A Survey of Secure Routing Protocol in MANET

(การสำรวจโปรโตคอลเส้นทางการส่งข้อมูลที่ปลอดภัยของเครือข่ายแอดฮอก)

Atibodee Maleehual (545020198-5), Hatairat Wongsuphan(545020146-4)

บทคัดย่อ—ในช่วงหลายปีที่ผ่านมามีหลายมีการใช้งานด้านโมบายแอดฮอกเน็ตเวริ์ค **(Mobile Ad hoc Networks (MANETs)) หรือมาเน็ต ในทางการทหารและแอฟพลิเคชั่นด้านธุรกิจ โดยในบทความสำรวจนี้ ได้มุ่งเน้นนำเสนอโปรโตคอลในการส่งข้อมูลอย่างปลอดภัย ซึ่งแต่ละโปรโตคอลมีกระบวนการส่งข้อมูลที่แตกต่างกัน โดยในบทความนี้นี้ได้เลือกการนำเสนอการโจมตีโปรโตคอลในการวิเคราะห์และประเมินผล อาทิเช่น แอดฮอกออนดีมานดิสเท่นเวกเตอร์เร้าท์ติ้ง (Ad Hoc on demand Distance Vector routing (AODV)), ไดนามิกซอร์ทเร้าติ้ง (Dynamic Source Routing (DSR)) และ ออฟติไมต์ลิงค์สเตทเร้าท์ติ้ง (Optimized Link State Routing (OLSR)) เป็นต้น ในด้านความปลอดภัยของเครือข่ายแอดฮอกมีความต้องการ 5 ประการดังนี้ การรักษาความลับ, ความถูกต้อง, การพิสูจน์ตัวตน, การยอมรับ และ ความพร้อมในการใช้งาน โดยความปลอดภัยเป็นวัตถุประสงค์หลักในการทำบทความนี้**

คำสำคัญ—**เครือข่ายไร้สายแอดฮอค, เครือข่ายไร้สายเฉพาะกิจ, Routing Protocal, MANETs, Attacks in MANETS.**

1. บทนำ

การพัฒนาเทคโนโลยีการสื่อสารไร้สายจากอดีตจนถึงปัจจุบันได้ปรับเปลี่ยนและพัฒนาไปอย่างมาก ไม่ว่าจะเป็นการพัฒนาของสื่อที่ใช้ในการสื่อสารหรือกระบวนการและวิธีการของการรับส่งข่าวสาร แต่เนื่องจากความต้องการของผู้ใช้ที่มีอยู่อย่างไม่หยุดยั้งทำให้การบริการที่มีอยู่ไม่เพียงพอทั้งในเชิงปริมาณและคุณภาพ ดังนั้นทำให้นักวิจัยและผู้เชี่ยวชาญได้พัฒนาศักยภาพของโครงข่ายโทรคมนาคมเพื่อให้เพียงพอและเป็นที่พอใจกับผู้บริโภค

เครือข่ายเคลื่อนที่เฉพาะกิจ)Mobile Ad hoc Network -MANET) เป็นเครือข่ายของอุปกรณ์คำนวณแบบเคลื่อนที่ได้ที่เชื่อมต่อกันเพื่อรับส่งข้อมูลระหว่างกันโดยไม่อาศัยสถานีฐาน)base station) ไม่มีการควบคุมจากส่วนกลาง และรูปแบบการเชื่อมต่อของอุปกรณ์คำนวณแบบเคลื่อนที่ได้ที่อยู่ภายในเครือข่าย หรือรูปแบบของทอพอโลยี)topology)นั้นสามารถเปลี่ยนแปลงได้อยู่ตลอดเวลา ขึ้นอยู่กับความเร็วและทิศทางในการเคลื่อนที่ จาก

ลักษณะดังกล่าวจึงต้องมีการพัฒนาโปรโตคอลค้นหาเส้นทางสำหรับเครือข่ายเคลื่อนที่เฉพาะกิจเพื่อให้อุปกรณ์ดังกล่าวสามารถรับส่งข้อมูลระหว่างกันได้

2. ความรู้พื้นฐานและทฤษฎีที่เกี่ยวข้อง

2.1 คุณลักษณะของโครงข่ายแบบแอดฮอก

โครงข่ายแอดฮอกเป็นโครงข่ายที่ประกอบด้วยโนดที่มีความสามารถในการเคลื่อนที่ได้อย่างอิสระ จึงทำให้โครงข่ายแอดฮอกเป็นโครงข่ายที่ไม่มีโครงสร้างที่แน่นอนและเปลี่ยนแปลงตลอดเวลานอกจากนี้การสื่อสารระหว่างคู่โนดยังปราศจากจุดเข้าถึง ในการควบคุมการเข้าถึงตัวกลาง ทำให้โนดแต่ละโนดต้องมีความสามารถในการจัดการการเข้าถึงตัวกลางได้ด้วยตนเอง นอกจากนี้โนดในโครงข่ายยังต้องมีความสามารถในการจัดเส้นทางสำหรับการส่งข้อมูลได้ด้วยตัวเอง ทำให้โนดทุกโนดในโครงข่ายต้องทำหน้าที่เปรียบเสมือนกับอุปกรณ์จัดเส้นทาง (Router) ซึ่งจะจัดเส้นทางการส่งแพ็กเกตข้อมูลไปยังโนดปลายทางได้ คุณสมบัติอื่น ๆ ที่สำคัญของโครงข่ายแอดฮอก สามารถสรุปได้ ดังนี้

2.1.1 ทอพอโลยีแบบพลวัต (Dynamic Topology) โนดในโครงข่ายแอดฮอกจะมีการเคลื่อนที่อยู่ตลอดเวลา โดยการเคลื่อนที่ของโนดเป็นแบบสุ่มดังนั้นระบบจะไม่สามารถคาดการณ์การเคลื่อนที่ของโนดได้ ซึ่งส่งผลให้ทอพอโลยีของโครงข่ายมีการเปลี่ยนแปลงอยู่ตลอดเวลาทำให้ลำบากในการควบคุมการเข้าถึงตัวกลางในโครงข่ายแอดฮอก

2.1.2 การสื่อสารเป็นแบบหลายช่วงเชื่อมต่อ (Multi-hop communication) เนื่องจากการสื่อสารในโครงข่ายแอดฮอกเป็นการสื่อสารกันโดยตรงโดยไม่ผ่านจุดของการเข้าถึง ดังนั้นโนดแต่ละโนดจะต้องมีความสามารถในการเป็นสถานีส่ง สถานีรับ และสถานีระหว่างทางโดยถ้าการสื่อสารเกินระยะของการส่งข้อมูล (Transmission range) การสื่อสารนั้นจำเป็นต้องอาศัยโนดระหว่างทาง (Intermediate node) ในการส่งข้อมูลนั้นไปยังโนดปลายทาง ซึ่งจะเห็นได้ว่ายิ่งมีการใช้โนดระหว่างทางมากขึ้นเท่าใดความซับซ้อนของโครงข่ายก็จะมากขึ้นเท่านั้น

2.1.3 การปฏิบัติการเป็นแบบกระจายศูนย์ (Decentralized operation) สถาปัตยกรรมของโครงข่ายแอดฮอกมีโครงสร้างที่ไม่แน่นอน อีกทั้งยังไม่มีการ

ควบคุมการเข้าถึงตัวกลางแบบรวมศูนย์ ดังนั้นโนดทุกโนดในโครงข่ายต้องมีความสามารถในการจัดการการเข้าถึงตัวกลางรวมถึงการควบคุมการไหลของทราฟฟิกให้ได้สมรรถนะโดยรวมที่ดีที่สุดโดยการใช้มาตรฐานที่โนดทุก ๆ โนดรับรู้ร่วมกัน

2.1.4 ข้อจำกัดทางด้านแบนด์วิดท์ (Bandwidth constrained) การสื่อสารแบบไร้สายจะมีการใช้ประโยชน์รวมของการใช้แบนด์วิดท์ที่ต่ำกว่าการสื่อสารแบบใช้สาย เนื่องจากผลกระทบของการเข้าถึงแบบหลายทาง (Multiple access) เฟดดิง (Fading) สัญญาณรบกวน (Noise) ปัญหาของสถานีที่ซ่อนเร้น (Hidden station problem) และปัญหาสถานีที่รับฟังได้ (Exposed station problem) เป็นต้น ซึ่งผลกระทบของปัญหาเหล่านี้ทำให้การใช้ประโยชน์ของการใช้แบนด์วิดท์มีค่าต่ำกว่าค่าแบนด์วิดท์สูงที่สุดที่สามารถใช้ได้

2.1.5 ข้อจำกัดทางด้านพลังงาน (Energy constrained) พลังงานของอุปกรณ์ที่ใช้ในโครงข่ายก็เป็นคุณลักษณะหนึ่งที่สำคัญ เนื่องจากการสื่อสารในโครงข่ายแอดฮอกเป็นแบบหลายช่วงเชื่อมต่อดังที่ได้กล่าวไปแล้ว ดังนั้นเมื่อพลังงานของอุปกรณ์ตัวหนึ่งตัวใดหมดไปหรือไม่เพียงพอในการส่งข้อมูล อาจจะส่งผลกระทบในการส่งข้อมูลภายในโครงข่ายได้เพราะฉะนั้นปัจจัยที่สำคัญในการออกแบบโพรโทคอลการจัดเส้นทางภายใต้ข้อจำกัดพลังงานคือการทำให้โนดหรืออุปกรณ์ที่ใช้งานประหยัดพลังงานให้มากที่สุดเท่าที่จะทำได้

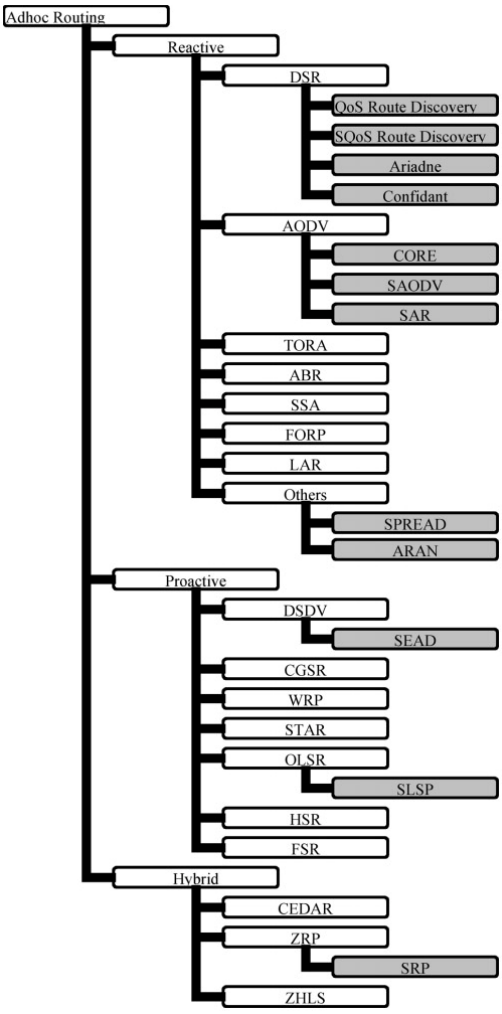
คุณสมบัติต่าง ๆ ที่มีผลกระทบต่อสรรถนะของระบบดังที่กล่าวข้างต้นเป็นคุณสมบัติที่สำคัญที่นักวิจัยได้ให้ความสนใจและนำไปสู่การออกแบบการทำงานด้านต่าง ๆ เช่น ความสามารถในการจัดเส้นทางเพื่อให้ส่งแพ็กเกตได้อย่างรวดเร็ว การพัฒนาในการหาตำแหน่งของโนดปลายทางหรือการจัดเส้นทางในการส่งข้อมูลเพื่อให้ได้เส้นทางที่ประหยัดพลังงานมากที่สุด เป็นต้น

2. 2 ความปลอดภัยแอดฮอกเร้าท์ทิงโปรโตคอล

เร้าท์ทิงโปรโตคอลสำหรับเครือข่ายไร้สายแอดฮอกสามามารถแบ่งออกเป็น 3 ประเภทบนพื้นฐานการปรับปรุงข้อมูลกลไกในการทำงาน เครือข่ายไร้สายแอดฮอก คือ รีแอคทีฟ (Reactive) เป็นการทำงานตามความต้อง, โปรแอคทีฟ (Proactive) เป็นการทำงานตามตาราง และไฮบริด ดังในรูปที่ 1 ได้แสดงถึงประเภทเร้าท์ทิงโปรโตคอลทั้ง 3 ประเภทและรายการของเร้าท์ทิงโปรโตคอลที่สามารถใช้งานได้ตามประเภทต่างๆ

2.2.1 **โปรโตคอลค้นหาเส้นทางแบบรีแอคทีฟ (REACTIVE)**

การค้นหาเส้นทางแบบรีแอคทีฟได้รับเส้นทางที่จำเป็น เมื่อต้องการ จากการใช้การสถาปนาการกระบวนการเชื่อมต่อ เช่น โปรโตคอลหลักไม่สามารถแลกเปลี่ยนข้อมูลเส้นทางที่มีการเปลี่ยนแปลงเป็นระยะๆ ในบทความส่วนนี้จะมุ่งเน้นถึง 3 โปรโตคอลค้นหาเส้นทางและเรื่องเกี่ยวความปลอดภัยบางรุ่น เช่น ดีเอสอาร์ (DSR)[1] , เอโอดีวี AODV[2]



รูปที่ 1 Ad hoc routing protocols [1]

