International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 11, Number 2, pages 121–139, July 2021

Collaborative Defense Techniques Against MANETs Malicious Nodes

Takeru Terai
Ritsumeikan University
Graduate School of Inf. Sci. and Eng.
is0316kf@ed.ritsumei.ac.jp

Masami Yoshida
Ritsumeikan University
Graduate School of Inf. Sci. and Eng.
is0195hr@ed.ritsumei.ac.jp

Alberto Gallegos Ramonet
Ritsumeikan University
College of Inf. Sci. and Eng.
ramonet@fc.ritsumei.ac.jp

Taku Noguchi
Ritsumeikan University
College of Inf. Sci. and Eng.
noguchi@is.ritsumei.ac.jp

Received: February 12, 2021
Revised: April 8, 2021
Accepted: May 27, 2021
Communicated by Eitaro Kohno

Abstract

Blackhole (BH) attacks are among the most significant threats in mobile ad-hoc networks. A BH is a security attack in which a malicious node absorbs data packets and sends fake routing information to neighboring nodes. BH attacks have been widely studied. However, existing defense methods wrongfully assume that BH attacks cannot overcome the most common defense approaches. A new wave of BH attacks is known as smart BH attacks. In this study, we used a highly aggressive type of BH attack that can predict sequence numbers to overcome traditional detection methods that set a threshold to sequence numbers. To protect the network from this type of BH attack, we propose a collaborative defense method that uses local information collected from neighboring nodes. We evaluated the performance of our defense method against a smart BH attack and a collaborative attack that uses the collaboration of another malicious node. Our results show that the proposed method successfully detects and contains these threats to some degree. Consequently, the smart BH attack success rate decreases.

Keywords: AODV, Routing protocols, MANET, Blackhole attack, Security, Ad-hoc networks, Wireless sensor networks

1 Introduction

In recent years, researchers have actively studied networks that communicate without the use of base stations, such as ad-hoc networks. Due to their nature, the usage of these networks is closely related to the networks used during natural disasters. In an ad-hoc network, packets are forwarded to their final destination in a multi-hop fashion; therefore, if there is a malicious node in any relay node, there is a possibility that attacks such as eavesdropping or data packet falsification may occur [17]. Unlike in centralized fixed networks, any node can freely participate in an ad-hoc network provided that no administrator exists. For this reason, there is an inherent problem with network security. In particular, blackhole (BH) attacks are among the most significant threats faced by ad-hoc networks.

[0]The present paper is an invited paper and a follow-up to the accepted and presented paper in the Eight International Symposium on Computing and Networking (CANDAR 2020).

In BH attacks, an attacking node directs data packets to itself and eavesdrops or discards them. When building an ad-hoc network, it is necessary to ensure reliable security. Therefore, research on defense methods against this type of attack is indispensable in the field of ad-hoc networks. Although defense methods for BH attacks have been discussed in previous studies, there are few research examples from the perspective of the attacker. When BH attacks use unexpected patterns, it is necessary to verify whether the existing defense methods can detect and protect against such new attacks. This study proposes an aggressive BH attack that can predict the sequence number in the popular ad-hoc on-demand distance-vector (AODV) protocol. We also propose a defense method that is effective against this attack. We named this the *collaborative defense method*. We evaluated the performance of this defense method in terms of rates of packet delivery, attack success, and false detection. Additionally, we demonstrated that the collaborative defense method is effective against BH attacks that can predict the sequence number values (we henceforth refer to these as smart BH attacks). The remainder of this paper is organized as follows. Section 2 briefly describes the function of the AODV routing protocol. In Section 3, we describe BH attacks and variants such as smart BH and smart BH attacks assisted by other malicious nodes. Section 4 contains a detailed description of our proposal: the collaborative defense method for mobile ad-hoc networks (MANETs). Finally, Section 5 presents our evaluations, followed by conclusions.

