

การตรวจจับการโจมตีแบบ Gray Hole บน Mobile Ad-Hoc Networks

แก้วใจ อารณพิศาล และ ศิริปรัชญ์ บุญครอง

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กรุงเทพฯ

Emails: nid_ke@hotmail.com, sirapatb@kmutnb.ac.th

บทคัดย่อ

การโจมตีแบบ Gray Hole เป็นการโจมตีชนิด Active Attack ของเครือข่ายเฉพาะกิจไร้สายแบบเคลื่อนที่ การโจมตีนี้มี 2 ระยะ คือ ระยะแรก โหนด Malicious ใช้โพรโทคอลค้นหาเส้นทางประกาศว่าตัวมันเองมีเส้นทางรับส่งข้อมูลที่ต้องการ และสั้นที่สุดที่จะไปยังโหนดปลายทาง ส่วนระยะที่สอง โหนด Malicious จะทำการดรอปปैคเก็ตข้อมูลที่ได้รับมาจากโหนดเพื่อนบ้าน และบางครั้งโหนดเหล่านี้จะกลับมาทำงานเป็นโหนดปกติอีกครั้ง ทำให้การตรวจจับทำได้ยาก และถ้าหากโหนด Malicious นี้อยู่ในเส้นทางการรับส่งข้อมูลที่สำคัญก็จะมีผลกระทบต่อระบบเครือข่ายเป็นอย่างมาก วิธีการแก้ไขปัญหาการโจมตีแบบ Gray Hole มีหลายลักษณะ คือ 1) การตรวจสอบแพ็กเก็ตเกิดตอบกลับเส้นทาง (Route Reply Packet: RREP) จากโหนดก่อนหน้า 2) การตรวจจับการดรอปปैคเก็ตข้อมูลด้วยโหนดผู้บุกรุก 3) การใช้งานระบบตรวจจับการบุกรุก และ 4) การตรวจจับโหนด Malicious ด้วยโพรโทคอลค้นหาเส้นทาง Ad-Hoc On-Demand Distance Vector (AODV)

คำสำคัญ – Gray Hole; เครือข่ายเฉพาะกิจไร้สายแบบเคลื่อนที่; ระบบตรวจจับการบุกรุก; AODV Routing Protocol

Abstract

Gray Hole attack is a type of active attack in Mobile Ad-Hoc Networks. This attack has two stages. First, the malicious node uses the ad-hoc routing protocol to announce itself as having a correct and shortest path to the destination node. Second, the malicious node drops the received data packets from the neighborhood's nodes, but later on these nodes will switch to the normal nodes again. This attack makes detection more difficult and if the malicious node is in the transmission of sensitive data, it will affect the network significantly. In order to mitigate the Gray Hole attack the following methods are used: 1) Checking the Route Reply Packet from the previous node 2) Drop-packet detection by Intruder node 3) Using an intrusion detection system and 4) Detecting the malicious node with the Ad-Hoc On-Demand Distance Vector Routing Protocol.

Keywords – Gray Hole; Mobile Ad-Hoc Networks; Intrusion Detection System; AODV Routing Protocol

1. บทนำ

ปัจจุบันเทคโนโลยีเครือข่ายแลนแบบไร้สายหรือ WLAN (Wireless LAN) กำลังได้รับความนิยมเป็นอย่างมาก เนื่องจากประโยชน์ของเครือข่ายแลนแบบไร้สายมีอยู่มากมาย โดยเฉพาะอย่างยิ่งเครือข่ายแลนแบบไร้สายสร้างความสะดวกและอิสระในการใช้งาน เทคโนโลยีสำหรับการเชื่อมต่ออุปกรณ์ต่างๆ ผ่านสื่อไร้สายที่รู้จักกันมีอยู่หลายเทคโนโลยี เช่น บลูทูธ, อินฟราเรด และ IEEE 802.11 เป็นต้น แต่ที่นิยมใช้กันอย่างแพร่หลายสำหรับเครือข่ายแลนแบบไร้สายคือ เทคโนโลยีตามมาตรฐาน IEEE 802.11 [1]