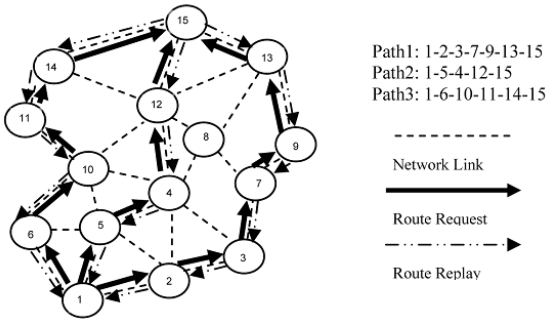
- **ดีเอสอาร์ (DSR)**

ดีเอสอาร์[2] คือการออกแบบโปรโตคอลตามความต้องการเส้นทางที่จำกัดแบนวิดธ์ โดยการควบคุมแพ็กเก็ตในเครือข่ายไร้สายแอดฮอก จากการปรับปรุงข้อมูลในตารางเส้นทางตามความต้องการในโปรโตคอลค้นหาเส้นทางแบบโปรแอคทีฟ ไม่มีบีคอนไม่จำเป็นต้องมีการปรับปรุง เฮลโล แพ็ค) (สัญญาณ) จอนห์สัน (เก็ตเป็นระยะ ซึ่งถูกใช้เพื่อแจ้งให้โหนดเพื่อนบ้านทราบ ได้แบ่งปัญหาของการค้นหาเส้นทางในสองพื้นที่ การค้นหาเส้นทางและการปรับปรุงเส้นทาง ในลำดับโหนดที่สื่อสารกับโหนดอื่นในเครือข่าย ในเริ่มแรกค้นหาเส้นทางที่เหมาะสม ใช้การส่งแพ็คเก็ตไปที่โหนดปลายทางจะเป็นอย่างนี้จนกระทั้งไม่มีการเปลี่ยนเงื่อนไข

ในขั้นตอนค้นหาเส้นทาง เริ่มต้นการส่งตามแพ็คเก็ตร้องขอเส้นทาง, การระบุเป้าหมายในการที่จะเป็นเส้นทางที่จำเป็น แต่ละโหนดขึ้นอยู่การรับการร้องขอเส้นทาง โดยทั่วไปการส่งซ้ำตามคำร้อง ถ้าไม่มีความพร้อมในการส่งจะสำเนาคำร้องเส้นทาง เมื่อโหนดปลายทางรับคำร้อง จะส่งกลับคำร้องขอเส้นทางไปที่ผู้เริ่มต้น การแสดงรายการเส้นทางจากการร้องขอ มากว่าการส่งต่อคำร้อง ซึ่ง

โหนดเป้าหมายส่งกลับแทนที่คำตอบรับเส้นทางสำหรับแต่ละสำเนาของการร้องขอเส้นทางที่ได้รับ ดังนั้น จึงทำการเลือกเส้นทางที่มีล่าช้าต่ำสุด แต่แพ็ตเก็ตร้องขอเส้นทาง แต่ละแพ็คเก็ตร้องขอเส้นทางจะสร้างหมายเลขลำดับของโหนดโดยแหล่งที่มาและเส้นทางที่ผ่านมา โหนดที่ได้รับแพ็คเก็ตร้องขอเส้นทางตรวจสอบหมายเลขลำดับบนแพ็คเก็ตก่อนส่งต่อ หมายเลขลำดับบนแพ็คเก็ตคือใช้ป้องกันการเกิดลูปและการหลีกเลี่ยงการส่งหลายครั้งของเส้นทางที่ร้องของแพ็คเก็ตเดียวกันจากโหนดที่ได้รับผ่านหลายเส้นทาง

เพื่อประโยชน์ของโหนดตัวกลางที่ใช้โปรโตคอลเก็บเส้นทางในหน่อยความจำชั่วคราว ทุกข้อมูลที่เป็นไปได้ในการสกัดแหล่งข้อมูลเส้นทางที่อยู่ในข้อมูลแพ็คเก็ต ถ้าโหนดกลางทำการรับคำร้องขอเส้นทางมีเส้นทางโหนดปลายทางในเส้นทางความจำชั่วคราว ในการตอบกลับข้อมูลของโหนดจากการส่งข้อความคำร้องกลับ และใส่ข้อมูลจากโหนดที่มีข้อมูลไปยังโหนดปลายทาง ได้อธิบายอัลกอลิทึมแบ็คออฟ คือการหลีกการใช้งานแพ็คเก็ตที่มีการร้องขอบ่อยๆเกิดการฟลัดดิ้นในเครือข่าย เมื่อปลายเกิดการคลาดเคลื่อน ดีเอสอาร์จะอนุญาต พิกกี้-แบ็คกิ้ง (piggy-backing) ของข้อมูลแพ็คเก็ตที่มีข้อความร้องขอเส้นทาง โดยข้อมูลแพ็คเก็ตสามารถส่งแพ็คเก็ตข้อมูลจะถูกส่งไปพร้อมกับข้อความที่ร้องขอเส้นทาง

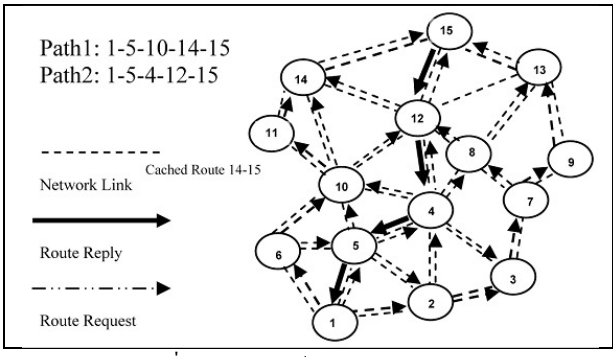


รูปที่ 2 การสถาปนาการเชื่อมต่อเส้นทางในดีเอสอาร์ [2]

ในขั้นตอนการบำรุงรักษาเมื่อมีโหนดในเส้นทางที่เคลื่อนออก ก่อให้เกิดการเชื่อมโยงในเครือข่ายไร้สายเสียหาย โดยจะมีข้อความที่บอกถึงเส้นทางที่เสียหายที่สร้างขึ้นจากโหนดที่อยู่ติดกับโหนดที่เสียหาย โหนดที่เป็นแหล่งข้อมูลจะทำการเริ่มต้นสถาปนาค่าใหม่อีกครั้ง รายการแคชที่โหนดและโหนดต้นทางจะถูกเอาออกเมื่อมีข้อผิดพลาดในเส้นทางของแพ็กเก็ตที่ได้รับ รูปที่ 2 แสดงให้ถึงการทำงานของดีเอสอาร์

เมื่อโหนด 1 ต้องการส่งข้อมูลไปยังโหนดที่ 15 นั้นจะทำการส่งคำร้องขอเส้นทางแรกไปยังทุกๆโหนดเพื่อนบ้าน แต่ละโหนดเพื่อนบ้านจะตรวจสอบเส้นทางในแคช ถ้ามีข้อมูลปลายทางก็จะแสดงรายการออกมา และส่งคำร้องขอเส้นทางกลับไปยังผู้ส่ง ถ้าไม่พอเส้นทางดังกล่าว จะส่งต่อคำร้องขอเส้นทางไปยังทุกโหนดที่เป็นเพื่อนบ้าน ตามลำดับเพื่อหลีกเลี่ยงการเกิดลูป แต่ละโหนดเพื่อนบ้านจะตรวจสอบ ถ้ามีความพร้อมในการส่งต่อคำร้องขอเส้นทางจะใช้หมายเลขลำดับมาช่วย ปลายทางโหนดที่ 15 จะตอบกลับทุกๆคำร้องขอเส้นทางที่ได้รับกับคำร้องตอบกลับ หนึ่งแหล่งที่มาจะรับทุกคำตอบกลับเส้นทาง กับกำหนดเวลา เพื่อจะได้ส่งข้อมูลตามเส้นทางที่จำนวนฮอฟที่น้อยที่สุด ดังในตัวอย่างเส้นทาง 15-12-4-5-1 ถ้ามีการหยุดเชื่อมโยงระหว่างโหนด 12 และ 15 นั้นจะทำให้โหนดส่งข้อมูลไหลพลาด (โหนด 12) จะส่งข้อความเส้นทางที่ผิดผ่านไปยังแหล่งที่มา ซึ่งแหล่งที่มาจะทำการสถาปนาเส้นทางใหม่ โดยส่งข้อความร้องขอ ทุกโหนดที่อยู่ระหว่างกลางลบข้อมูลเส้นทางในแคชหมด เพื่อรอทำการสร้างเส้นทางใหม่อีกครั้ง

ในส่วนนี้ไม่มีเรื่องเกี่ยวกับปลอดภัยมาอธิบายร่วมด้วย ซึ่งเพียงแต่อธิบายถึงหลักการเบื้องต้นของดีเอสอาร์ รวมถึงการจัดการทรัพยากรที่ไม่ได้ใช้ ตัวอย่างเช่น ถ้ามีโหนดตัวกลางไม่ทราบที่อยู่ปลายทาง ตัวโหนดจะการส่งต่อคำร้องขอเส้นทางไปยังทุกโหนดเพื่อนบ้าน



รูปที่ 3 การติดต่อเส้นทางใน เอโอดีวี [3]

- **เอโอดีวี (AODV)**

เอโอดีวี [3] ลักษณะการทำงานคล้ายดีเอสอาร์มาก ดีโอดีวีทำงานโดยสามารถส่งคำร้องขอเส้นทางไปยังปลายทาง โหนดต้นทางและโหนดกลางจะจัดเก็บข้อมูลฮ็อฟถัดไปที่สอดคล้องกับการไหลสำหรับการส่งแพ็กเก็ตข้อมูล ความแตกต่างที่สำคัญระหว่าง AODV และอื่น ๆ บนโปรโตคอลเส้นทางความต้องการคือการใช้หมายเลขลำดับปลายทาง (DesSeqNum) ที่ตรวจสอบถึงวันที่เส้นทางไปยังปลายทาง โหนดจะปรับปรุงเส้นทางปลายเพียงเท่านั้น ถ้าหมายเลขลำดับปลายทางของแพ็กเก็ตในปัจจุบันที่ได้รับมีค่ามากกว่าโหนดล่าสุด ข้อความขอเส้นทางดำเนินหกรายการ : ระบุแหล่งที่มา, ระบุปลายทาง, หมายเลขลำดับของแหล่งที่มา, หมายเลขลำดับปลายทาง, ระบุการกระจายและช่วงเวลาที่อยู่

ในรูปที่ 3 เมื่อโหนดหนึ่งส่งคำร้องขอเส้นทาง โหนดตัวกลางจำส่งต่อคำร้องหรือตอบกับด้วข้อความเส้นทาง ถ้ามีเส้นทางที่ผิดพลาดที่ปลายทาง การระบุกระจายสัญญาณและระบุต้นทางคือใช้สองอย่างด้วยกันในการตรวจสอบ ถ้าโหนดที่รับแล้วได้สำเนาคำร้องขอเส้นทางก่อนหน้า โหนดที่มาอาจได้รับมากกว่าหนึ่งคำตอบซึ่งในกรณีนี้มันจะได้กำหนดต่อที่ข้อความเพื่อเลือกขึ้นอยู่กับการนับฮอป ทุกโหนด ก่อนที่จะส่งต่อแพ็คเก็ต จะเก็บค่ากระจายสัญญาณและหมายเลขโหนดก่อนหน้าจากที่ขอมา จับเวลาที่ใช้แล้วโดยโหนดกลางนี้เพื่อลบรายการนี้ในกรณีที่ตอบไม่ได้รับการร้องขอ หากมีข้อความตอบกลับที่โหนดกลางที่จัดเก็บอีกครั้งระบุออกกระจายและโหนดก่อนหน้านี้จากที่ตอบมา

เอโอดีวี ไม่สามารถปรับปรุงเส้นทางที่ขาดค้ เมื่อการเชื่อมต่อขาด ซึ่งจะถูกกำหนดโดยการสังเกตบีคอนหรือข้อความแอค(ACK) โหนดต้นทางและปลายทางจะได้รับแจ้ง โหนดต้นทางเมื่อทำการเชื่อมต่อใหม่ด้วย (โหนดปลาย) ชั้นปลายทางที่สูงกว่า ตารางที่2 แสดงลำดับของขั้นตอนแต่ละกรณีของโหนด 1 ที่ตั้งใจส่งข้อความไปยังโหนดที่ 15 ในเครือข่าย ดังที่แสดงในรูปที่ 5

สิ่งสำคัญที่ควรจำถึงความแตกต่างหลังของดีเอสอาร์และเอโอดีวี ดีเอสอาร์โปรโตคอลค้นหาเส้นทางในเครือข่ายไร้สายแอดฮอกตามความต้องการเท่านั้น เอโอดีวีคือการเริ่มต้นการเชื่อมต่อซึ่งรวมทั้งสองคือดีเอสอาร์และดีเอสอาร์วี[48] นำกลไกแบบตามความต้องการพื้นฐานของการค้นพบเส้นทางและการบำรุงรักษาเส้นทางจากดีเอสอาร์ รวมถึงการใช้การค้นหาเส้นทางแบบฮอปต่อฮอป หมายเลขลำดับและส่งค่าบีคอนเป็นระยะจากดีเอสดีวี

เอโอดีวีไม่ได้ให้ความปลอยภัยกับทุกประเภท รวมไปถึงการจัดการพลังงาน กล่าวคือไม่ได้ใช้งานได้ดี ตัวอย่างน่น ถ้าโหนดตัวกลางไม่ทราบที่อยู่ปลายทาง จะทำการส่งต่อคำร้องไปยังทุกๆโหนดในเครือข่าย

