโหนดที่ได้รับประโยชน์อาจจะเป็นโหนดต้นทางหรือโหนดปลายทางหรือทั้งสองโหนดก็ได้ขึ้นอยู่กับวิธีการของผู้ออกแบบ แต่วิธีการนี้ยังมีข้อเสียคือ ไม่ได้คำนึงความเท่าเทียมในการทำงานของโหนด ยกตัวอย่างเช่น โหนดต้องการจะให้ความร่วมมือในการส่งต่อข้อมูลกับเครือข่าย แต่โหนดไม่ได้รับการเลือกให้ทำหน้าที่ในการส่งข้อมูลต่อจากเราติ้งโปรโตคอลทำให้โหนดไม่มีโอกาสในการส่งต่อข้อมูลของโหนดอื่นเลย มีผลให้โหนดเหล่านี้ไม่มีเงินจำลองเพื่อที่ใช้ในการส่งข้อมูลของตนเองผ่านเครือข่าย และนอกจากนี้ควรคำนึงถึงความเป็นอิสระจากกันของแต่ละโหนดทำให้พฤติกรรมเครือข่ายของแต่ละโหนดแตกต่างกัน รวมถึงแรงจูงใจสำหรับการให้ความร่วมมือกับเครือข่ายที่ต่างกัน งานวิจัยที่ผ่านมายังไม่มีการศึกษาเกี่ยวกับผลประโยชน์ที่โหนดได้รับกับทรัพยากรที่โหนดเสียไป ซึ่งสิ่งเหล่านี้คือแรงจูงใจที่ทำให้โหนดให้ความร่วมมือกับเครือข่าย งานวิจัยชิ้นนี้ใช้พลังงานที่โหนดใช้ไปเหล่านี้ มาคำนวนหาค่าความยุติธรรมที่เกิดขึ้นในเครือข่ายเพื่อให้เห็นถึงผลประโยชน์ที่โหนดเสียและได้รับจากการเข้าร่วมเครือข่ายเคลื่อนที่เฉพาะกิจ ซึ่งเราสามารถนำค่าความยุติธรรมที่ได้มาวิเคราะห์เพื่อสร้างแรงจูงใจที่เหมาะสมกับโหนดในเครือข่ายได้