เครือข่ายเฉพาะกิจไร้สายแบบเคลื่อนที่ (Mobile Ad-Hoc Network: MANETs) เป็นระบบเครือข่ายไร้สายชั่วคราวที่สามารถเคลื่อนที่ได้โดยไม่มีการกำหนดรูปแบบที่แน่นอน โดยการรวมตัวของอุปกรณ์แบบพกพา เช่น สมาร์ทโฟน, โน้ตบุ๊กคอมพิวเตอร์ และเซินเซอร์ เป็นต้น หลายโหนดเข้าไว้ด้วยกัน การติดต่อสื่อสารจะทำงานเครือข่ายเฉพาะกิจไร้สายแบบเคลื่อนที่ที่มีลักษณะแตกต่างกัน เช่น การเปลี่ยนแปลงรูปแบบของโครงข่าย (Network Topology) ทำได้ตลอดเวลา, ไม่มีเราเตอร์ (Router) หรือสถานีแม่ (Access Point) ในการติดต่อสื่อสารระหว่างโหนด แต่ละโหนดจึงทำหน้าที่เป็นทั้งเราเตอร์ (Router) และโฮสต์ (Host) เพื่อส่งต่อแพ็กเก็ตและรับแอปพลิเคชันในเวลาเดียวกัน [2]

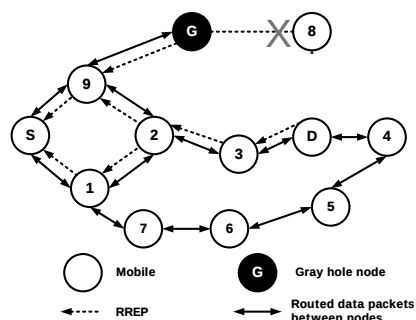
การโจมตีบน Network Layer ประกอบด้วย 1) การโจมตีแบบ Black Hole คือ โหนด Malicious แจ้งโปรโตคอลค้นหาเส้นทางว่า โหนด Malicious มีเส้นทางไปยังโหนดปลายทางที่ถูกต้องและสั้นที่สุด 2) การโจมตีแบบ Worm Hole ฝ่ายตรงข้ามสามารถสมรู้ร่วมคิดที่จะส่งเส้นทางและแพ็กเก็ตอื่นออกมายังโหนด Worm Hole 3) การโจมตีแบบ Gray Hole คือ โหนด Malicious จะมีวิธีการโจมตีที่แตกต่างจากการโจมตีแบบ Black Hole โดยบางครั้งโหนด Malicious จะทำการดริบดแพ็กเก็ตที่

เข้ามาจากโดยโหนดสำคัญในเครือข่าย ในขณะที่กำลังส่งต่อไปยังโหนดถัดไป จากนั้นโหนด Malicious จะกลับมาทำงานเป็นโหนดปกติ [3]

โดยบทความนี้จะกล่าวถึงเรื่องการตรวจจับการโจมตีแบบ Gray Hole บน Mobile Ad-Hoc Networks โดยเนื้อหาในบทความนี้ประกอบไปด้วย ส่วนที่ 2 กล่าวถึงการโจมตีแบบ Gray Hole, ส่วนที่ 3 วิธีการแก้ปัญหาการโจมตีแบบ Gray Hole, ส่วนที่ 4 การเปรียบเทียบ ส่วนที่ 5 บทสรุป, และส่วนที่ 6 กล่าวถึงเอกสารอ้างอิงที่ได้ศึกษา