2.2.2 โปรโตคอลการค้นหาเส้นทางแบบโปรแอคทีฟ (PROACTIVE)

ในเชิงรุกหรือตารางการขับเคลื่อนของโปรโตคอลค้นเส้นทาง เช่นดีเอสดีวี DSDV[4] หรือ โอแอลเอสอาร์ OLSR[5] ทุกโหนดจะเก็บข้อมูลโครงสร้างเครือข่ายในรูปแบบของตารางเส้นทางด้วยข้อมูลการค้นหาเส้นทางตามระยะที่มีการเปลี่ยนแปลง โดยทั่วไปแล้วข้อมูลในการค้นหาเส้นทางจะไหลไปในเครือข่ายทั้งหมด เมื่อใดก็ตามที่โหนดต้องการเส้นทางที่จะไปยังโหนดปลายทาง มันจะวิ่งไปตามเส้นทางที่อัลกอลิทึมค้นหาเส้นทางได้หาไว้อย่างเหมาะสมแล้วบนโครงสร้างข้อมูลที่ได้ถูกบำรุงรักษาไว้

- ดีเอสดีวี (DSDV) [4]

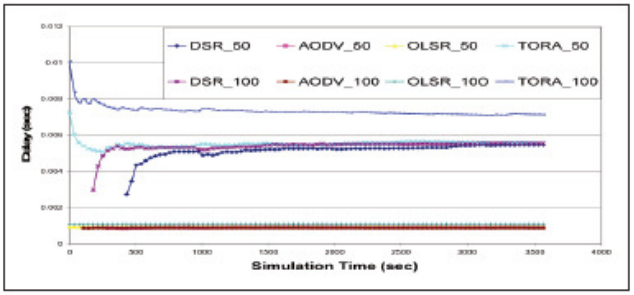
โปรโตคอลที่กำหนัดลำดับของโหนดปลายทางด้วยดิสแตนซ์เวกเตอร์ (Destination Sequenced Distance Vector protocols) เป็นอัลกอลิทึมที่ระบุถึงเส้นทางที่สั้นที่สุดที่อยู่บนพื้นฐานของเบลแมนฟอร์ด (Bellman-Ford) โหนดอื่นๆที่มีตารางที่มีรายละเอียดของเส้นทางที่สั้นที่สุดไปยังทุกๆโหนดภายในเครือข่าย ตารางเหล่านี้จะถูกปรับปรุงอยู่เสมอและจะถูกส่งต่อไปยังโหนดอื่นๆภายในเครือข่ายเมื่อตรวจพบว่ามีการเปลี่ยนแปลง เมื่อโหนดได้รับการปรับปรุงแล้วสามารถปรับปรุงตารางหรือถือไว้ในขณะนั้นเพื่อเลือกเส้นทางที่สั้นที่สุด รูปที่ เป็น 15 เป็นโหนดต้นทางและ โหนดที่ 1 แสดงตัวอย่างเมื่อโหนดที่ 10 แสดงให้เ 3 ตารางที่ 1 โหนดปลายทาง ตารางค้นหาเส้นทางของโหนดที่หึนว่าเส้นทางที่สั้นที่สุดที่โหนดจะได้รับคือการผ่านโหนด ในขณะที่เส้นทางที่จะไป 8 ฮอป เมื่อตรวจพบว่าการขาดการเชื่อมต่อ โหนดปลายทางจะมีการ 4 ถึงมีปรับปรุงตาราง ข้อความที่ปรับปรุงมีมากมายที่ถูกกำหนดขึ้นและหมายเลขลำดับสำหรับโหนดปลายทาง เมื่อโหนดได้รับข้อความจะถูกส่งอย่างรวดเร็วไปยังโหนดข้างเคียง

- **โอแอลเอสอาร์ (OLSR) [5]**

โปรโตคอลในการค้นหาเส้นทางที่มีสถานะในการเชื่อมต่อที่เหมาะสม (The Optimized Link State Routing Protocol) [5] เป็นโปรโตคอลค้นหาสถานะของเส้นทางในเชิงรุก รายละเอียดของ OLSR สามารถหาได้จาก IETF RFC 3626 [42] OLSR มีสองประเภทของข้อความที่ใช้ในการควบคุม ดังนี้ ข้อความ Hello และโครงสร้างในการควบคุมข้อความ (Topology Control)

ข้อความ Hello จะใช้ในการสร้างพื้นที่ใกล้เคียงของโหนดและการค้นพบโหนดที่อยู่ภายในบริเวณใกล้เคียงของโหนด ข้อความเหล่านี้ยังใช้ในการคำนวณรีเลย์ในหลายจุดของโหนด OLSR ได้มีการบอร์ดแคสข้อความ Hello เป็นระยะๆ เพื่อส่งให้ถึงพื้นที่ใกล้เคียงของโหนดเพื่อตรวจสอบมาตรฐานของสัญญาณวิทยุ ข้อความ Hello จะได้รับในทุกๆฮอปที่อยู่ใกล้เคียงแต่จะไม่มีการส่งต่อ สำหรับทุกช่วงเวลาที่คงที่จะรู้จักกันว่าเป็นช่วงเวลา Hello ของโหนดที่บอร์ดแคสข้อความ Hello ข้อความ Hello ยังอนุญาตให้โหนดสามารถค้นหาโหนดใกล้เคียงได้สองฮอป ตั้งแต่ช่วงที่โหนดได้ยินการส่งไปจนถึงช่วงที่มีการส่งผ่านไปยังฮอปข้างเคียง สถานะของการเชื่อมโยงเหล่านี้กับโหนดอื่น ๆ ในละแวกใกล้เคียงอาจจะสมมาตรหรือไม่สมมาตรหรือมีการตอบกลับในหลายๆจุด(MultiPoint Relay) ก็ได้ การเชื่อมโยงแบบสมมาตรซึ่งหมายความว่าการเชื่อมต่อมีสองทิศทาง ในขณะที่การเชื่อมโยงแบบไม่สมมาตรจะมีการเชื่อมต่อแบบทิศทางเดียว การได้รับหนึ่งฮอปหรือสองฮอปจากโหนดใกล้เคียง โหนดนั้นสามารถดำเนินการเลือกรีเลย์หลายจุดได้ ซึ่งจะช่วยให้เข้าถึงโหนดที่อยู่ใกล้เคียงทั้งหมดที่อยู่ในช่วงสองฮอป ทุกๆโหนด k จะเลือกเก็บค่าที่ถูกกำหนดโดย MPR ซึ่งประกอบด้วยโหนดทั้งหมดที่ได้เลือกโหนดที่ k เป็น MPR ดังนั้นโหนดที่ k สามารถบอร์ดแคสข้อความที่ได้รับซ้ำได้เท่านั้นจากโหนดที่พบใน MPR ที่เลือกไว้ [50]

ข้อความ Topology Control จะมีข้อมูล MPR ที่ถูกเลือกไว้ ข้อความเหล่านี้จะส่งแบบบอร์ดคาสเป็นระยะๆ ภายในช่วงที่มีการส่ง TC ไปยัง MPR อื่นๆ สามารถถ่ายทอดข้อมูลเพิ่มเติมไปยัง MPR เหล่านั้นได้ ดังนั้นโหนดใดๆในเครือข่ายก็สามารถเข้าถึงได้ผ่าน MPR กับพื้นที่ใกล้เคียงกับข้อมูลโทโปโลจิคอล โหนดสามารถสร้างทั้งตารางค้นหาเส้นทางของเครือข่าย การค้นหาเส้นทางไปหาโหนดอื่นเป็นการคำนวณที่ใช้อัลกอลิทึมในการค้นหาเส้นทางทางที่สั้นที่สุด เช่น อัลกอลิทึมไดเจสตรา (Dijkstra'a) หมายเลขลำดับใช่เพื่อให้มั่นใจว่ามีการปรับปรุงการค้นหาเส้นทางที่ไม่ใช่ข้อมูลเก่า เมื่อใดก็ตามที่มีการเปลี่ยนแปลงโทโปโลจีหรือมีการเปลี่ยนไปยังโหนดข้างเคียง MPR จะถูกนำมาคำนวณอีกครั้ง การปรับปรุงจะถูกส่งไปยังเครือข่ายทั้งหมด ดั้งนั้นการค้นหาเส้นทางต้องมีการคำนวณใหม่เพื่อให้ข้อมูลเส้นทางมีการอับเดทไปยังปลายทางอื่นๆที่รู้จักภายในเครือข่าย



รูปที่ 5 Wireless delay [5]

ตามที่ได้กล่าวไว้ข้างต้น ข้อความ Hello จะมีการเปลี่ยนแปลงระหว่างหนึ่งฮอปเท่านั้น ตั้งแต่ขนาดของ MANET ที่สามารถระบุได้ และมีความจำเป็นที่จะต้องใช้ประสิทธิรูปมากขึ้น ในแนวทางของโทโปโลยที่ไม่มีการแชร์ข้อมูล การสื่อสารกับโหนดที่อยู่ระยะไกลจะใช้โปรโตคอลกำหนดเส้นทางแบบรีแอคทีฟ (reactive routing protocols)

วิธีการดั้งเดิมจะเป็นส่งออกไปทั้งเครือข่ายเครือข่าย ซึ่งง่ายต่อการดำเนินงาน แต่มันก็ทำให้ด้อยในด้านของประสิทธิรูปในการควบคุมแพ็คเก็ตเช่นกัน แนวคิด MPR ได้รับการออกแบบเพื่อลดโอเวอร์เฮดของการควบคุมที่เกิดจากการกระจายไปตามเส้นทางที่เลือกไว้ โดยเลือกเฉพาะโหนด MPR ที่ได้รับอนุญาต เพื่อส่งข้อมูล topological แบบบอร์ดคาสซ้ำได้

โดยทั่วไปแล้วการค้นหาเส้นทางการจราจรที่จะใช้ในการส่งและรับของ DSR และ TORA ซึ่งจะดีกว่า AODV และ OLSR อย่างไรก็ตามความล่าช้าของเครือข่ายจะแสดงใน รูปที่ 11 ในAODV และ OLSR จะดีกว่า DSR และ TORA

ผลลัพธ์เหล่านี้มีความสำคัญมากเมื่อมีการออกแบบความปลอดภัยของโปรโตคอลในการค้นหาเส้นทาง เมื่อทรัพยากรในเครือข่ายเป็นปัจจัยที่สำคัญที่สุดในการกำหนดความสำเร็จของโปรโตคอล ตัวอย่างเช่น เมื่อเป้าหมายของเราคือการออกแบบโปรโตคอลที่มีความปลอดภัยจะต้องทำให้มีการจราจรที่ต่ำ และเราควรเริ่มต้นการออกแบบไปตามประเภทของของกลไกที่คล้ายกับ DSR และ TORA ในอีกด้านหนึ่งถ้าเป้าหมายหลักของเรา)ที่นอกเหนือจากการรักษาความปลอดภัยคือความล่าช้าในเครือข่ายแล้วเราควรคิดเกี่ยวกับกลไกที่ (คล้ายกับสิ่งที่ได้รับจากการดำเนินการในAODV และ OLSR

2.2.3 ไฮบริดเร้าทิ้งโปรโตคอล (HYBRID ROUTING PROTOCOLS)
โปรโตคอลในการค้นหาเส้นทางแบบไฮบริด เช่น ZRP [6] และ SRP [7] เป็นโปรโตคอลที่รวมคุณสมบัติที่ดีที่สุดทั้งสองด้านเอาไว้ และ โปรโตคอลกำหนดเส้นทางแบบโปรแอคทีฟ)proactive routing protocolsตัวอย่างเช่น สำหรับการ (สื่อสารระหว่างโหนดเพื่อนบ้านจะใช้โปรโตคอลกำหนดเส้นทางเชิงรุก ส่วนการสื่อสารกับโหนดที่อยู่ระยะไกลจะใช้โปรโตคอลกำหนดเส้นทางแบบรีแอคทีฟ)reactive routing protocols(

- **แซดอาร์พี (ZRP) [6]**

Zone Routing Protocol (ZRP) [6] เป็นลูกผสมระหว่างโปรแอคทีฟกับรีแอคทีฟ โหนดทุกโหนดจะมีกลไกแบ่งเป็นโซนภายในกับโซนภายนอก เมื่อมีโหนดต้องการที่จะทำงานกับโซนภายใน มันจะใช้โปรโตคอลในการสื่อสารในเครือข่ายแอดฮอกตัวอื่น เช่น DSDV เมื่อต้องการสื่อสารกับโหนดภายนอก ซึ่ง) ก็จะใช้โปรโตคอล (เป็นโซนพิเศษในการสื่อสารอย่างใดอย่างหนึ่ง เช่น DSR หรือ AODV

- **เอสอาร์พี (SRP) [7]**

เป็นโปรโตคอลที่ไม่รักษาความปลอดภัยของแพ็กเก็ตในเส้นทางที่เกิดข้อผิดพลาด แต่แทนที่จะมอบหมายฟังก์ชั่นในการค้นหาเส้นทางไปยังเส้นทางที่มีการบำรุงรักษาของโปรโตคอลที่จัดการด้านความปลอดภัยในการขนส่ง SRP ใช้หมายเลขลำดับในการร้องขอเพื่อให้แน่ใจว่าเป็นข้อมูลใหม่เสมอ แต่หมายเลขลำดับนี้สามารถตรวจสอบที่เป้าหมายได้ SRP ต้องการในส่วนของความสัมพันธ์ด้านความปลอดภัยระหว่างการสื่อสารระหว่างโหนดเท่านั้น และใช้ความสัมพันธ์ด้านความปลอดภัยนี้เป็นเพียงแค่การตรวจสอบเส้นทางการร้องขอ และตอบกลับเส้นทางที่ผ่านการใช้งานด้วยรหัสข้อความที่ใช้ในการตรวจสอบ ที่เป้าหมาย SRP สามารถตรวจจับการเปลี่ยนแปลงของการขอเส้นทาง และที่แหล่งกำเนิด SRP สามารถตรวจจับการเปลี่ยนแปลงของเส้นทางตอบได้ด้วย