2.5 การทดลองแบบซิมมูเลชั่น

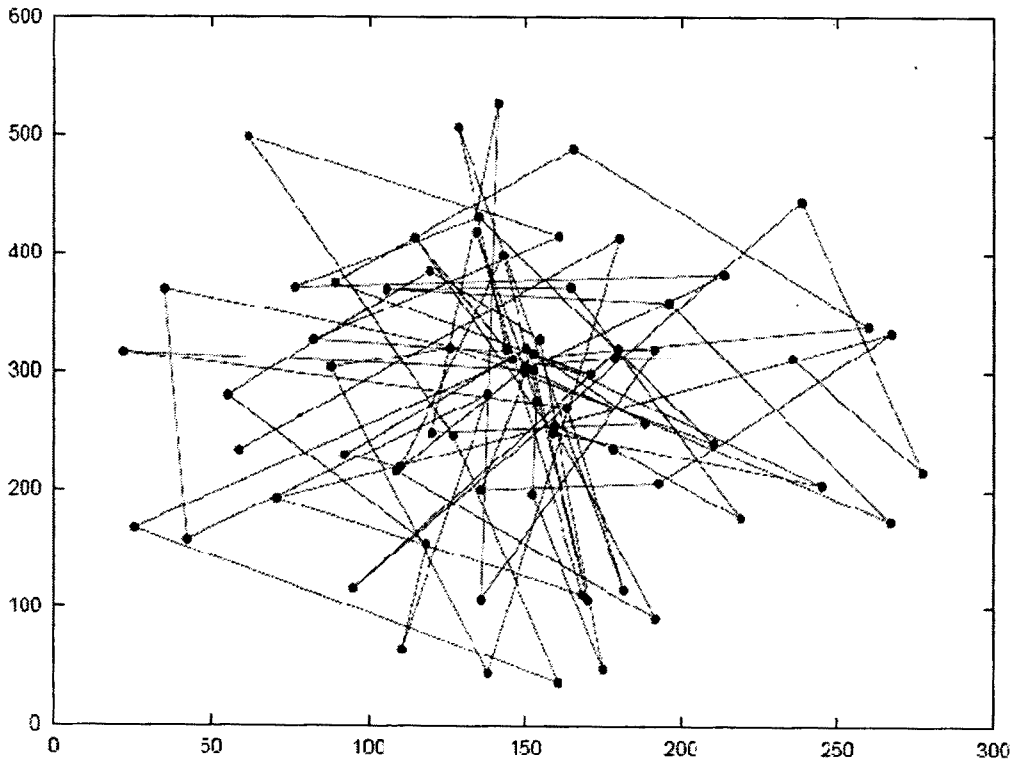
การทำซิมมูเลชั่น เป็นการทดลองวัดประสิทธิภาพของเครือข่ายวิธีการหนึ่ง แต่มีข้อดีในด้านประหยัดค่าใช้จ่ายและเวลากว่าการทำอีมูเลชั่น (Emulation) และการพัฒนาโปรโตไทป์ (Prototype) ที่มีการใช้ฮาร์ดแวร์จริงร่วมด้วย ซิมมูเลชั่นนั้นง่ายต่อการทดสอบวัดผลการประสิทธิภาพของเครือข่าย เมื่อมีการเปลี่ยนแปลงบางอย่างเกิดขึ้นในเครือข่าย เช่น เปลี่ยนหรือเพิ่มเติมโปรโตคอลในการทำงาน หรือเปลี่ยนโทโปโลจีของเครือข่าย เป็นต้น ซิมมูเลเตอร์สำหรับงานวิจัยทางด้านเครือข่ายมีหลายตัวด้วยกัน เช่น อ็อปเน็ต (Opnet) เอ็นเอสทู (NS2) ออมเน็ตพลัสพลัส (OMnet++) สำหรับงานวิจัยชิ้นนี้ทดลองโดยใช้ซิมมูเลเตอร์เอ็นเอสทู

เอ็นเอสทูเป็นซิมมูเลเตอร์ประเภทดิสครีตอีเวนต์ (Discrete Event) ที่ถูกพัฒนามาเพื่อใช้ในงานวิจัยทางด้านเครือข่าย ซึ่งแต่เดิมเป็นเครือข่ายแบบมีสายทั้งหมด และต่อมาได้มีการพัฒนาให้สามารถซิมมูเลชั่นเครือข่ายประเภทไร้สาย เช่น เครือข่ายแลนไร้สาย หรือเครือข่ายเคลื่อนที่เฉพาะกิจได้ โดยกลุ่มโมนาช (Monarch Group) เอ็นเอสทูเวอร์ชั่นปัจจุบัน (NS 2.31) ได้จัดเตรียมสิ่งแวดล้อมต่างๆ ที่จำเป็นสำหรับเครือข่ายเคลื่อนที่เฉพาะกิจ เช่น เราติ้งโปรโตคอลสำหรับเครือข่ายเคลื่อนที่เฉพาะกิจ โมบิลิตี้โมเดลไอทริปเปิลอี 802.11 แม็กโปรโตคอล ทำให้เอ็นเอสทูเป็นซิมมูเลเตอร์ที่ได้รับความนิยมสูงสำหรับงานวิจัยด้านเครือข่ายเคลื่อนที่เฉพาะกิจ [4]