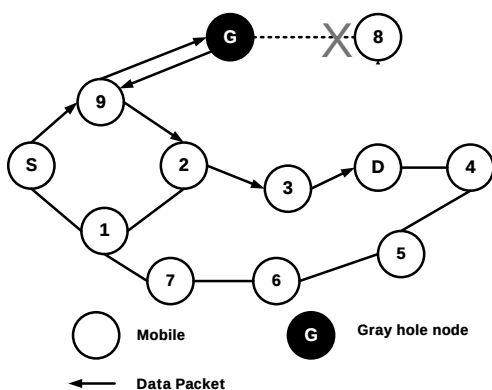
2. การโจมตีแบบ Gray Hole

การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS) มีหลายแบบโดยหนึ่งในนั้นคือ การโจมตีแบบ Gray Hole โดยเริ่มต้นจากโหนด Malicious จะทำงานเป็นโหนดปกติ เมื่อเวลาผ่านไปจะทำงานเป็นโหนด Malicious เลือกแพ็กเก็ตข้อมูลที่ส่งมาจากโหนดก่อนหน้าแล้วดริบดแพ็กเก็ตข้อมูลอย่างเจียบ ๆ ก่อนที่จะถึงโหนดปลายทาง [4] การโจมตีแบบ Gray Hole เป็นการโจมตีที่การตรวจจับได้ยากกว่าการโจมตีแบบอื่น ๆ เนื่องจากโหนด Malicious จะพรางตัวปะปนกับโหนดทั่วไป บางครั้งทำตัวเป็นปกติโดยการส่งข้อมูลให้ บางครั้งก็ดริบดแพ็กเก็ตข้อมูลบางส่วนทิ้งไป ซึ่งแตกต่างจากการโจมตีแบบ Black Hole ที่จะดริบดแพ็กเก็ตข้อมูลทิ้งไปทั้งหมด



รูปที่ 1. การโจมตีแบบ Gray Hole [5]

จากรูปที่ 1 การโจมตีแบบ Gray Hole พบว่า โหนดต้นทาง (S) ทำการบรอดคาสต์ (Broadcast) แพ็กเก็ตร้องขอเส้นทาง (Route Request Packet: RREQ) ไปยังโหนดเพื่อนบ้านใกล้เคียง เมื่อโหนด Gray Hole ได้รับแพ็กเก็ตร้องขอเส้นทางที่ส่งมา จะทำการส่งแพ็กเก็ตตอบกลับเส้นทาง (Route Reply Packet: RREP) กลับมายังโหนดต้นทาง [5] เมื่อโหนดต้นทางได้รับแพ็กเก็ตตอบกลับเส้นทางจากโหนด Gray Hole ก่อนโหนดเพื่อนบ้านอื่น ๆ โหนดต้นทางยกเลิกได้รับแพ็กเก็ตตอบกลับเส้นทางทั้งหมด และโหนดต้นทางเริ่มต้นส่งแพ็กเก็ตข้อมูลไปยังโหนดปลายทาง (D) ตามตารางเส้นทาง (Routing Table)



รูปที่ 2. การส่งแพ็กเก็ตข้อมูลของการโจมตีแบบ Gray Hole

จากรูปที่ 2 โหนดต้นทางส่งแพ็กเก็ตข้อมูลไปยังโหนด 9 จากนั้น โหนด 9 จะส่งต่อไปยังโหนด Gray Hole โหนด Gray Hole เลือกตอบแพ็กเก็ตข้อมูลจำนวนหนึ่งทิ้งไป และส่งแพ็กเก็ตข้อมูลส่วนใหญ่ที่ผ่านมาในระหว่างการส่งข้อมูลไปยังโหนดปลายทาง [6] และเมื่อถึงเวลาที่ปรับการทำงานของโหนด Gray Hole กลับมาทำงานเป็นโหนดปกติอีกครั้ง

จากตัวอย่างข้างต้นอธิบายเป็นขั้นตอนได้ดังนี้ ขั้นตอนแรก การโจมตีแบบ Gray Hole นั้นเป็นการหลอกให้