SRP ไม่ได้พยายามที่จะป้องกันไม่ให้มีการปรับเปลี่ยนโดยที่ไม่ได้รับอนุญาต ของฟิลที่มีการแก้ไขตามปกติในระหว่างการการส่งต่อแพ็กเก็ตเหล่านี้ ตัวอย่างเช่น โหนดสามารถเคลื่อนที่ได้อย่างอิสระ หรือรายการของโหนดที่เสียหายจากแพ็กเก็ตที่ถูกร้องขอจากโหนดเหล่านั้น

เพราะ SRPต้องมีความสัมพันธ์ด้านความปลอดภัยระหว่างโหนดที่สื่อสารกันเท่านั้น จะใช้กลไกไลท์เวท (light-weight) มากเพื่อป้องกันการโจมตีอื่น ๆ ตัวอย่างเช่น เพื่อจำกัดการฟลัดดิ้ง (flooding) โหนที่บันทึกอัตราการส่งต่อของแพ็กเก็ต และให้ความสำคัญกับการส่งแพ็คเก็ตผ่านโหนดเพื่อนบ้านที่มีการส่งไม่บ่อยนัก กลไกดังกล่าวสามารถรักษาความปลอดภัยโปรโตคอลเมื่อมีผู้โจมตีน้อย อย่างไรก็ตามเทคนิคดังกล่าวจัดให้เป็นการโจมตีแบบเซคัลดารี (secondary) เช่นการส่งแพ็คเก็ตต้องการค้นหาเส้นทางปลอมเพื่อลดประสิทธิรูปของเส้นทางที่โหนดร้องขอ

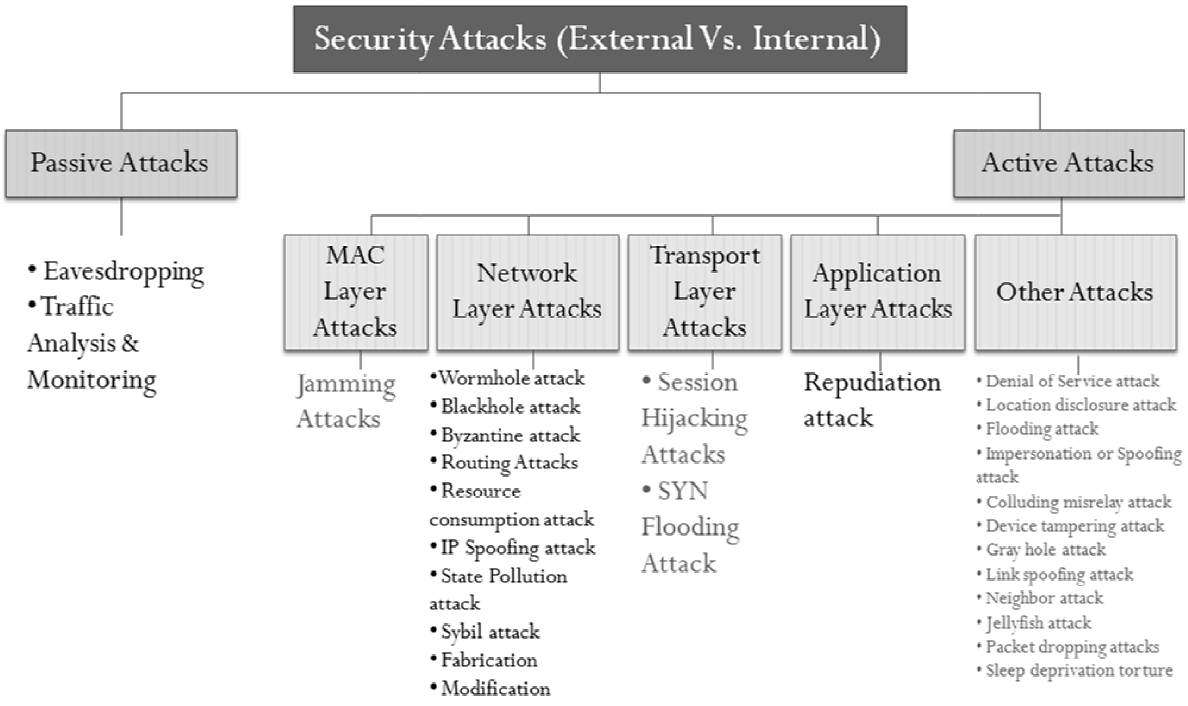
SRP ไม่พยายามที่จะถามที่อยู่ในการบำรุงรักษาเส้นทาง ใน SRP เช่นเดียวกับใน Ariadne มีการตอบกลับมากมายสำหรับหลายๆการร้องขอ โหนดที่ใช้ SMT เพื่อให้แน่ใจว่าส่งแพ็คเก็ตข้อมูลสำเร็จ ข้อความจะถูกแบ่งออกเป็นแพ็คเก็ต โดยใช้เทคนิคการแบ่งแบบซ่อนเร้นเพื่อที่ว่าถ้า M ออกจาก N แพ็คเก็ตดังกล่าวจะได้รับข้อความจะถูกสร้างขึ้นใหม่

2.3 ประเภทการโจมตีในเครื่อข่ายไร้สายแอดฮอค [8]

ประเภทการโจมตีแบ่งเป็น เอ็กเทอร์นอล (External) และ อินเทอร์นอล (Internal) การโจมตีแบบเอ็กเทอร์นอล (External) เป็นลักษณะการโจมตีจากภายนอก ก่อสัญญาณรบกวนการส่งข้อมูล สร้างความแออัดในการส่งสัญญาณข้อมูล การเปลี่ยนแปลงเส้นทางในการส่ง ส่วนการโจมตีแบบอินเทอร์นอล (Internal) นั้นเป็นลักษณะการโจมตีภายในเครือข่าย โดยการปลอมตัวเป็นโหนดที่ใช้รับส่งข้อมูลภายในเครือข่าย ลักลอบดักฟังข้อมูล ไม่ส่งต่อข้อมูล หรือเปลี่ยนแปลงทำลายข้อมูลที่ส่ง เป็นต้น

การโจมตีใน MANET ได้แบ่งการโจมตีไว้เป็น 2 ประเภทหลักคือ การโจมตีแบบพาสซีฟ (Passive attacks) และ การโจมตีแบบแอคทีฟ (Active attacks) ซึ่งอภิบายในรูปที่ 6

- **การโจมตีแบบพาสซีฟ (Passive Attacks)** การโจมตีที่ทำให้เครือข่ายไม่สามารถทำงานได้ปกติ เป็นลักษณะการดักฟังข้อมูล และอาจนำข้อมูลไปใช้ในทางเสียหาย การแก้ปัญหาของโจมตีในลักษณะนี้คือการใช้กลไกลการเข้ารหัสข้อมูล ในการส่งข้อมูลในเครือข่าย



รูปที่ 6 Different Type of attacks on MANET

- การดักฟังข้อมูล (Eavesdropping) เป็นการโจมตีที่มักเกิดขึ้นในเครือข่ายไร้สายแบบแอดฮอค แนวทางการป้องกันต้องรักษาความลับระหว่างการส่งข้อมูลในเครือข่ายมีกุญแจส่วนตัว (private key) สำหรับข้อมูลที่ต้องการรักษาความลับ หรือใช้รหัสลับ (password) ในการส่งต่อข้อมูลในแต่ละโหนด
- วิเคราะห์จราจรและการบำรุงรักษา (Traffic Analysis & Monitoring) ผู้โจมตีจะทำการวิเคราะห์การจราจรเส้นทางในเครือข่ายและการรักษาเส้นทางเพื่อหาแหล่งที่มา
- การโจมตีแบบแอคทีฟ (Active Attacks) ลักษณะการโจมตีแทรกแซงการทำงานของเครือข่าย การเปลี่ยนแปลงข้อมูลที่ผิดปกติ โดยการโจมตีลักษณะนี้สามารถเป็นทั้งแบบอินเทอร์นอลและเอ็กเทอร์นอลได้ ซึ่งการโจมตีแบบเอ็กเทอร์นอลจะดำเนินการจากโหนดนอกเครือข่าย และการโจมตีแบบอินเทอร์นอลจะเป็นการโจมตีภายในเครือข่ายโดยแฝงตัวเป็นส่วนใดส่วนหนึ่งในเครือข่าย การโจมตีในเครือข่ายนั้นมีมานานแล้ว โดยการโจมตีจากภายในจะรุนแรงกว่าการโจมตีจากภายนอก การโจมตีมีโหนดบุกรุก เช่น การเลียนแบบ, ปรับเปลี่ยน, ประดิษฐ์และการแทนที่ ดังภาพที่ 2 ที่ได้จำแนกประเภทการโจมตี
- **การโจมตีที่แมคเลเยอร์ (MAC LAYER ATTACKS)**
- การส่งสัญญาณรบกวน (Jamming attack) การรบกวน เป็นระดับการโจมตีของการโจมตีแบบ ดีโอเอส (DoS attacks) โดยมีวัตถุประสงค์ในการรบกวนการสื่อสารในเครือข่ายไร้สาย โดยสามารถทำให้การป้องกันแหล่งที่มาของข้อมูลจริงไม่สามารถส่งออกแพ็คเกจได้ หรือป้องกันการรับแพ็คเก็จ
- **การโจมตีที่เน็ตเวริ์คเลเยอร์ NETWORK LAYER ATTACKS**
- การโจมตีแบบวอร์มโฮล (Wormhole attack) เป้าหมายเพื่อปลอมแปลงเส้นทางการสื่อเพื่อให้ผู้บุกรุกทำหน้าที่นำส่งข้อมูล เพื่อในการแก้ไขหรือแอบฟังข้อมูลในเครือข่าย
- การโจมตีแบบแบล็คโฮล (Blackhole attack) มีลักษณะการโจมตี 2 ลักษณะ อย่างแรกคือการหาประโยชน์จากโหนดในการหาเส้นทางเครือข่ายไร้สายแบบแอดฮอค อย่างที่สองเป็นลักษณะการรับแพ็คเกตจากโหนดก่อนหน้า แต่ไม่ทำการส่งต่อไปยังโหนดถัดไป ซึ่งทำให้การบำรุงรักษาเครือข่ายไม่สามารถทำงานได้ปกติ อย่างไรก็ตามกระบวนการโจมตีของผู้บุกรุกมีความเสี่ยงจากโหนดข้างเคียงที่ไม่สามารถบำรุงรักษาและการโจมตีอย่างต่อเนื่อง ซึ่งรูปแบบการโจมตีที่ซับซ้อนยิ่งขึ้น จากการโจมตีเหล่านี้แพ็คเก็ตจะถูกส่งต่อโดยผู้บุกรุกทำการปรับเปลี่ยนแพ็คเก็ตหรือป้องกันบางโหนดที่ส่งมา ทำให้โหนดอื่นๆในเครือข่ายได้รับผลกระทบ

- การโจมตีแบบไบแซนไทน์ (Byzantine attack) เป็นลักษณะการสมรู้ร่วมทำในเครือข่าย เช่นการสร้างลูปการกำหนดเส้นทางการส่งต่อแพ็คเก็ตผ่านเส้นทางที่ไม่เหมาะสมหรือส่งแพ็คเก็ตลดลง ซึ่งทำให้เกิดการหยุดชะงักหรือการหยุดให้บริการเส้นทางในเครือข่าย
- การโจมตีแบบเร้าท์ทิง (Routing Attacks) มีลักษณะการโจมตีหลายลักษณะในการโจมตีการหาเส้นทางบนเครือข่าย ที่มีวัตถุประสงค์เพื่อขัดขวางการดำเนินงานการหาเส้นทางของโปรโตคอล ในบทความนี้จำกัดคำอธิบายดังนี้