2.5.1 โมบิลิตี้โมเดลสำหรับเครือข่ายเคลื่อนที่เฉพาะกิจ (MANET Mobility Model) เพื่อให้การทดลองได้ผลที่ใกล้เคียงกับการทำงานจริงมากที่สุด ดังนั้นจึงต้องมีการจำลองรูปแบบการเคลื่อนไหวของผู้ใช้ในเครือข่ายเคลื่อนที่เฉพาะกิจ (Mobility Model) เราแบ่งประเภทของแบบจำลองการเคลื่อนไหวของโหนดออกเป็น 2 ประเภทคือ 1) เทรส (Trace) คือ รูปแบบการเคลื่อนไหวที่ได้มาจากการใช้งานจริง ซึ่งจะทำให้ได้ข้อมูลที่ถูกต้องจริงๆ โดยเฉพาะเมื่อการสังเกตเกิดจากเครือข่ายขนาดใหญ่และใช้เวลาในการสังเกตนานพอสมควร แต่การจะสังเกตเพื่อให้ได้แบบการเคลื่อนที่ที่เหมาะสมกับแต่ละสถานการณ์เป็นเรื่องยาก ดังนั้นจึงมีโมบิลิตี้โมเดลอีกแบบนึงคือ 2) ซินเทติก (Synthetic) เป็นการจำลองการเคลื่อนไหวของโหนดให้เหมือนจริงมากที่สุดโดยไม่ต้องมีการเทรส การเคลื่อนไหวจะมีการเปลี่ยนแปลงความเร็วและทิศทางของโหนดจะเกิดขึ้นในเวลาที่เหมาะสมอย่างมีเหตุผล ตัวอย่างของโมบิลิตี้โมเดลประเภทนี้ ได้แก่

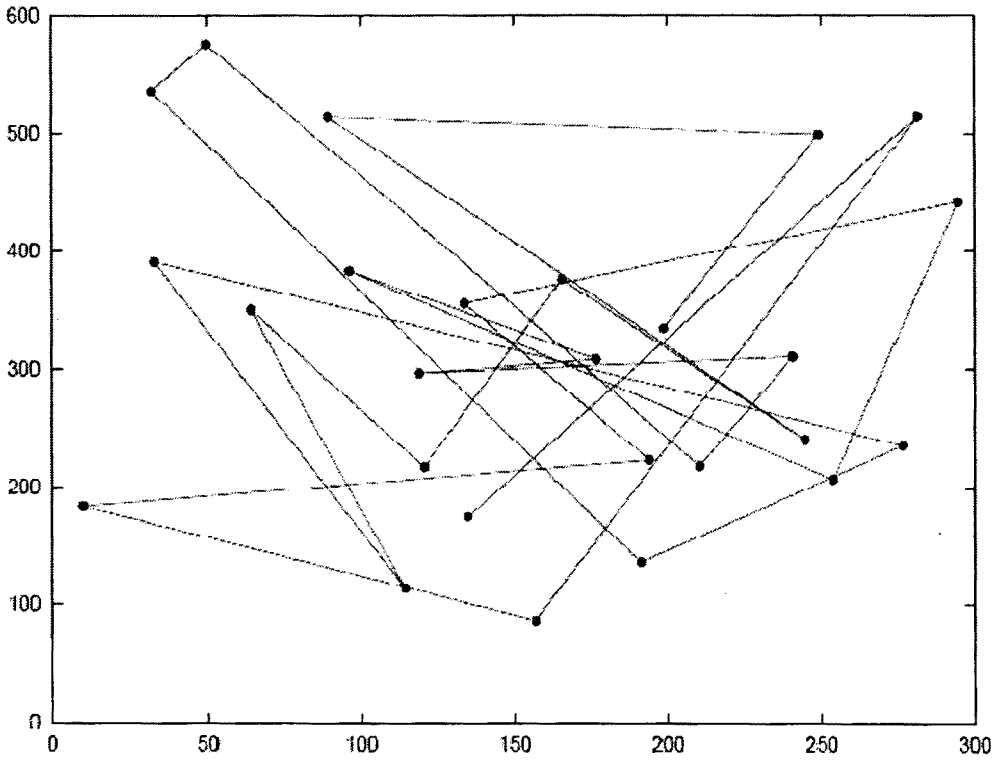
2.5.1.1 แรนดอมวอล์คโมบิลิตี้โมเดล (Random Walk Mobility Mode) ทุกโหนดจะเคลื่อนที่แบบที่ไม่สามารถคาดเดาได้ โหนดจะเคลื่อนออกจากที่อยู่ปัจจุบันไปยังที่อยู่ใหม่โดยสุ่มเลือกทิศทางและความเร็วในการเคลื่อนที่ โดยตัวเลขความเร็วที่สุ่มออกมาได้จะอยู่ในช่วงความเร็วต่ำสุดถึงความเร็วสูงสุดที่ได้กำหนดไว้แล้ว และทิศทางอยู่ในช่วง [0, 2¶] ถ้าโหนดเคลื่อนที่ไปถึงขอบของพื้นที่การทดลองโหนดจะเด้งออกจากขอบตามมุมที่ตกกระทบและเคลื่อนที่ต่อไป