2 AODV

AODV [12] is a routing protocol widely used in MANETs. Routing protocols are used to interconnect different points of a network using multiple nodes. A routing table is used in a routing protocol to describe the information of the routes in the network. Protocols that create a routing table can be classified as either proactive or reactive. The former is a method in which a routing table is created before communication is initiated. The latter does not create routing tables initially but rather when a communication request is issued. AODV belongs to the reactive category and is suitable for creating routes in networks with high node mobility. When determining a route, a sequence number is used. This number increases when communication is established. If there are multiple route candidates, the route with the larger sequence number is regarded as the newest route and is therefore adopted. AODV was first proposed over 15 years ago; however, the protocol is still relevant today for the creation of mesh networks [9]. In fact, an implementation based on AODV can be found in the Texas Instruments Z-Stack 3.10 (SimpleLink CC26 $\times$ 2 SDK). This stack is used by some Texas Instruments MCUs, such as CC26X2R1 [4].

2.1 AODV route construction

AODV builds and maintains routes using three types of packets: route request (RREQ), route reply (RREP), and route error (RERR). In the present study, only RREP and RREQ packets are discussed as they are the only relevant packet types involved in BH attacks. Detailed information on the functioning of the AODV protocol can be found in the original specification [12]. The information contained in the RREQ and RREP packets is listed in Tables 1 and 2, respectively.

Table 1: AODV RREQ packet specification.

Packet Type	Reserved	Hop Count
RREQ ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Source Sequence Number		

Table 2: AODV RREP packet specification

Packet Type	Reserved	Hop Count
Destination IP Address		
Destination Sequence Number		
Source IP Address (RREQ originator)		
Lifetime		

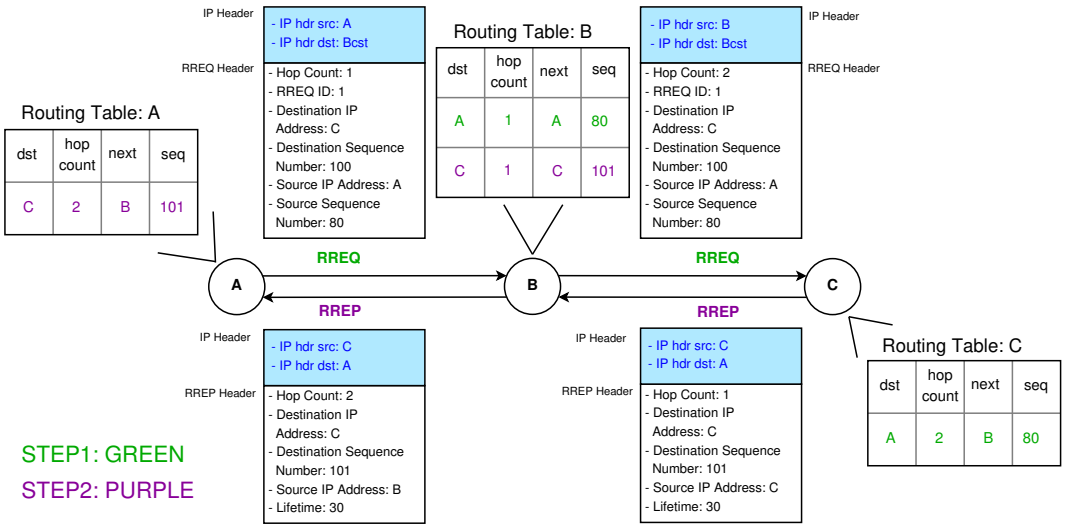

Figure 1: AODV: Route construction using RREQ and RREP.

An RREQ packet is formed by the following elements:

- *Hop Count.* The number of hops from the originator IP address to the node handling the request.
- *RREQ ID.* A sequence number uniquely identifies the particular RREQ when taken in conjunction with the originating node's IP address.
- *Destination IP address.* The IP address of the destination for which a route is desired
- *Destination Sequence Number.* The latest sequence number received in the past by the originator for any route towards the destination.
- *Source Ip Address (originator).* The IP address of the node that originated the route request.
- *Source Sequence Number.* The current sequence number to be used in the route entry point towards the originator of the route request.