1) เร้าท์ทิงเทเบิ้ลโอเว่อร์โฟลว์ (Routing Table Overflow) เป็นการโจมตีจากผู้บุกรุกที่สร้างเส้นทางให้ส่งไปยังโหนดที่ไม่มีอยู่จริง วัตถุประสงค์เพื่อสร้างเส้นทางใหม่หรือเพื่อเอาชนะโปรโตคอล อัลกลอริทึมการค้นหาเส้นทางของผู้โจมตีนั้นต้องการข้อมูลเส้นทางเดิมก่อน เพียงรอให้มีการสร้างอัลกอริทึมของเส้นทางเดิม ผู้บุกรุกก็สามารถส่งคำร้องหลอกไปยังเร้าเตอร์เพื่อให้ใช้เส้นทางใหม่
2) เร้าท์ทิงเทเบิ้ลพ้อยน์โซนิ่ง (Routing Table Poisoning) : โหนดที่บุกรุกในเครือข่ายส่งค่าการหาเส้นทางหลอกที่ทำการเปลี่ยนแปลงแล้วเพื่อปรับเปลี่ยนแพ็กเก็ตในการส่งต่อไปยังโหนดอื่นๆในเครือข่าย โดยโหนดที่ได้รับแพ็กเก็ตหลอกอาจมีผลในการทำงานเกิดการสับเปลี่ยนเส้นทางย่อย หรือทำให้บางส่วนของเครือข่ายไม่สามารถเข้าถึงได้
3) การทำแพ็กเก็ตซ้ำ (Packet Replication) : ลักษณะการโจมตีนี้จะทำการซ้ำแพ็คเก็ตเดิม ทำเกิดเพิ่มของแบนวิดส์และการใช้พลังงานแบตเตอร์รี่เพิ่มมาขึ้น และความสับสนในการกระบวนการค้นหาเส้นทาง
4) เร้าท์แคชพ้อยน์โซนิ่ง (Route Cache Poisoning) ในกรณีขึ้นอยู่กับรูปแบบการค้นหาเส้นทางตามความต้องการ (เช่น AODV[xx]) แต่ละโหนดจะบำรุงรักษาเส้นทางแคชข้อมูลที่ได้รับมาจากโหนดที่เคยส่งมาแล้ว มีวัตถุประสงค์คล้ายกับเร้าท์ทิงเทเบิ้ลพ้อยน์โซนิ่ง ที่ทำการแคชเส้นทาง
5) การโจมตีแบบรัชชิ่ง (Rushing Attack) รูปแบบการหาเส้นทางแบบตามความต้องการ นั้นใช้การป้องกันระหว่างในการค้นหาเส้นทางซึ่งมีความเสี่ยงในการถูกโจมตีสูง โหนดตรงข้ามได้รับแพ็คเก็ตร้องขอเส้นทางจากโหนดต้นทางที่ทำการส่งแพ็กเก็ตอย่างรวดเร็วทั่วทั้งเครือข่าย ทำให้โหนดที่อื่นที่ต้องการขอเส้นทาง ไม่สามารถตอบสนองความต้องการรอขอจากโหนดอื่นได้ โหนดที่ได้รับแพ็คเก็ตร้องขอเส้นทางที่ต้องถือว่าเป็นแพ็ตเก็ตเหล่านั้นเป็นรายการซ้ำกันทำให้เกิดทิ้งแพ็ตเก็ตเหล่านั้นที่ร้องขอมา เส้นทางใดที่ถูกคลุมด้วยโหนดต้นทางจะประกอบด้วยที่ตรงข้ามเป็นโหนดกลาง ดังนั้นโหนดต้นทางจะไม่สามารถหาเส้นทางที่ปลอดภัย, ที่อยู่, เส้นทางที่ไม่รวมโหนดที่ฝ่ายตรงข้าม ซึ่งเป็นการยากมากที่จะตรวจจับการโจมตีดังกล่าวในเครือข่ายไร้สายแบบแอดฮอค

- **การโจมตีเพื่อใช้งานทรัพยากร (Resource consumption attack)** การโจมตีที่ไม่สามารถให้เครือข่ายได้พักได้ ซึ่งเป็นการโจมตีหรือโหนดบุกรุกพยายามใช้งานพลังงานของโหนดในเครือข่ายในการหาเส้นทางที่มากเกินไป หรือทำให้การส่งแพ็ตเก็ตของโหนดที่ตกเป็นเหยื่อส่งไม่ได้
- การโจมตีแบบปลอมแปลงไอพี (IP Spoofing attack) ความยากลำบากในการตรวจสอบการใช้ทรัพยากร เมื่อโหนดใหม่เลือกสุ่มที่อยู่และการกระจายของสัญญาณในการตรวจจับแพ็คเก็ตในเครือข่ายไร้สายแบบแอดฮอค ซึ่งหลายๆ การป้องกันจากโหนดใช้ที่อยู่ ถ้าโหนดบุกรุกทำการครอบงำสมาชิกโหนดในเครือข่ายที่มีไอพีเดียวกันและจะทำการส่งคำปฏิเสธออกมา เรียกว่าการโจมตีแบบปลอมแปลงไอพี
- การโจมตีทำให้สภาพเกิดความเสียหาย (State Pollution attack) ถ้าโหนดบุกรุกให้ค่าที่ไม่ถูกต้องในส่งกลับนั้นเรียกว่า การโจมตีที่ทำให้สภาพเกิดความเสียหาย ตัวอย่างคือ การพยายามแจกจ่ายให้ดีที่สุด การแจกจ่ายจากโหนดบุกรุกสามาให้ส่งให้โหนดใหม่ได้แล้วโหนดใหม่ก็จะถูกครอบครองโดยโหนดบุกรุก ซึ่งนำไปสู่การส่งซ้ำ การทำเสนาข้อความที่อยู่เดิมในเครือข่ายและก็จะการปฏิเสธโหนดใหม่
- การโจมตีแบบไซบิล (Sybil attack) ถ้าโหนดบุกรุกทำการปลอมโหนดโดยซ่อนโหนดไว้ และโหนดบุกรุกจะเข้าทำงานแทน ในการโจมตีในลักษณะนี้ในการบริการเครือข่ายเมื่อเข้าสู่เครือข่ายแสร้งให้ความร่วมมือและจะตั้งค่าบางอย่างอัตโนมัติ ซึ่งความหลักการความปลอดภัยจะอนุญาตเพราะมีความเชื่อถือ อย่างไรก็ตามยังไม่มีวิธีการใดในการป้องกันในลักษณะนี้
- การสร้างขึ้นมาใหม่ (Fabrication) ทำการปรับเปลี่ยนเส้นทางหรือรบกวนการส่งแพ็ตเก็ตในเครือข่าย โหนดผู้ไม่หวังดีนั้นสามารถสร้างแพ็ตเก็ตขึ้นมาเป็นของตัวเองและสามารถทำการรบกวนการทำงานในเครือข่ายได้ โดยโจมตีโดยการปลอมข้อความและทำการโจมตีด้วยแพ็คเก็ตในเครือข่ายเช่น การทำให้เครือข่ายทำงานตลอดเวลาไม่ได้หยุดพักในการรอรับข้อมูล อย่างไรก็ตาม ข้อความที่ถูกปลอมจะไม่ทำงานแค่ในโหนดบุกรุก ซึ่งการทำงานดังกล่าอาจมาจากโหนดที่ทำการปรับปรุงภายในเครือข่ายได้
- การแก้ไข (Modification) ในข้อความที่ถูกปลอมแปลง จะทำข้อความที่ถูกส่งไปจะทำการค้นหาเส้นทางเปลี่ยนไปและเป็นอันตรายต่อแพ็คเก็ตที่สมบรูณ์ในเครือข่าย ซึ่งโหนดเครือข่ายไร้สาย

แบบแอดฮอคมีการเคลื่อนย้ายและจัดการทรัพยากรของตัวเองมีการเชื่อมต่อกับโหนดอื่นๆ บางครั้งก็อาจเชื่อกับโหนดบุกรุก โดยโหนดที่เป็นอันตรายเหล่านี้ใช้ประโยชน์จากการเชื่อมต่อนี้ เข้ามาในกระบวนการส่งต่อแพ็คเก็ต และหลังจากการทำงานของข้อความปลอม ตัวอย่างการโจมตีข้อความปลอมแบ่งได้เป็นแบบคือการทำให้เส้นทางขาดไปและการเปลี่ยนแปลงเส้นทาง

- **TRANSPORT LAYER ATTACKS**
- การโจมตีเซสชั่นไฮแจ็คกิ้ง (Session Hijacking attack) การใช้เซสชั่นเป็นที่นิยมในการสื่อสารมากที่สุด เพื่อเป็นการป้องการโดยตั้งค่าเซสชั่น (การให้สิทธิ) ในการโจมตีทีซีพีเซสชั่น ผู้บุกรุกจะทำการโจมตีไอพีแอดเดรสของเหยื่อ กำหนดหมายเลขซีเควน (sequence) ที่คล้ายว่าถูกต้องจากปลายทาง และจากนั้นทำการโจมตีเหยื่อในรูปแบบดีโอเอส ดังนั้นการโจมตีเลียนแบบโหนดที่เป็นเหยื่อและใช้เซสชั่นตามเป้าหมาย
- การโจมตีเอสวายเอ็ดฟลัดดิ้ง (SYN Flooding attack)
- การโจมตีแบบเอสวายเอ็ดฟลัดดิ้งคือการโจมแบบดีโอเอส ผู้บุกรุกจะสร้างหมายเลขจำนวนมากในการเปิดการเชื่อมต่อทีซีพีของโหนดเหยื่อ แต่ไม่สามารถทำได้สมบรูณ์เพราะเปิดการติดต่อแฮนด์เชร์ดเต็ม
- **การโจมตีในชั้นแอฟพลิเคชั่นเลเยอร์ (APPLICATION LAYER ATTACKS)**
- การโจมตีด้วยการทำซ้ำ (Repudiation attack) ในชั้นเน็ตเวร์ิคเลเยอร์ไฟล์วอลล์สามารถติดตั้งเพื่อเก็บแพ็กเก็ตเข้าออก ในชั้นเลเยอร์ทรานสปอตร์ การเชื่อมต่อทั้งหมดจะถูกเข้ารหัสแบบเอ็นทูเอ็น แต่ปัญหานั้นยังไม่ได้แก้ไขในการตรวจสอบสิทธิ์หรือปัญหาการเลียนแบบในทั่วไป การปฏิเสธเป็นส่วนหนึ่งของการติดต่อสื่อสาร เช่น การจัดการตนเองในการปฏิเสธกระบวนการจ่ายเงินของเครดิตการ์ด หรือปฏิเสธทุกๆรายการออนไลน์ของธนาคาร การโจมตีจะอยู่ในลักษณะระบบพาณิชย์
- **การโจมตีอื่นๆ OTHER ATTACKS**
- การโจมตีให้หยุดบริการ (Denial of Service attack) เป็นประเภทการโจมตีอื่น ที่มีการส่งแพ็คเก็ตเป็นจำนวนไปให้เครือข่าย ซึ่งแพ็คเก็ตที่หายไปเหล่านี้มีความสำคัญกับทรัพยากรเครือข่ายและการแนะนำช่องสัญญาณไร้สายและเครือข่ายในเอ็มเอเน็ตอีที โดยตารางการหาเส้นทางเกิดโอเวอร์โฟลว์จากการโจมตีและการโจมตีขัดขวางการพักมีสองประเภทของการโจมตีแบบดีโอเอส ในการตารางการค้นหาเส้นทางจะถูกโจมตีเกิดโอเว่อร์โฟลว์ เพื่อเป็นการทำลายเส้นทางการเดินทางของโหนด ทั้งหมดนี้ก็เพื่อทำให้มีการใช้งานแบตเตอรี่ของโหนดที่เป็นเหยื่อจนหมด
- การโจมตีเปิดเผยที่อยู่ (Location disclosure attack) ผู้บุกรุกเปิดเผยที่อยู่ของโหนดในเครือข่าย เช่นแผนที่เส้นทางและจากนั้นมีแผนการที่จะโจมตีต่อไป การวิเคราะห์การจราจร เป็นหนึ่งในส่วนของการโจมตีความปลอดภัยในเครือข่ายไร้สายแอดฮอคที่ยังไม่ได้แก้ไข ผู้บุกรุกพยายามที่จะระบุตัวตนที่ใช้สื่อสารและศึกษารูปแบบวิเคราะห์การจราจรและการติดตามรูปแบบจราจรที่เปลี่ยนแปลง โดยการรั่วไหลของข้อมูลดังกล่าวมีความเสียงมากในการรักษาความปลอดภัยบนเครือข่าย
- การโจมตีแบบพลัดดิ้ง (Flooding attack) ผู้บุกรุกจะใช้ทรัพยากรในเครือข่ายจนหมดสิ้น เช่นแบรนวิดส์และทรัพยากรของโหนด ได้แก่ การประมวลผลและพลังงานแบตเตอรรี่หรือเพื่อขัดขวางกระบวนการหาเส้นทาง ทำให้เส้นทางเครือข่ายเกิดการเสื่อมโทรมใช้งานไม่ได้ ตัวอย่างเช่น ในการหาค้นหาเส้นทางแบบเอโอดีวีโหนดบุกรุกจะส่งหมายเลขอาร์อาร์อีคิวจำนวนมากในช่วงเวลาสั้นที่ส่งถึงโหนดปลายทางทำให้ไม่สามารถส่งออกข้อมูลในเครือข่ายได้ เพราะว่าไม่มีการตอบกลับอาร์อาร์อีคิวเอส เพราะถูกโจมตีฟลัดดิ่งแล้ว ผลลัพธ์คือโหนดทั้งหมดใช้พลังงานแบตเตอรี่ แบรนวิดส์บนเครือข่ายถูกใช้และไม่สามารถให้บริการได้
- การเลียนแบบหรือปลอมแปลงโจมตี (Impersonation or Spoofing attack) การปลอมแปลงเป็นกรณีพิเศษของการโจมตีแบบความสมบูรณ์ โดยโหนดบุกรุกจะเลียนแบบโหนดตามลักษณะโหนดที่มีสิทธิ์ในการใช้งานในการค้นหาเส้นทางเครือข่ายไร้สายแอดฮอค วัตถุประสงค์หลักของการปลอมแปลงเพื่อบิดเบือนโครงสร้างเครือข่ายหรืออาจทำให้เกิดลูปในเครือข่าย ซึ่งขาดการตรวจสอบในการกำหนดเส้นทางโปรโตคอลสร้างการโจมตี ผลลัพธ์ที่เส้นทางในการส่งข้อความผิดพลาดและปลอม
- การโจมตีโดยการสมรู้ร่วมคิด (Colluding misrelay attack) ในการโจมตีในลักษณะนี้จะทำการงานโดยการแก้ไขหรือทิ้งแพ็คเก็ตหาเส้นทางซึ่งเป็นการขัดขวางกระบวนการทำงานในเครือข่ายไร้สายแอดฮอค โดยการโจมตีนี้มีความยากในการตรวจสอบจากการใช้แบบเดิม เช่นว้อทด็อก (watchdog) และ พารท์ราเทอร์ (pathrater)
- การแก้ไขอุปกรณ์ในการโจมตี (Device tampering attack) โหนดในเครือข่ายไร้สายแอดฮอคจะไม่เหมือนกับโหนดเครือข่ายที่มีสาย มีความกระชับ เบา และพวกพาสะดวก เป็นธรรมชาติ ซึ่งสามารถเกิดความเสียหายและสูญหายได้ง่ายกว่า ในการประมวลผลการค้นหา