ข้อดีของการเคลื่อนที่แบบนี้คือ ใช้หน่วยความจำน้อยเนื่องจากการกำหนดตำแหน่งและทิศทางของโหนดในปัจจุบันไม่จำเป็นต้องจดจำตำแหน่งที่ผ่านมา แต่ยังมีความไม่สมจริงคือโหนดอาจจะหยุดกระทันหันและเลี้ยวแบบหักมุมในทันที ตามรูปที่ 2.12



รูปที่ 2.12 การเคลื่อนที่แบบแรนดอมวอล์คในเทอมของเวลา

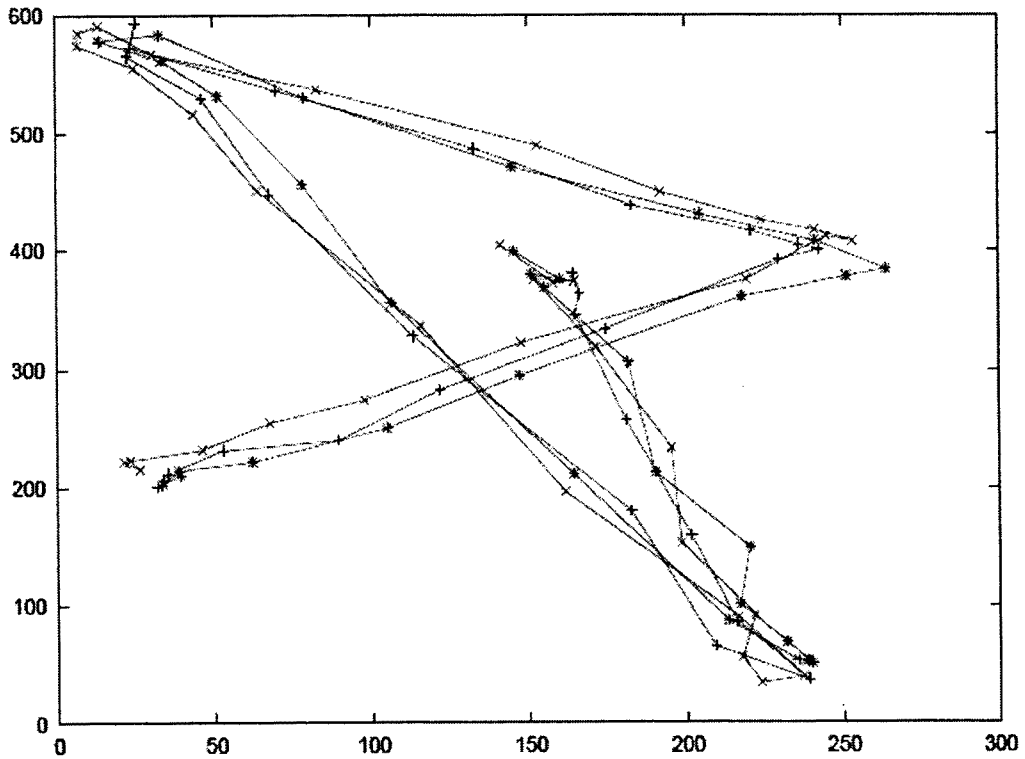
2.5.1.2 แรนดอมเวย์พอยต์โมบิลิตี้โมเดล (Random Waypoint Mobility Model) ปรับปรุงมากจากแรนดอมวอล์คโมบิลิตี้โมเดล โดยการเพิ่มเวลาหยุด (Pause Time) ในระหว่างการเปลี่ยนทิศทาง เมื่อโหนดหยุดครบกำหนดเวลาโหนดถึงจะสุ่มเลือกจุดหมายใหม่ที่อยู่ในพื้นที่การทดลอง และเลือกเวลาอย่างมีแบบแผนกระจายอยู่ในช่วง [minspeed, ,maxspeed] โหนดก็จะเคลื่อนที่ไปยังเป้าหมายด้วยความเร็วที่เลือกไว้ เมื่อไปถึงโหนดก็จะหยุดอยู่จบครบเวลาที่กำหนดแล้วจึงเริ่มการทำงานใหม่อีกครั้ง