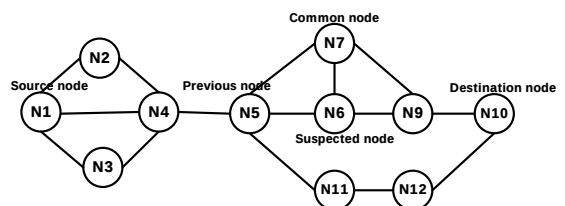
โหนดต่างๆ ส่งข้อมูลผ่านโหนด Gray Hole เพื่อประโยชน์ในการดักจับข้อมูล และบางทีก็กีดกันไม่ให้ข้อมูลไปถึงโหนดปลายทาง ขั้นตอนที่ 2 โหนด Gray Hole ประกาศให้โหนดต่างๆ ให้เข้าใจผิดว่า โหนด Gray Hole มีเส้นทางที่ดีที่สุดสำหรับส่งข้อมูลไปโหนดปลายทางที่โหนดเหล่านั้นต้องการส่งข้อมูลไป โดยไม่สนใจว่า ที่จริงแล้วโหนด Gray Hole นั้นจะมีเส้นทางส่งต่อข้อมูลหรือไม่ และขั้นตอนสุดท้าย โหนดต่างๆ ที่โดนหลอกก็จะส่งข้อมูลผ่านโหนด Gray Hole เพื่อขอให้ช่วยส่งต่อ ถ้าโหนด Gray Hole ไม่มีเส้นทางส่งต่อ ข้อมูลจะถูกดักจับ แต่ถ้ามันมีเส้นทางส่งต่อข้อมูลให้ได้ โหนด Gray Hole ก็จะเลือกแบบสุ่มว่า เมื่อใดมันจะส่งต่อให้ข้อมูลนั้นให้ หรือจะดักจับข้อมูลนั้นทิ้งไป

3. วิธีการแก้ปัญหการโจมตีแบบ Gray Hole

การตรวจสอบการโจมตีแบบ Gray Hole มีหลายแบบดังนี้

3.1 การตรวจสอบแพ็กเก็ตตอบกลับเส้นทาง (Route Reply Packet: RREP) ที่ส่งมาจากโหนดก่อนหน้า

ในโพรโทคอลค้นหาเส้นทาง Ad-Hoc On-Demand Distance Vector (AODV) นั้น แต่ละโหนดจะมีการเก็บข้อมูลโหนดเพื่อนบ้าน



รูปที่ 3. เครือข่ายไร้สายเฉพาะกิจแบบเคลื่อนที่ [4]

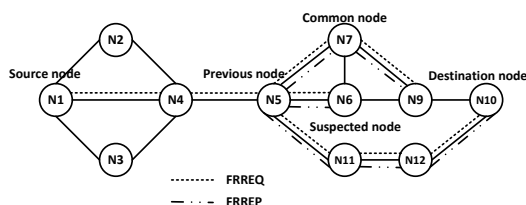
จากรูปที่ 3 โหนด 1 ทำการแพร่กระจายหรือเรียกว่า บรอดคาสต์ (Broadcast) แพ็กเก็ตร้องขอเส้นทาง (Route Request Packet: RREQ) ไปยังโหนดเพื่อนบ้าน ถ้าโหนดเพื่อนบ้านเป็นโหนดปลายทางก็จะส่ง แพ็กเก็ตตอบกลับเส้นทางกลับมายังโหนดต้นทาง และทำการปรับปรุงตารางเส้นทาง (Routing Table)

การตรวจสอบแพ็กเก็ตตอบกลับเส้นทางที่ส่งมาจากโหนดก่อนหน้ามีระยะทาง 1 hop มีขั้นตอนที่ 1 เก็บแพ็กเก็ตตอบกลับเส้นทางจากโหนดก่อนหน้า จะเห็นได้ว่าโหนด 7 เป็นโหนดเพื่อนบ้านของโหนด 6 ซึ่งเป็นโหนดต้องสงสัย ทำให้โหนด 7 มีลักษณะเป็นโหนด Cooperative โดยจะช่วยเหลือโหนด 6 และส่งแพ็กเก็ตตอบกลับเส้นทางปลอม (False Route Reply: FRREP) ไปยังโหนดก่อนหน้าว่า โหนดต้องสงสัยเป็นเส้นทางที่ถูกต้อง ทำให้โหนดต้นทางส่งแพ็กเก็ตข้อมูลมาตามเส้นทางดังกล่าว และโหนดต้องสงสัยทำการดรอปปข้อมูลบางแพ็กเก็ต ทำให้ข้อมูลไปไม่ถึงโหนดปลายทาง ดังตารางที่ 1