An RREP packet is formed by the following elements:

- *Hop Count.* The number of hops from the originator IP address to the destination IP address.
- *Destination IP Address.* The IP address of the destination for which a route is supplied.
- *Destination Sequence Number.* The destination sequence number associated with the route.
- *Source IP Address (RREQ originator).* The IP address of the node that originated the RREQ for which the route is supplied.
- *Lifetime.* The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

A routing table in AODV is created and populated in two steps:

Step 1: RREQ flooding. The source node does not possess information about the destination and therefore broadcasts an RREQ to its neighboring nodes. The node that receives the RREQ checks whether there is a route to the destination node by consulting its routing table. If there is no route or if the routing table is outdated, the node updates its routing table with the information from the RREQ and then broadcasts the RREQ to its neighboring nodes. This process is performed until an RREQ reaches the destination node or a relay node with an updated route to the destination node.

Step 2: RREP transmission. When Step 1 is completed (i.e., an RREQ reaches a node with a route to the destination or the destination itself), an RREP is unicasted to the node that emitted the RREQ. When a node receives an RREP, it updates its routing table, and if it is not the node that originated the RREQ, it transmits a new RREP toward the node that sent the first RREQ. These two steps establish a bidirectional path between the source and destination nodes. If the source node receives multiple RREPs, the RREP with the largest sequence number or the smallest number of hops to the target node is adopted. Figure 1 provides an example of route creation in AODV using these two steps.

3 Blackhole attack

A black hole (BH) is a type of denial of service (DoS) attack that discards or eavesdrops on data packets that are sent from a source node to a destination node [11, 20]. The BH node catches an RREQ and returns an RREP with a spoofed sequence number to the source node, thereby constructing a communication path that includes the BH node. This node can disrupt communication by absorbing the passing packets. Consequently, the throughput and packet arrival rate decreased dramatically.

3.1 Blackhole attack procedure

As previously mentioned, the BH node directs data packets to itself by using spoofed RREPs. Figure 2 shows this process, where B represents the attacking node.

Step1: Transmission of a spoofed RREP. When the BH node receives the RREQ, it sends a spoofed RREP. At this time, the number of hops described in the RREP is set to a small value, and the sequence number is set to a value larger than the actual sequence number. In AODV, the route with the highest sequence number is regarded as the newest and most stable route. Traditional BH attacks take advantage of this weakness and set the sequence number to a large value, ensuring that the path that includes the BH node is considered by the neighboring nodes as the most up-to-date route.

Step 2: Data packet routing. The source node receives the spoofed RREP from the BH node. When the source node receives this information, it assumes that this path, containing the malicious node, has the smallest number of hops and is the most up-to-date path. Therefore, the source node sends data packets to a malicious node.

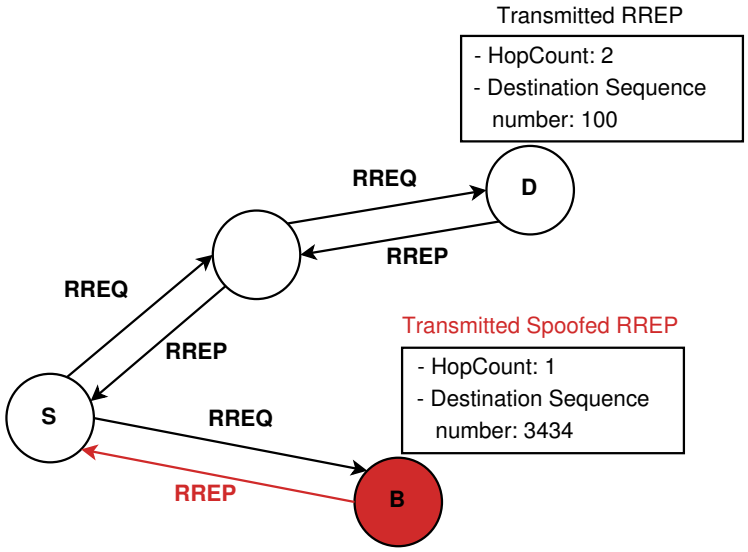

Figure 2: Blackhole attack.