รูปที่ 2.13 การเคลื่อนที่แบบแรนดอมเวย์พอยท์ในเทอมของเวลา

2.5.1.3 เรฟเฟอร์เรนซ์พอยต์กรุ๊ปโมบิลิตี้โมเดลหรืออาร์พีจีเอ็ม (Reference Point Group Mobility Model - RPGM) แสดงการเคลื่อนที่แบบเป็นกลุ่ม โดยที่แต่ละโหนดจะเคลื่อนที่แบบสุ่มภายในกลุ่ม การเคลื่อนที่แบบเป็นกลุ่มจะอิงจากโหนดศูนย์กลางของกลุ่ม จากรูปที่ 2.13 แสดงให้เห็นว่ามี 3 โหนดเคลื่อนที่แบบอาร์พีจีเอ็ม การเคลื่อนที่ของโหนดศูนย์กลางสามารถเลือกใช้โมเดลการเคลื่อนที่แบบใดก็ได้

อาร์พีจีเอ็มถูกออกแบบมาเพื่อเลียนแบบการเคลื่อนที่ของกลุ่มให้ความช่วยเหลือ (Rescue) ยกตัวอย่างเช่น ในระหว่างการให้ความช่วยเหลือ สุนัขตำรวจจะเคลื่อนไหวโดยมีมนุษย์เป็นจุดศูนย์กลาง และทั้งคู่เคลื่อนที่ไปหาผู้เคราะห์ร้าย



รูปที่ 2.14 การเคลื่อนไหวแบบอาร์พีจีเอ็ม

2.5.1.4 เกาซ์มาร์คอฟโมเดล (Guass-Markov) ถูกออกแบบมาให้เหมาะสมกับระดับของการสุ่มที่แตกต่างกันโดยใช้จูนนิ่งพารามิเตอร์ตัวเดียว (one tuning parameter) ตอนเริ่มต้นแต่ละโมบายโหนดจะมีค่าความเร็วและทิศทางของตัวเอง และในขณะเวลา n โหนดจะเคลื่อนที่ด้วยค่าความเร็วและทิศทางใหม่ ซึ่งคำนวนโดยอิงจากความเร็วและทิศทางที่ผ่านมา ตามสมการที่ 2.1 และ 2.2

$$s_n = \alpha s_{n-1} + (1-\alpha)\bar{s} + \sqrt{(1+\alpha^2)}s_{xn-1} \quad (2.1)$$

$$d_n = \alpha d_{n-1} + (1-\alpha)\bar{d} + \sqrt{(1+\alpha^2)}dd_{xn-1} \quad (2.2)$$

โดยที่ค่า s_n และ d_n คือ ความเร็วและทิศทางใหม่ของโมบายโหนดที่เวลา n ค่า α เป็นค่าจูนนิ่งพารามิเตอร์ มีค่าตั้งแต่ 0 ถึง 1 โดยค่า 0 คือ การสุ่มทั้งหมดและ 1 คือการเคลื่อนที่แบบเป็นเส้นตรง $\bar{s}$ และ $\bar{d}$ คือค่าคงที่เฉลี่ยของความเร็วและทิศทางเมื่อ n เข้าใกล้อินฟินิตี้ และ S_{xn-1} และ d_{xn-1} คือค่าตัวแปรสุ่มจากการกระจายแบบเกาซ์เซียน