ขั้นตอนที่ 2 ตรวจสอบระยะ 2 hop ของโหนดต้องสงสัย ไปยังโหนดปลายทาง

ตารางที่ 1. ระยะ 1 hop ของโหนดต้องสงสัย [4]

NODE	Node	Node	Node	Node
6	5	7	9	10



รูปที่ 4. การขอเส้นทางจากโหนดก่อนหน้า [4]

จากรูปที่ 4 โหนดก่อนหน้าจะตรวจสอบตารางจัดเส้นทางของโหนดปลายทางว่า โหนด 6 มีระยะทาง 1 hop ไปยังโหนดปลายทางหรือไม่ ถ้าไม่ใช่ระยะทาง 1 hop แล้ว โหนด 6 และโหนด 7 จะถูกเพิ่มลงในตารางโหนด Black Listed และในขั้นตอนสุดท้าย แพ็กเก็ตร้องขอเส้นทางใหม่ (Fresh Route Request Packet: FRREQ) ส่งไปถึงโหนดก่อนหน้าและหากไม่มีระยะทาง 1 hop จากโหนดต้องสงสัย โหนดปลายทางปฏิเสธแพ็กเก็ตตอบกลับเส้นทาง และบรอดคาสต์แจ้งเตือนโหนดอื่นๆ ในเครือข่าย [4]

3.2 การตรวจจับการดรอปปแพ็กเก็ตข้อมูลด้วย

โหนดผู้บุกรุก

การตรวจจับโหนด Malicious ที่ทำการดรอปปแพ็กเก็ตข้อมูลด้วยโหนดผู้บุกรุก โดยวิธีการนี้โหนดต้นทางส่งข้อความเริ่มต้น (Prelude Message) ไปยังโหนดปลายทางก่อนการส่ง เพื่อแจ้งเกี่ยวกับจำนวนแพ็กเก็ตข้อมูลที่ส่ง แต่โหนดในเส้นทางจะทำการมอนิเตอร์การจราจรบนเครือข่าย โหนดเพื่อนบ้านจะทำการนับจำนวนแพ็กเก็ตข้อมูลที่ส่งมา และได้รับข้อมูลจำนวนแพ็กเก็ตข้อมูลที่ส่งมาจากโหนดต้นทาง โหนดเพื่อนบ้านของแต่ละโหนดจะเปรียบเทียบจำนวนแพ็กเก็ตข้อมูลที่นับได้กับจำนวนแพ็กเก็ตข้อมูลที่ส่งมาจากโหนดต้นทาง ถ้าหากจำนวนแพ็กเก็ตข้อมูลไม่ตรงกัน โหนดเพื่อนบ้านจะตอบกลับไปหาโหนดต้นทางด้วยข้อความสรุปจำนวนแพ็กเก็ตที่ได้รับ (Postlude Message) เพื่อให้โหนดต้นทางนำข้อมูลที่ได้ไปตรวจสอบจะหาข้อมูลที่หายไประหว่างการส่ง และเริ่มกระบวนการตรวจจับโหนด Malicious และนำโหนด Malicious ออกจากเครือข่าย [7]

3.4.3 โมดูลตรวจจับความผิดปกติของโหนด

Cooperative

โมดูลนี้เพิ่มความน่าเชื่อถือในการตรวจจับด้วยการลดความเป็นไปได้ที่จะพบความผิดพลาดของโมดูลการตรวจจับความผิดปกติของโหนด Local