เส้นทาง การควบคุมการสร้างข้อความจากโหนดแบบเดี่ยวและการตรวจสอบจากโหนดผู้รับนั้น การค้นหาเส้นทาง การป้องการโจมตีเกิดได้ง่ายเช่นการสร้างเส้นทางให้เป็นลูป การสร้างเส้นทางใหม่เพราะโหนดไม่สามารถสร้างและลักษณะแพ็ตเก็ต ชื่อปลอมหรือคิดค้นโหนด เพราะไม่มีการควบคุมจากศูนย์กลางของเครือข่ายทำให้ทำมีการเปลี่ยนแปลงหรือปลอมแปลงได้ง่าย

- การโจมตีเกรย์โฮล (Gray hole attack) การโจมตีลักษณะนี้มีสองลักษณะ ส่วนแรกโหนดบุกรุกจะหาประโยชน์จากรูปแบบการหาเส้นทางของเอโอดีวีโดยการโฆษณาตัวเองเป็นเส้นทางที่ถูกต้อง เพื่อต้องการสกัดกั้นการส่งแพ็คเก็ตในเส้นทางปลอม ในส่วนที่สองจะเป็นลักลอบทำลายโหนดในการรับส่งข้อมูลแพ็กเก็ต โดยการโจมตีเกรย์โฮลพฤติกรรมที่อันตรายด้วยวิธีการแตกต่างกัน ซึ่งอาจทิ้งแพ็กเก็ตที่มาจากโหนด(หรือโหนดปลายทาง) บางโหนดที่ถูกกำหนดในเครือข่ายที่มีการส่งต่อแพ็กเก็ตไปโหนดอื่นๆ โดยโหนดแต่ละชนิดของเกรย์โฮล อาจทำงานตามระยะเวลาที่ถูกกำหนดในการโจมตีอยู่ในแพ็คเก็ตเมื่อถึงเวลาก็จะเปลี่ยนพฤติกรรม หากเกรย์โฮลมีพฤติกรรมทั้งสองลักษณะรวมกัน จะสามารถทำให้ตรวจจับได้ยากมากยิ่งขึ้น
- โจมตีการปลอมแปลงการเชื่อมโยง (Link spoofing attack) ในการโจมตีลักษณะนี้โหนดบุกรุกทำการโฆษณาหลอกในการเชื่อมโยงกับโหนดเพื่อนบ้านเพื่อรบกวนการดำเนินกระบวนการหาเส้นทาง ในรูปแบบการหาเส้นทาง โอแอลเอสอาร์ ผู้โจมตีนั้นสามารถสร้างเส้นทางหลอกมีเป้าหมายคือโหนดเพื่อนบ้านสองโหนด โดยโหนดเป้าหมายที่ถูกเลือกในการทำลายนั้นเอ็มพีอาร์ โดยโหนดเอ็มพีอาร์โหนดบุกรุกสามารถจัดการข้อมูลหรือเส้นทางจารจรได้ เช่น การเปลี่ยนแปลงหรือทิ้งการหาเส้นทาง จนกระทั่งการทำงานโจมตีแบบดีโอเอส
- การโจมตีจากเพื่อนบ้าน (Neighbor attack) เมื่อได้รับแพ็กเก็ต โหนดจะบันทึกไอดีก่อนที่ส่งต่อแพ็คเก็ตไปยังโหนดถัดไป อย่างไรก็ตามถ้ามีผู้โจมตีการส่งแพ็คเก็ตจะไม่สามารถทำการบันทึกไอดีในแพ็คเก็ต โดยทำให้สองโหนดไม่สามารถสื่อสารกันได้ ซึ่งเชื่อว่าโหนดเพื่อนบ้านถ้าโหนดเพื่อนบ้านหายไป ส่งผลให้เส้นทางหยุดชะงัก
- การโจมตีแบบเจลลี่ฟิช (Jellyfish attack) การโจมตีในลักษณะนี้คล้ายกับการโจมตีแบบแบล็คโฮล โดยเจลลี่ฟิชการโจมตีครั้งมีความตั้งการที่จะก่อกวนในการส่งของกลุ่มและจากนั้นเมื่อการส่งเกิดความล่าช้าเพื่อจะใช้ถ่วงเวลาก่อนมีการส่งต่อ ส่งผลให้เกิดความล่าช้าแบบเอ็นทูเอ็น ซึ่งให้เกิดความล่าช้ากว่าประสิทธิภาพในการใช้งานจริง
- การโจมตีโดยการทิ้งแพ็กเก็ต (Packet dropping attacks) เป็นการขัดขวางการส่งข้อความในเส้นทางโดยตรงจากการทิ้งแพ็คเก็ต ในหลักการการโจมตีโดยการทิ้งแพ็คเก็ต ซึ่งผู้บุกรุกจะหลอกให้ความร่วมมือในการทำงานปกติระหว่างกระบวนการค้นหาเส้นทางและจเปิดการโจมตีด้วยการลดแพ็กเก็ต ซึ่งมีการเก็บรวบรวมอยู่ในโหนดหนึ่ง
- การขัดขวางการหลัด (Sleep deprivation torture) เป็นการโจมตีในลักษณะที่กำหนดในเครือข่ายไร้สายแบบแอดฮอค พบในการโจมตีในลักษณะนี้มานานหรือแม้ในเครือข่ายที่มีสาย แนวคิดการโจมตีคือเบื้องหลังการส่งคำร้องขอบริการ จะมีขอใช้งานบริการบางอย่างจากโหนด มากเกินไป ซึ่งจะทำให้โหนดผู้ให้บริการไม่สามารถที่จะหยุดให้บริการเกิดการใช้พลังงาน ไม่มีโอกาสได้พักการให้บริการ เหตุนี้สามารถทำลายเครือข่ายได้เนื่อโหนดมีทรัพยากรที่จำกัดเพราะพลังงานได้จากแบตเตอรี่ โดยนอกจากนี้ยังสามารถทำไปสู่เกิดการติดขัดทางธุรกิจได้

3. งานวิจัยที่เกี่ยวข้อง

ในบทความของ P.J.J. McNerney และ Ning Zhang [9] ได้กล่าวถึงความจำเป็นในการสนับสนุนการบรูณาการ เพื่อความปลอดภัยและคิวโอเอส ในสภาพที่เป็นอันตรายในเครือข่ายมาเน็ต ซึ่งได้นำเสนอแนวคิดวิธีการในการบรูณาการดังกล่าวเช่น การใช้วิธีการปรับการค้นหาเส้นทางแบบมัลติพาท์ เพื่อใช้ข้อมูลตามบริบทบรรเทาผลกระทบที่ได้จากการโจมตีแบบดีโอเอ โดยการตัดสินใจในการส่งมอบเส้นทางแบบชิงเกิ้ลพาท์ ไม่สามารถจองหรือการจองที่ใช้การปรับปรุงมาจากวิธีการค้นหาเส้นทางแบบมัลติพาท์ ซึ่งในบทความนี้ได้นำเสนอถึงการศึกษาการทดสอบ 2 หลักการ โดยใช้โปรโตคอลค้นหาเส้นทาง คือ ดีเอสอาร์ และ ไอเอ็นเอสไอจีเอ็นไอเอ คิวโอเอส เฟรมเวิร์ค (INSIGNIA QoS framework) ภายใต้โหนดโจมตีที่หลากหลาย จากการศึกษาพบว่า ไอเอ็นเอสไอจีเอ็นไอเอ มีประสิทธิภาพดีกว่าในด้านอัตราการส่งแพ็คเก็ต แม้ว่าระดับของผลที่รับจะแตกต่างกัน ปริมาณการโหลดและระดับการคุกคามที่อยู่ในเครือข่ายต้นแบบ การหาจุดต่อไปสู่การใช้ไฮบริดของการค้นหาเส้นทางแบบชิงเกิ้ลพาท์และมัลติพาท์ ที่มีการปรับตัวไปตามบริบทของเครือข่าย

ในบทความนี้ได้อธิบายถึง ไอเอ็นเอสไอจีเอ็นไอเอว่าเป็นคิวโอเอสเฟรมเวิร์ค ที่ออกแบบมาเฉพาะสำหรับมาเน็ตเอสไอพีเบส (MANETs IP-based) ซึ่งสนับสนุนสองระดับของคิวโอเอส : ส่งการจองเพื่อทราฟฟิคที่ความสำคัญมากและการส่งที่ดีที่สุด (best-effort delivery) สำหรักทราฟฟิคที่มีความสำคัญไม่มาก ไอเอ็นเอสไอจีเอ็ดไอเอ็นไอเอถูกออกแบบมาให้มีความเบาและการ

ปรับปรุงเพื่อตอบสนองการเปลี่ยนแปลงในเงื่อนไขของเครือข่ายและรูปแบบการเคลื่อนที่ สนองต่อการเปลี่ยนแปลงแบบไดนามิกในสภาวะเครือข่ายและโครงสร้าง โดยใช้อินแบนคิวโอเอส (in-band QoSs) จากการห่อห้อมข้อมูลในส่วนที่เพิ่มเติมของฟิลด์ไอพีในทุกๆแพ็คเกต [9]

N. Purohit, R. Sinha และ K. Maurya [10] ได้ศึกษาการลักษณะการประเมินการทิ้งแพ็ตเก็ตจากการส่งต่อข้อมูลของการโจมตีแบบแบล็คโฮลและเจลลี่ฟิช ในเส้นทางที่นำไปสู่เส้นทางที่ผิดเอ็นทูเอ็น (end-to-end) โปรโตคอลที่ใช้ในการควบคุมความแออัด โดยการโจมตีนี้เป็นไปตามโพรโทคอและยังมีผลกระทบร้ายแรงต่อทรูพุทของการปิดการไหลของลูป เช่นการไหลของทีซีพีและการจัดการความแออัดการไหลของยูดีพี เพื่อความสมบรูณ์ในบความนี้ได้พิจารณาการโจมตีแบล็คโฮล ที่มีผลกระทบต่อการเปิดการไหลของลูป กล่าวคือเหมือนกับผลกระทบของการโจมตีแบบเจลลี่ฟิชในการปิดการไหลของลูป โดยได้ศึกษาการโจมตีจากการทดสอบที่ใช้เอ็นเอสทรีและมีการแสดงถึงปริมาณความเสียที่เกิดขึ้น ซึ่งอาจแสดงถึงความประหลาดใจ เช่นการเพิ่มขึ้นของจำนวนการโจมตีของเครือข่ายไร้สายแอดฮอค ที่มีความกระหายทุกการไหลหลายฮอปและการแสดงถึงทุกทรัพยากรใช้ในการไหลหนึ่งฮอฟ ไม่สามารถจะดักจับได้จากเจลลี่ฟิชและแบล็คโฮล เช่นระบบการแบ่งพาร์ติชันที่ไม่พึงประสงค์อย่างชัดเจน คือยังพิจารณามาตรที่เท่าเทียมและจำนวนครั้งเฉลี่ยของฮอปส์สำหรับแพ็คเกตที่ได้รับเป็นมาตรการที่มีประสิทธิภาพที่สำคัญสำหรับระบบภายใต้การโจมตี อย่างไรก็ดีกลไกลการตรวจสอบที่สร้างในโหนดของเครือข่ายมาเน็ต ตามลำดับที่ระบุและแยกโหนดที่เห็นแก่ตัวจากเครือข่าย บางการเรียงลำดับของแรงกระตุ้นของกลไกลอาจรวมอยู่ในเครือข่ายการบังคับใช้ความร่วมมือระหว่างทุกโหนดในเครือข่ายมาเน็ต เพื่อปรับปรุงประสิทธิภาพเครือข่ายโดยร่วม [10]

การเลือกผู้นำของกลุ่มในการโจมตี (Group Leader Selection (GLS) attack) โหนดที่เป็นอันตรายสามารถเปิดการโจมตีกลุ่มการดำเนินการคัดเลือกผู้นำโดยการหลอกลวงที่ไม่ใช่สมาชิกกลุ่มเช่นเดียวกับสมาชิกในกลุ่มที่จะเป็นผู้นำกลุ่มแม้ว่าจะอยู่นอกมัลติแคสทรี

การเชื่อมโยงที่หลอกหลวง (False link breakage (FLB) attack) โหนดที่เป็นอันตรายสามารถเปิดการโจมตีต้นไม้มัลติแคสนี้ โดยกำหนดการเชื่อมโยงการปรับปรุงกระบวนการเชื่อมโยงสำหรบลิงค์ที่ขาดในมัลติแคสทรี การตัดแต่งกลุ่มผู้นำ (Group leader pruning (GLP) attack) โหนดที่เป็นอันตรายสามารถเปิดการโจมตีมัลติแคสทรีนี้โดยการตัดแต่งกิ่งผู้นำกลุ่มจากมัลติแคสทรี