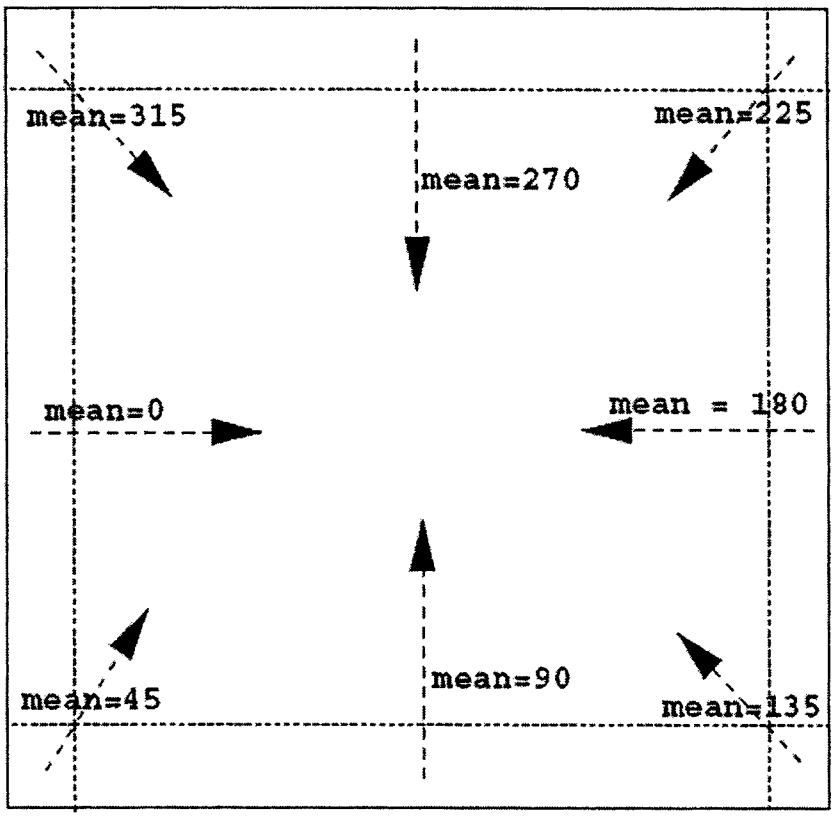
สำหรับในรอบเวลาถัดไป ค่าตำแหน่งจะได้จากการคำนวนจากตำแหน่ง เวลาและทิศทางในปัจจุบันตามสมการที่ 2.3 และ 2.4

$$x_n = x_{n-1} + s_{n-1}\cos x_{n-1} \quad (2.3)$$

$$y_n = y_{n-1} + s_{n-1}\sin d_{n-1} \quad (2.4)$$

โดยที่ค่า (x_n, y_n) และ (x_{n-1}, y_{n-1}) คือ ค่าพิกัด x และ y ของโหนด ณ เวลาที่ n^{th} และ (n-1)st ตามลำดับ และ s_{n-1} และ d_{n-1} คือความเร็วและทิศทางของโหนดตามลำดับ ที่เวลา (n-1)st