ตารางที่ 3. ProbeCheck for Node 5

NID (NODE ID)	PROBE STATUS
4	1
7	0
11	1

เมื่อโหนดเริ่มต้นบรอดคาสต์ข้อความตรวจจับโหนด Cooperative ไปยังโหนดเพื่อนบ้านทุกโหนดของโหนดต้องสงสัย เมื่อโหนดเพื่อนบ้านได้รับข้อความดังกล่าวแล้วแต่ละโหนดจะส่งแพ็กเก็ตร้องขอเส้นทางไปยังโหนดต้องสงสัย เพื่อหาเส้นทางไปยังโหนดเริ่มต้น หลังจากนั้นโหนดต้องสงสัย จะส่งแพ็กเก็ตตอบกลับเส้นทางกลับมาแต่ละโหนดเพื่อนบ้านจะทำการส่ง Probe Packet ไปยังโหนดเริ่มต้นตามเส้นทาง เส้นทางนี้จะพบว่ามีโหนดต้องสงสัย จากตารางที่ 3 พบว่า โหนด 5 ได้รับ Probe Packet จากโหนดเพื่อนบ้านทั้งหมดของโหนดต้องสงสัย ยกเว้นโหนด 7 เป็นไปได้ว่าโหนด 7 อาจจะถูกดักจับด้วยโหนดต้องสงสัย หรือมีการชนกันของข้อมูลทำให้ Probe Packet หายไป ดังนั้นเพื่อหลีกเลี่ยงการชนกันหรือบัฟเฟอร์เต็มที่โหนดต้องสงสัย แต่ละโหนดจะส่ง Probe Packet 3 แพ็กเก็ต ในช่วงเวลาสั้น ๆ ถ้าไม่มีทั้ง 3 แพ็กเก็ตส่งจากโหนดเพื่อนบ้านมาถึงโหนดเริ่มต้นก็แสดงว่าโหนดต้องสงสัยมีพฤติกรรมเป็นการโจมตีแบบ Gray Hole โดยอาจจะจะมี 1 โหนด หรือมากกว่านั้น

3.4.4 โมดูลแจ้งเตือนการโจมตีแบบ Gray Hole

ระบบแจ้งเตือนทำการส่งข้อความเตือนที่มีลงลายมือชื่ออิเล็กทรอนิกส์ ไปยังทุกโหนดบนเครือข่ายเกี่ยวกับโหนด Malicious ที่ตรวจจับได้โดยโมดูลการตรวจจับความผิดปกติของโหนด Cooperative [9-10]

4. การเปรียบเทียบ

ผลการเปรียบเทียบข้อดีและข้อจำกัดของวิธีการแก้ไขปัญหาการโจมตีแบบ Gray Hole แสดงดังตารางที่ 4

จากการเปรียบเทียบวิธีการแก้ไขปัญหาการโจมตีแบบ Gray Hole ดังตารางที่ 4 พบว่า การตรวจจับโหนด Malicious ด้วยโพรโทคอลค้นหาเส้นทาง AODV เป็นวิธีการที่ดีที่สุดทั้งหมด 4 วิธีที่นำเสนอ เนื่องจากอัตราการรับส่งแพ็กเก็ตข้อมูลจากโหนดต้นทางไปยังโหนดปลายทางอยู่ที่ระดับร้อยละ 90 ขึ้นไป ขึ้นอยู่กับจำนวนโหนดที่มีในเครือข่าย [9] วิธีนี้เพิ่มประสิทธิภาพเครือข่ายเฉพาะกิจไร้สายแบบเคลื่อนที่ที่สามารถรับส่งข้อมูลได้ปลอดภัยจากการโจมตีแบบ Gray Hole มากขึ้น