เอ็มเอโอดีวี (MAODV Multicast Ad-hoc On-demand Distance Vector) [11] คือโปรโตคอลค้นหาเส้นทางแบบมัลติแคส สำหรับเครือข่ายแอดฮอค ซึ่งเป็นแบบไดนามิกโครงสร้างต้นไม้ที่ใช้ร่วมกันหลายผู้รับที่เชื่อมต่อสมาชิกในกลุ่มอาจจะผ่านบางโหนดที่ไม่ใช่สมาชิก โดยมีการปรับตัวที่รวดเร็วในการเชื่อมโยงแบบไดนามิกตามเงื่อนไข การประมวลผลต่ำ โอเว่อร์เฮดใช้หน่วยความจำที่ต่ำและการใช้เครือข่ายในระดับต่ำ ซึ่งจะสร้างมัลติแคสทรีแบบสองทิศทางที่ใช้ร่วมกันในการเชื่อมต่อแหล่งที่มามัลติแคสและผู้รับ โครงสร้างมัลติแคสทรีจะรักษากลุ่มสมาชิกในกลุ่มที่มีอยู่ภายในส่วนเชื่อมต่อของเครือข่าย แต่ละกลุ่มมัลติแคสโดยมีผู้นำกลุ่มที่มีความรับผิดชอบหือการรักษาหมายเลขลำดับของกลุ่มเพื่อใช้ในการยืนยันว่าเส้นทางนั้นมีความพร้อมส่งข้อมูลเสมอ

ในบทความนี้ [11] ได้สำรวจชนิดการโจมตีที่แตกต่างกัน ที่เผชิญหน้ากับกระบวนการเอ็มเอโอดีวี ซึ่งจะระบุและอธิบายถึงสามโปรโตคอลใหม่ที่ขึ้นอยู่กับโจมตีบนกระบวนการทำงานของเอ็มเอโอดีวี เช่น การโจมตีแบบจีแอลเอส (Group Leader Selection (GLS)) , เอฟแอลบี (False Link Breakage (FLB)) และ (Group Leader Pruning (GLP)) โดยได้จำลองสถานการณ์เพื่อแสดงผลกระทบต่อประสิทธิภาพของเครือข่าย ซึ่งได้จำลองการทดสอบประสิทธิภาพเอ็มเอโอดีวี ภายใต้การโจมตีอย่างหนักที่ขอบเขตที่ใหญ่ ดังนั้นจึงเสนอแนวทางรักษาความปลอดภัยสำหรับการโจมตีบนเอ็มเอโอดีวี จากการระบุการโจมตี ผลการจำลองแสดงให้เห็นว่าการตอบโต้มีประสิทธิภาพและมีประสิทธิภาพภายใต้การโจมตี โดยเฉพาะอย่างยิ่งเมื่อเทียบกับที่ไม่มีการรักษาความปลอดภัยของเอ็มเอโอดีวี , ตอบโต้ที่เสนอปรับปรุงพีดีอาร์ (Packet Delivery Ratio (PDR)) กับ 85% ค่าโอเว่อร์เฮดในการควบคุมเพิ่มเติมเพิ่มโดยการตอบโต้การเสนอเพิ่มค่าโอเวอร์เฮดไบต์โดยอัตราส่วนถึง 30% [11]

การโจมตีสมรู้ร่วมคิด (Colluding Injected Attack CIA) นอกจากนี้การโจมตีซีไอเอในพื้นที่ใกล้เคียงมีเป้าหมายที่จะทำให้เข้าใจผิดโหนดในการตรวจสอบแบบวิอทซ์ด๊อก (โหนดที่ใช้ในการตรวจสอบพฤติกรรมจากโหนดอื่น ๆ ในพื้นที่ใกล้เคียง) ในการรายงานอย่างไม่ยุติธรรมโหนดโจมตี (โหนดที่ถูกต้อง) เป็นพฤติกรรมประสงค์ร้ายในโหนดเพื่อนบ้าน

บทความนี้ได้นำเสนอในการโจมตีสมรู้ร่วมคิดซีไอเอซึ่งในฝ่ายตรงข้ามหลังจากที่สูญเสียโหนดที่ถูกต้อง จากนั้นจะทำการสร้างโหนดจำลองและมีการใส่เข้าไปในเครือข่ายหลังจากที่แยกโหนดที่ถูกบุกรุก ดังนั้นจึงไม่มีการตรวจจับโหนดอื่นจากนั้นฝ่ายตรงข้ามจะนำโหนดอื่นที่สมรู้ร่วมคิดกับจำลองแบบเพื่อเปิดการโจมตีที่มีวัตถุประสงค์เพื่อทำให้เข้าใจผิดก่อนหน้านี้การตรวจสอบรูปแบบในการรายงานโหนดโจมตีซึ่งเป็นโหนดที่ถูกต้องว่าเป็นอันตรายของมัน นอกจากนี้ด้วยการเปิดตัวการโจมตีครั้งนี้มีโหนดปลายทางโดยศัตรูจะป้องกันไม่ให้โหนดปลายทางที่ได้รับแพ็กเก็ตใด ๆ จากแหล่งที่มาจึงจะไม่สามารถตอบกลับด้วยข้อความใด ๆ ในสถานการณ์เช่นนี้มาอาจสรุปได้ว่าโหนดปลายทางคือที่เข้าไม่ถึง ผลการจำลองแสดงให้เห็นว่ารูปแบบการตรวจสอบก่อนหน้านี้อาจจะมีการนำเสนอผิด โดยการโจมตีของแบบสมรู้ร่วมคิด [12]

เจอาร์-เอสเอ็นดี-การค้นพบเพื่อนบ้านรบกวนยืดหยุ่นปลอดภัย (JR-SND jamming-resilient secure neighbor discovery) , การค้นพบเพื่อนบ้านรบกวนยืดหยุ่นปลอดภัยสำหรับโครงการมาเน็ตเอสตามลำดับคลื่นกระจายโดยตรงและการแพร่กระจายแบบสุ่มรหัสก่อนการกระจายออกไป โดยเจอาร์-เอสเอ็นดี ช่วยให้โหนดข้างเคียงที่จะค้นพบอย่างปลอดภัยซึ่งกันและกันด้วยความน่าจะเป็นที่ครอบงำแม้จะมีการปรากฏตัวของผู้ที่แทรกอยู่ทั่วไปทุกหนทุกแห่ง ในบความนี้ได้นำเสนอเจอาร์-เอสเอ็นดี, โครงการที่อยู่บนพื้นฐานดีเอสเอสเอสและการแพร่กระจายรหัสก่อนการจัดกระจายเพื่อให้เกิดการค้นพบเพื่อนบ้านรบกวนยืดหยุ่นในมาเน็ตเอส โดยเจอาร์-เอสเอ็นดี สามารถเปิดใช้งานทั้งสอง

โหนดข้างเคียงที่จะประสบความสำเร็จในการค้นพบอื่น ๆ แต่ละคนมีความน่าจะเป็นที่ครอบงำแม้จะมีอยู่ทั่วไปทุกหนทุกแห่งผู้ที่แทรกเข้าสู้เครือข่าย

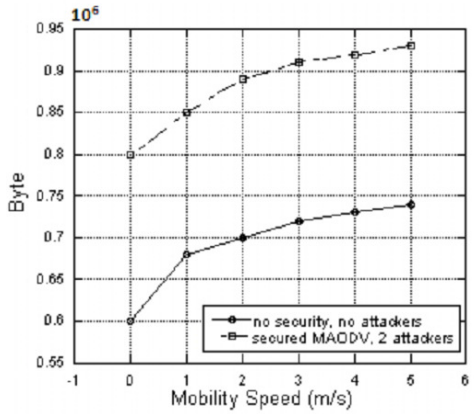


Fig. 7. Byte overhead for authentication

รูปที่ 7 Byte overhead for authentication [13]

รูปที่ [13] ให้ไบต์โอเวอร์เฮดที่เกิดจากการควบคุมโอเวอร์เฮดเพิ่มเติมซึ่งเพิ่มโดยการตอบโต้ที่เสนอ เนื่องจากในการควบคุมการตรวจสอบแพ็คเก็ตและขนาดที่เพิ่มขึ้นการควบคุมแพ็กเก็ต เปรียบเทียบกับที่ไม่มีหลักประกันของเอ็มเอโอดีวีโอเวอร์เฮดไบต์, ตอบโต้ด้วยการปรากฏตัวของสองที่ติดตาม, เพิ่มโอเวอร์เฮดไบต์โดยอัตราส่วนถึง 30% ซึ่งถือเป็นค่าที่สามารถยอมรับได้ ที่แสดงให้เห็นถึงการโจมตีที่มีผลกระทบมากเมื่อเทียบกับประสิทธิภาพของโปรโตคอล [13]

บทความนี้นำเสนอการศึกษาของการใช้สองคุณสมบัติการตรวจสอบเพื่อตรวจสอบการเกิดขึ้นของการโจมตีเอ็นเอเอสเอฟบนมาเน็ต โดยสมมติฐานพื้นฐานของการสืบสวนต้องอาศัยความจริงที่ว่าหลักฐานทางเครือข่ายที่มีการบันทึกอย่างถูกต้องและเก็บรักษา เพื่อนำมาวิเคราะห์ข้อมูลในทางกฎหมาย การตรวจหาคุณสมบัติตามการวิเคราะห์ทางสถิติของไฟล์ ไอดีเอส ล็อก(ดีเอฟ-1) IDS log (DF-1) และข้อมูลอัตราการไหล (ดีเอฟ-2) (DF-2) อัตราส่วนการตรวจสอบเวลาและอัตราการตรวจจับเท็จที่ใช้ในการประเมินประสิทธิภาพของการตรวจสอบเอ็นเอเอสเอ จากผลการจำลองแสดงให้เห็นว่าภายใต้รูปแบบการโจมตีที่แตกต่างกันรวมเข้าด้วยกันดีเอฟ-1 และ ดีเอฟ-2 มีความสามารถในการส่งมอบการตรวจจับการโจมตีที่เชื่อถือได้ของเอ็นเอเอสเอ [14]

ในบทความนี้ได้กล่าถึง หลักฐานทางเครือข่ายคือกระบวนการจับภาพ, การบันทึกและวิเคราะห์เหตุการณ์ที่เกิดในเครือข่าย เพื่อค้นหาแหล่งที่มาของการโจมตีหรือเหตุการณ์ปัญหาที่เกิดขึ้นอื่น ๆ ในบทความนี้ได้มุ่งเน้นในการวิเคราะห์ ซึ่งได้ตรวจสอบและจำลองการโจมตีเอเอสเอ็มในรูปแบบของเราที่ตรวจสอบพารามิเตอร์ ในการโจมตีทั้งสี่รูปแบบ แบบต่างๆ นอกจากได้นำเสนอรูปแบบการวิเคราะห์หารูปแบบเฉพาะของการจราจรโจมตีเอเอสเอฟ ผลลัพธ์ในการพัฒนานี้สามารถช่วยในการวิเคราะห์ตรวจสอบทางด้านหลักการวิทยาศาสตร์ของเครือข่าย ตรวจสอบว่ามีความผิดปกติในการจราจรและไม่ว่าผิดปกติคือการโจตีเอเอสเอฟ กำหนดเวลาในขณะที่การโจมตีจะเริ่มต้น [15]

โจมตีแบบวอร์มโฮลเป็นหนึ่งในอันตรายมากที่สุดในการรักษาความปลอดภัยจากการโจมตีบนเครือข่ายไร้สายมาเน็ต ท้ายสุดของการแก้ปัญหาที่อยู่ของการโจมตีแบบวอร์มโฮลในมาเน็ต มีความยากในการดำเนินการตรวจสอบประสิทธิภาพในการทำงานที่ดี โดยในบทความนี้ได้นำเสนอรวบรวมเปรียบเทียบและการวัดลักษณะการตรวจจับวอร์มโฮลของอาร์ทีที ซึ่งการใช้อาร์ทีทีระบุการโจมตีจากวอร์มโฮล และวัดลักษณะการเคลื่อนที่ที่รวมเข้าไปในโหนดเพื่อนบ้านจากรายการที่น่าสงสัย โดยการจำลองการทดสอบได้แสดงถึงโครงสร้างที่สามารถบรรลุอัตราการตรวจจับที่สูงและความถูกต้องในการเตือนภัย

โดยในบทความนี้ได้อธิบายถึง อาร์ทีที (round trip time (RTT)) ระหว่างสองโหนด จะทำการพิจารณามากยิ่งขึ้น โดยตรวจสอบหมายเลขของเพื่อนบ้าน ถ้าค่าของจำนวนเพื่อนบ้านมากกว่าจำนวน จำนวนเฉลี่ยเพื่อนบ้านโดยถ้าค่ามากกว่าค่าเฉลี่ย จะถูกส่งสัยว่ามีการเชื่อมโยงวอร์มโฮส์อยู่ในนั้น [16]