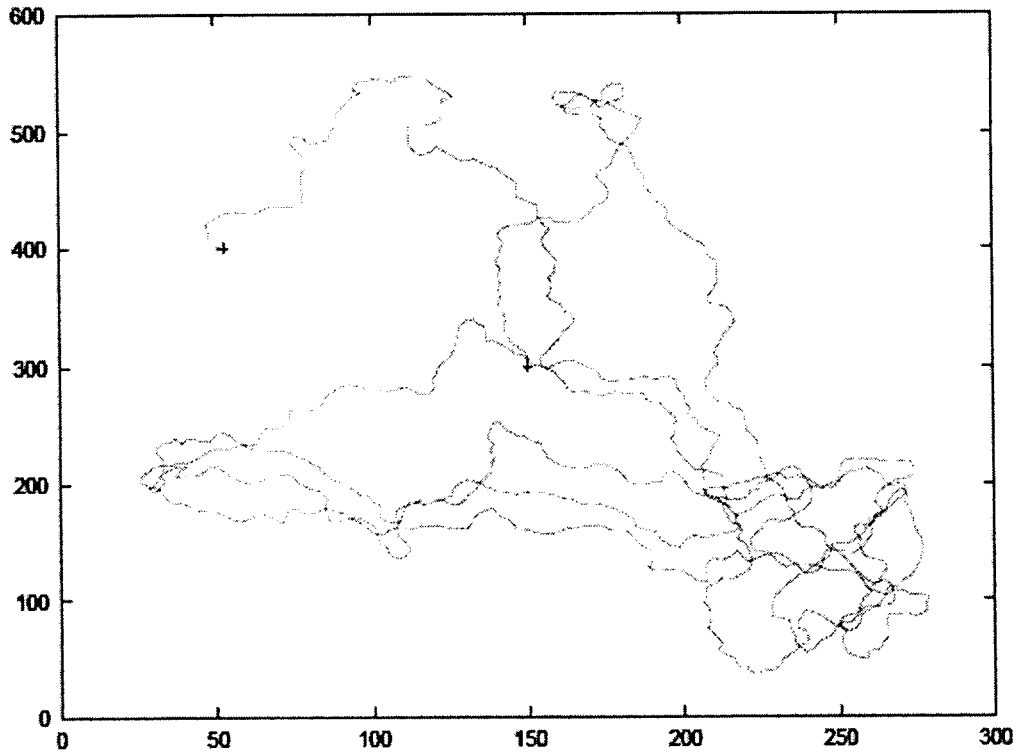
เพื่อให้แน่ใจว่าโหนดไม่ได้เคลื่อนที่อยู่ที่ขอบพื้นที่ โมบายโหนดจะถูกบังคับให้เคลื่อนออกห่างจากของเมื่ออยู่ในระยะที่ใกล้กับขอบ ตัวอย่างเช่น เมื่อโมบายโหนดเคลื่อนที่ใกล้กับขอบด้านขวาของการซิมมูเลชั่นค่า $\bar{d}$ จะเปลี่ยนเป็น 180 องศา ดังนั้นโหนดจะเคลื่อนที่ออกห่างจากขอบด้านขวา ค่าเฉลี่ยของทิศทางสำหรับตำแหน่งขอบที่ต่างกัน ดังรูปที่ 2.15



รูปที่ 2.15 มุมของการเคลื่อนที่ที่เปลี่ยนไปเมื่อโหนดเข้าใกล้กรอบ (ในหน่วยดีกรี)

และในรูปที่ 2.16 แสดงตัวอย่างการเคลื่อนที่แบบเกาซ์มาคอฟโมบิลิตี้โมเดล โดยโหนดเริ่มต้นที่กลางพื้นที่ของการซิมมูเลชั่นที่พิกัด (150, 300) และเคลื่อนที่เป็นเวลา 1000 วินาที และตั้งค่า n เป็น 1 วินาที และ α คือ 0.75 sxn-1 และ dxn-1 เลือกมาจากแรนดอมเกาซ์เซียนดิสทริบิวชั่นที่มีค่าเฉลี่ยเป็น 0 และมีการกระจายมาตรฐาน (standard deviation) เป็น 1 ค่า $\bar{S}$ คงที่ที่ 10 เมตรต่อวินาที และ $\bar{d}$ เริ่มต้นที่ 90 องศาและจะเปลี่ยนตลอดเวลาขึ้นอยู่กับระยะที่ห่างจากขอบ

เกาซ์มาคอฟโมบิลิตี้โมเดล ทำให้ไม่มีการหยุดอย่างกระทันหันของโหนดและไม่มีการเลี้ยวหักมุมเหมือนกับโมเดลที่ผ่านมาดังแสดงในรูปที่ 2.16



รูปที่ 2.16 การเคลื่อนที่แบบเกาซ์มาคอฟโมบิลิตี้โมเดล

เราสามารถจำลองการทำงานของเครือข่ายเคลื่อนที่เฉพาะกิจที่ต้องจากได้จากการทดลองบนซิมมูเลเตอร์เอ็นเอสทู ซึ่งสามารถจำลองสิ่งต่างๆ บนเครือข่ายเคลื่อนที่เฉพาะกิจได้ ไม่ว่าจะเป็นการเคลื่อนที่ของโหนด การส่งข้อมูลระหว่างโหนด สัญญาณวิทยุและการลดทอน นอกจากนี้เอ็นเอสทูยังเตรียมเทรสไฟล์ที่แสดงเหตุการณ์ที่เกิดขึ้นบนเครือข่ายเคลื่อนที่เฉพาะกิจ ณ เวลาต่างๆ ได้ ทำให้เราสามารถวัดค่าต่างๆ ในเครือข่ายได้อย่างถูกต้อง