5. บทสรุป

การโจมตีแบบ Gray Hole เป็นการโจมตีที่ผู้โจมตีทำให้เข้าใจผิดบนเครือข่ายโดยการส่งแพ็กเก็ตข้อมูล โดยเมื่อโหนด Malicious ได้รับแพ็กเก็ตข้อมูลจากเพื่อนบ้าน จะทำการดักจับแพ็กเก็ตข้อมูล และทำการโจมตีแบบปฏิเสธการให้บริการ ภายหลังการโจมตีสิ้นสุดลง โหนด Malicious จะกลับมาทำงานปกติ ในบทความนี้ได้นำเสนอลักษณะของการโจมตีแบบ Gray Hole จากนั้นจึงนำเสนอวิธีการตรวจจับเพื่อแก้ปัญหาการโจมตี ซึ่งจะช่วยทำให้ผู้สนใจในการโจมตีแบบ Gray Hole เข้าใจและเกิดแนวคิดในการนำไปใช้งานหรือเป็นจุดเริ่มต้นในการทำวิจัยเกี่ยวกับการตรวจจับการโจมตีแบบ Gray Hole บน Mobile Ad-Hoc Networks

ผลการสำรวจพบว่า แนวทางการตรวจจับการโจมตีแบบ Gray Hole บน Mobile Ad-Hoc Networks นั้นมี 4 แนวทาง คือ 1) การตรวจสอบแพ็กเก็ตเกิดตอบกลับเส้นทาง (Route Reply Packet: RREP) ที่ส่งมาจากโหนดก่อนหน้านี้ ซึ่งสามารถทำการตรวจจับโหนด Malicious ได้มากกว่า 1 โหนด 2) การตรวจจับการรีปแพ็กเก็ตเกิดข้อมูลด้วยโหนดผู้บุกรุก ทำให้ได้เส้นทางที่ปลอดภัยจากการโจมตีแบบ Black/Gray Hole 3) การใช้งานระบบตรวจจับการบุกรุก เป็นการเพิ่มความปลอดภัยให้แก่โพรโทคอลค้นหาเส้นทาง ทำการรับส่งข้อมูลอยู่ในร้อยละ 80.40 และ 4) การตรวจจับโหนด Malicious

ด้วยโพรโทคอลค้นหาเส้นทาง AODV เป็นการเพิ่มความน่าเชื่อถือของการตรวจจับด้วยอัลกอริธึม Collaborative and Distributed ที่มีอัตราการรับส่งแพ็กเก็ตข้อมูลจากโหนดต้นทางไปยังโหนดปลายทางที่ระดับร้อยละ 90 ขึ้นไป

จากแนวทางที่กล่าวมาทั้งหมดนั้นสามารถแก้ปัญหาการโจมตีแบบ Gray Hole ได้ในระดับหนึ่งเท่านั้น ยังคงต้องมีการปรับปรุงการตรวจจับเหล่านี้ให้มีประสิทธิภาพมากขึ้นต่อไป