Po-Chun TSOU [16] ในบทความนี้ได้นำเสนอทดสอบความปลอดภัยโปรโตคอลค้นหาเส้นทางดีเอสอาร์ ที่มีชื่อบีดีเอสอาร์ (BDSR (Baited-Black-hole DSR)) โดยบีดีเอสอาร์ ตรวจสอบและหลีกเลี่ยงการโจมตีแบบแบล็คโฮลที่อยู่บนพื้นฐานของการรวมโครงสร้างแบบโปรแอคทีฟและรีแอคทีฟในเครือข่ายไร้สายมาเน็ต ซึ่งใช้การจำลองเสมือนจริงและใช้ที่อยู่ปลายทางโดยเหยื่อที่เป็นอันตรายจะตอกลับคำร้องอาร์อาร์อีพี ในบทความนี้มีข้อเสนอแนะในการรวมเอาข้อดีของการตรวจจับแบบโปรแอคทีฟที่สามารถหลีกเลี่ยงเพียงใจโครงสร้างแบบรีแอคทีฟที่ประสบความสำเร็จในการโจมตีแบล็คโฮลในระยะแรก ที่เหนือกว่านั้นคือการตอบสนองปฏิกริยาที่สามารถลดการสูญเสียของทรัพยากรได้ โดยใช้การจำลองด้วยเครื่องมือควัลเน็ต (QualNet) และเปรียบเทียบบีดีเอสอาร์ กับการตรวจจับแบบวิอทซ์ด๊อก บนหลักการทำงานในการส่งแพ็คเก็ตและค่าโอเวอร์เฮดของโปรโตคอลค้นหาเส้นทางดีเอสอาร์ ซึ่งผลลัพทธ์การจำลองนี้แสดงให้เห็นถึงประสิทธิภาพที่ดีของบีดีเอสอาร์ ในหลักการส่งแพ็คเก็ตที่ดีขึ้นและไม่มีเกิดค่าโอเวอร์เฮดมากในเครือข่าย การพัฒนาต่อจะมีการเพิ่มประสิทธิภาพและการตรวจสอบบีดีเอสอาร์ โดยจะทำการศึกษาโปรโตคอลที่สามารถด้านทานการโจมตีแบบแบล็คโฮลและการโจมตีแบบเกรย์โฮล

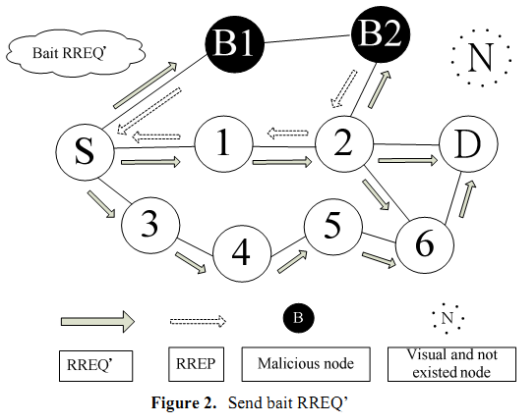


Figure 2. Send bait RREQ'

รูปที่ 8 การส่ง อาร์อาร์อีคิวของเหยื่อ [17]

ในบทความนี้ได้นำเสนอลักษณะทำงานของบีดีเอสอาร์ว่า เมื่อโหนดต้นทางเริ่มทำการค้นหาเส้นทาง จะทำการกระจ่ายเหยืออาร์อาร์อีคิว ที่อยู่

ตารางที่ 1. ตารางเปรียบเทียบการโจมตี

		DoS	Modifiation	Impersonation	Fabrication	Black-Hole	Wormhole	Rushing	Jellyfish	Flooding
Proactive	DSDV	√	√			√	√			
	SEAD					√				
	WRP									
	CGSR									
	STAR									
	OLSR	√				√	√			
	SLSP									
	FSR									
	HSR									
	GSR									
Reactive	DSR	√	√	√	√	√	√		√	√
	AODV	√	√	√	√	√	√	√	√	√
	AVR									
	SSA									
	FORP									
	FLBR									
	TORA									
	ABR							√		
	LAR									
	ARAN					√	√	√		
	SPREAD									
Hybrid	CEDAR									
	ZRP									
	SRP							√		
	ZHLS									

เป้าหมายของอาร์อาร์อีคิวถูกสุ่ม เสมือนและไม่มีอยู่จริง เพื่อหลีกเลี่ยงเครือข่ายที่เต็มไปด้วยอาร์อาร์อีคิว จากนั้นบีดีเอสอาร์ทำหน้าที่เหมือนกับอาร์อาร์อีคิวของดีเอสอาร์ อาร์อาร์อีคิวจะส่งกระจายอยู่ในช่วงเวลาหนึ่งเท่านั้น ซึ่งสามารถใช้ประโยชน์จากคุณสมบัติของการโจมตีแบบแบล็คโฮลที่สามารถหลอกหาเส้นทางที่สั้นที่สุดและส่งข้อมูลกลับไปยังโหนดโดยตรง โหนดที่เป็นเหยื่อแบล็คโฮลตอบกลับอาร์อาร์อีคิวจากกลไกนี้ เพราะอาร์อาร์อีคิวมีความสามารถในการแสดงที่อยู่ของโหนดที่เป็นอันตรายหลังจากการปรับเปลี่ยน โดยจะสามารถที่จะตรวจจับโหนดในเครือข่ายในช่วงเวลาที่กำหนด ขณะที่เหยื่ออาร์อาร์อีคิวกำลังส่งและกำลังรับจากโหนดประสงค์ร้าย ซึ่งมีการอ้างว่ามีข้อมูลเส้นทางไปยังที่อยู่เสมือนและที่ปลอมดังรูปที่ [17]

ในบทความนี้ได้กล่าวถึงความปลอดภัยของโปรโตคอลค้นหาเส้นทางเอโอดีวีในเครือข่ายไร้สายมาเน็ตซึ่งมีตรวจสอบโดยการระบุผลกระทบของการโจมตีแบบฟลัดดิ้ง การโจมตีนี้ในโปรโตคอลเอโอดีวีถูกจำลองเครือข่ายในเอ็นเอส-ทรี ซึ่งให้ผลลัพธ์ที่คล้ายกันโปรโตคอลดีเอสอาร์ มีข้อสังเกตว่าการปรากฏตัวของโหนดประสงค์ร้ายในเครือข่ายมาเน็ตที่พลัดดิ้ง มีผลกระทบต่อประสิทธิภาพในเครือข่ายไร้สายและสามารถทำหน้าที่อีกอย่างหนึ่งในการคุกความปลอดภัยที่สำคัญ จากการจำลองสามารถสรุปได้ว่า ผลกระทบจากฟลัดดิ้งในเครือข่าย มีค่าเฉลี่ยร้อยละของแพ็คเก็ตที่สูญหาย ค่าเฉลี่ยโอเวอร์เฮดในการค้นหาเส้นทาง และค่าเฉลี่ยความต้องการแบนวิดธ์ ที่เพิ่มขึ้นจึงลดการส่งผ่านเครือข่ายโดยรวม ซึ่งกลไกการตรวจสอบที่เข้มแข็งจะต้องดำเนินการในโหนดที่เคลื่อนของเครือข่ายมาเน็ตเพื่อการระบุและแยกจากฟลัดดิ้งที่ถูกบุกรุกโหนดจากเครือข่าย การเรียงลำดับของกลไกแรงที่อาจถูกจัดตั้งขึ้นในเครือข่ายที่มีการบังคับใช้ความร่วมมือระหว่างทุกโหนดในเครือข่ายมาเน็ต เพื่อปรับปรุงประสิทธิภาพของเครือข่ายโดยรวม [18]

C. King Sun [91] ได้ศึกษาการโจมตีแบบไบเซนไทน์วอร์มโฮลเป็นหนึ่งคุกคามการโจมตีความปลอดภัยในโทรศัพท์มือถือเครือข่ายแอดฮอค ซึ่งการแก้ปัญหาที่มีอยู่สำหรับการโจมตี ไบเซนไทน์วอร์มโฮลมุ่งเน้นไปที่ผลกระทบของการโจมตีบเซนไทน์วอร์มโฮล เช่น การทิ้งแพ็คเก็ตและตรวจจับเปลียนแปลงแพ็คเก็ตของไบเซนไทน์วอร์มโฮล ในบทความนี้ได้พยายามที่จะตรวจจับการโจมตีไบเซนไทน์วอร์มโฮลโดยตรง ซึ่งได้นำเสนอในการตรวจสอบความผิดปกติรูปแบบการเปลี่ยนแปลงเครือข่าย ซึ่งนำมาจากการโจมตีของบเซนไทน์วอร์มโฮล ด้วยการตรวจจับการโจมตีบเซนไทน์วอร์มโฮล โดยเชื่อมโยงภายใต้การโจมตีไบเซนไทน์วอร์มโฮล สามารถหลีกเลี่ยงได้อย่างสมบูรณ์ในระหว่างขั้นตอนการกำหนดเส้นทางและจึงจำกัด ผลกระทบจากการถูกไบเซนไทน์วอร์มโฮลให้น้อยที่สุด ผลการจำลองแสดงให้เห็นว่าโครงการสามารถบรรลุอัตราการตรวจจับสูงและความถูกต้องของการเตือนภัย การดำเนินการตามโครงการของเรายังเป็นที่เรียบง่าย [19]

4. สรุปผลและแนวทางการพัฒนา

เทคโนโลยีเครือข่ายไร้สายแอดฮอค (MANET) เป็นระบบเครือข่ายไร้สายที่สามารถแลกเปลี่ยนข้อมูล แต่มีข้อจำกัดด้านความเสี่ยง ความปลอดภัยในการส่งข้อมูลระหว่างเครือข่าย เนื่องจากโหนดที่ใช้ในการสื่อสารสามารถเคลื่อนที่ได้เป็นอิสระหรือการกระจายสัญญาณ ที่ทำให้อาจถูกโหนดที่ไม่ประสงค์ดีทำลายหรือขโมยข้อมูล ในเครือข่ายไร้สายแอดฮอค

ในบทความนี้มุ่งเสนอลักษณะการค้นหาเส้นทาง การโจมตีเครือข่ายไร้สายแอดฮอค และกระบวนการหาเส้นทางที่ปลอดภัยจากการโจมตีในรูปแบบต่างๆ

เอกสารอ้างอิง

[1] L. Abusalah, A. Khokhar and M. Guizani, "A survey of secure mobile Ad Hoc routing protocols," Communications Surveys & Tutorials, IEEE ,Vol.10, pp.78 - 93, 2008.

[2] D. B. Johnson, “Routing in Ad Hoc Networks of Mobile Hosts,” Proc. IEEE Wksp. Mobile Computing Systems and Applications, Dec. 1994.

[3] V. D. Park and M. S. Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks,” Proc. IEEE INFOCOM ’97, 1997, pp. 1405–13.

[4] C. E. Perkins and E. M. Royer, “Ad-Hoc On-Demand Distance Vector Routing,” Proc. 2nd IEEE Wksp. Mobile Computer Systems and Applications, 1999, pp. 90–100.

[5] T. H. Clausen et al., “The Optimized Link-State Routing Protocol, Evaluation through Experiments and Simulation,” Proc. IEEE Symp. Wireless Personal Mobile Communications 2001, Sept. 2001.

[6] M. Guerrero Zapata, “Secure Ad hoc On-Demand Distance Vector Routing,” Mobile Computing and Commun. Review, vol. 6, no. 3.

[7] Y. Hu and D. B. Johonson, “Securing Quality-of-Service Route Discovery in On-Demand Routing for Ad Hoc Networks,” Proc. ACM SASN ‘04, Oct. 20, 2004.

[8] PRADIP M. JAWANDHIYA, MANGESH M. GHONGE, DR. M.S.ALI and PROF. J.S. DESHPANDE, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology 2010, V.9, 2011.

[9] P.J.J. McNerney and Ning Zhang, "Towards an Integration of Security and Quality of Service in IP-Based Mobile Ad Hoc Networks," Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , pp. 1-6 , 2011.

[10] N. Purohit, R. Sinha and K. Maurya, "Simulation study of Black hole and Jellyfish attack on MANET using NS3," ,Engineering (NUiCONE), 2011 Nirma University International Conference on, pp. 1-5, 2011.

[11] A.M.A. Mo'men, H.S. Hamza and I.A. Saroit, "New attacks and efficient countermeasures for multicast AODV,", High-Capacity Optical Networks and Enabling Technologies (HONET), 2010, pp.51-57, 2010.

[12] F. Kandah, Y. Singh and W. Chonggang,"Colluding injected attack in mobile ad-hoc networks," Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, pp. 235-240, 2011.

[13] Z. Rui , Z. Yanchao and H. Xiaoxia, "JR-SND: Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks," Distributed Computing Systems (ICDCS), 2011 31st International Conference on, pp.529-538, 2011.

[14] G. Yinghua, I. Lee, "Forensic Analysis of DoS Attack Traffic in MANET," Network and System Security (NSS), 2010 4th International Conference on, pp. 293-298, 2010.

[15] G. Yinghua and M. Simon, "Network Forensics in MANET: Traffic Analysis of Source Spoofed DoS Attacks," Network and System Security (NSS), 2010 4th International Conference on, pp. 128 - 135, 2010.

[16] M. Rafiqul Alam and C. King Sun, "RTT-TC: A topological comparison based method to detect wormhole attacks in MANET," Communication Technology (ICCT), 2010 12th IEEE International Conference on, pp. 991 - 994, 2010.

[17] T. Po-Chun, C. Jian-Ming, L. Yi-Hsuan, C. Han-Chieh and C. Jiann-Liang, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs," Advanced Communication Technology (ICACT), 2011 13th International Conference on, pp. 755 - 760, 2011.

[18] A. Bandyopadhyay, S. Vuppala and P. Choudhury, "A simulation analysis of flooding attack in MANET using NS-3," Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, pp. 1 - 5, 2011.

[19] C. King Sun and M.R. Alam, "TCBWD: Topological comparison-based Byzantine wormhole detection for MANET," Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on, pp. 388 - 394, 2011.

[20]