ตารางที่ 4. การเปรียบเทียบวิธีแก้ไขปัญหการโจมตีแบบ Gray Hole

วิธีการแก้ปัญหา	ข้อดี	ข้อจำกัด
การตรวจสอบแพ็กเก็ตเกิดตอบกลับเส้นทาง (Route Reply Packet: RREP) ที่ส่งมาจากโหนดก่อนหน้านี้ มีระยะทาง 1 hop [4]	เทคนิคการตรวจจับการโจมตีกลุ่มแบบ Gray Hole ผ่านโหนดปลายทาง สามารถตรวจจับโหนด Malicious ได้มากกว่า 1 โหนด	อัลกอริธึมที่นำเสนอต้องทำการตรวจสอบแพ็กเก็ตเกิดตอบกลับเส้นทางที่ได้รับมาจากโหนดก่อนหน้านี้ทุกครั้ง เพื่อตรวจสอบว่าแต่ละโหนดมีลักษณะเป็นโหนด Malicious และโหนด Cooperative
การตรวจจับการรีปแพ็กเก็ตเกิดข้อมูลด้วยโหนดเริ่มต้นโหนดผู้บุกรุก [7]	เป็นการค้นหาเส้นทางที่ปลอดภัยในการส่งข้อมูลจากโหนดต้นทางไปยังปลายทาง โดยหลีกเลี่ยงการโจมตีแบบ Black/Gray Hole	วิธีการที่นำเสนอนั้นยังไม่มีมีการทดสอบประสิทธิภาพในเรื่องของ Throughput, Overhead และ False Positives
การใช้งานระบบตรวจจับการบุกรุก (Intrusion Detection System: IDS) [8]	เป็นการพัฒนาโพรโทคอลค้นหา AODV ให้มีความปลอดภัย โดยเปลี่ยนเป็น IDSAODV และเพิ่มประสิทธิภาพของเครือข่าย โดยอัตราการรับส่งข้อมูลร้อยละ 80.40 ที่จำนวน 7 โหนด	วิธีการนี้เป็นการใช้งาน IDS ในการตรวจจับโหนด Malicious นี้ทำการทดสอบกับโพรโทคอลค้นหาแบบ AODV เท่านั้น
การตรวจจับโหนด Malicious ด้วยโพรโทคอลค้นหาเส้นทาง AODV [9-10]	กลไกการรักษาความปลอดภัยที่นำเสนอนี้เพิ่มความน่าเชื่อถือของการตรวจจับด้วยอัลกอริธึม collaborative and distributed มีผลต่อโหนดเพื่อนบ้านของโหนด Malicious	กลไกที่นำเสนอจะเหมาะกับโพรโทคอลค้นหา เช่น AODV เนื่องจากโหนดต้องการทราบข้อมูลเกี่ยวกับโหนดเพื่อนบ้านเท่านั้นสำหรับการกำหนดเส้นทางในการส่งแพ็กเก็ตข้อมูล

เอกสารอ้างอิง

- [1] Y. Yao, J. Chong and W. Xingwei, "Enhancing RC4 algorithm for WLAN WEP protocol", in Control and Decision Conference (CCDC), pp. 3623–3627, Chinese 2010
- [2] J. Hoebeke et al, "An overview of mobile ad hoc networks: applications and challenges", JOURNAL-COMMUNICATIONS NETWORK, 3, vol. 3, pp. 60–66, 2004.
- [3] V. Sharma and A. Baghel, "A Review of Security Attacks in MANETs". Search & Research, Bhopal, India, pp.58-63, Aug. 30, 2010.
- [4] A. Kumar and M. Chawla, "Destination based group Gray Hole attack detection in MANET through AODV", International Journal of Computer Science, vol.9, issue4, no.1, pp 292-295, July. 2012.
- [5] A. M. Kanthe, D. Simunic and R. Prasad, "A Mechanism for Gray Hole Attack Detection in Mobile Ad-hoc Networks", International Journal of Computer Applications, 53, vol. 16, pp. 23–30, 2012.
- [6] O. V. Chandure et al, "SIMULATION OF SECURE AODV IN GRAY HOLE ATTACK FOR MOBILE AD-HOC NETWORK", Internation Journal of Advances in Engineering & Technology, vol.5, no.1, pp.67-76, 1963.
- [7] S. Banerjee, "Detection/removal of cooperative black and Gray Hole attack in mobile ad-hoc networks", in Proceedings of the World Congress on Engineering and Computer Science, pp. 22–24, 2008.
- [8] A. Megha and K. J. Yogendra, "Grayhole Attack and Prevention in Mobile Adhoc Network", International Journal of Computer Applications, vol. 27, no. 10, pp. 21–26, 2011.
- [9] J. Sen et al, "A mechanism for detection of Gray Hole attack in mobile Ad Hoc networks", in Information, Communications & Signal Processing, 2007 6th International Conference on IEEE, pp. 1–5, 2007.
- [10] O. V. Chandure and V. T. Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International Journal of Computer Applications (0975–8887) Vol.41, no.5, pp. 27-32, Mar. 2012.