3.2 Existent defense methods and smart BH attacks

BH attacks constitute a significant threat to MANETs. A BH attack can severely degrade the performance of most networks, even to the point of invalidating them. In modern networks, anonymous node participation in a MANET can be limited by using an authentication control header. This authentication mechanism can effectively eliminate the possibility of an anonymous node joining and disrupting the network. However, an authenticated node with a certificate could initiate an attack while complying with the protocol standards. In addition, frequent security key exchanges can impose a performance burden on the network in networks where energy consumption is still a concern (e.g., wireless sensor networks) [7]. For this reason, it is not unlikely to find networks that opt not to implement these security measures. In many cases, implementing a BH detection method can produce a lower overhead than these security authentication methods. Some BH defense methods use a dummy RREQ [5] to detect the existence of BH nodes. This defense method assumes that a BH node responds to an RREP immediately upon receiving the RREQ. According to this defense method, nodes responding to a dummy RREQ with a nonexistent address are considered BH nodes. However, smart BH nodes can infer whether the destination address exists and can easily overcome this defense. Other existing defenses against BH attacks primarily comprise setting a threshold for sequence numbers [10, 15]. Typical BH attacks create RREP messages with a large sequence number value. Therefore, simply limiting the sequence numbers can help protect against these attacks. This type of defense method is known as *threshold-based defense* and is shown in Figure 3. In this figure, node S sets the sequence number threshold to 1000. Since the destination sequence number of the RREP created by node D is 100 (which is below the threshold), node S identifies node D as a safe node. In contrast, the destination sequence number of the RREP created by node B is 3434 (which is larger than the threshold); therefore, node S determines that the destination sequence number of the RREP created by node B is spoofed, thereby identifying node B as a BH node, and discarding its subsequent RREPs. However, this method does not consider that the BH node can use a sophisticated attack capable of setting sequence numbers intelligently. Smart BH attacks defeat threshold-based defense methods by taking note of the destination-node sequence numbers of the received RREQ and predicting the sequence number values accurately to some extent using the least-squares method (dynamic threshold attack) [19, 20]. It is reasonable to assume that smart BH attacks can overcome most defense methods that use a similar approach to that of threshold-based defense methods. For example, the method proposed in [16] achieves a high packet delivery rate even under regular BH attacks. According to the authors, this is possible by creating a threshold that is set as a small amount above the average of all received RREPs. However, this method does not consider smart BH attacks. Therefore, it is ineffective against attacks that predict sequence numbers. Multiple studies [6, 13, 18] are effective against regular BH attacks, but are considered to be incompetent against smart BH attacks. Security is an indispensable part of MANETs and WSNs, and defense methods should be able to detect and prevent BH attacks that can predict sequence numbers. In this study, we created a smart BH attack and devised a defense method against it. Additionally, we confirmed the effectiveness of this smart BH attack when traditional BH defense methods were used. In our evaluations, we used the common *threshold-based defense* method to demonstrate the effectiveness of the smart BH attack. Our original defense method can manage smart BH attacks. This method leverages the cooperation of neighboring nodes to set even more suitable thresholds for sequence numbers.

3.3 Collaborative BH attacks

A complex form of BH attack where multiple malicious nodes collude to execute a BH attack is possible [2]. For example, malicious nodes can share information about known RREP threshold values from network nodes and perform a smart BH attack. Similar to defense methods, when a malicious node possesses more information, it can better estimate the RREP threshold value from neighboring nodes. When malicious nodes collude together to execute a BH attack like this one, they can easily overcome most existing BH defense methods and become a more dangerous threat [1, 8]. This threat becomes even more alarming when considering that most defense mechanisms rarely acknowledge the possibility of a collaborative attack by multiple malicious nodes. In this research,

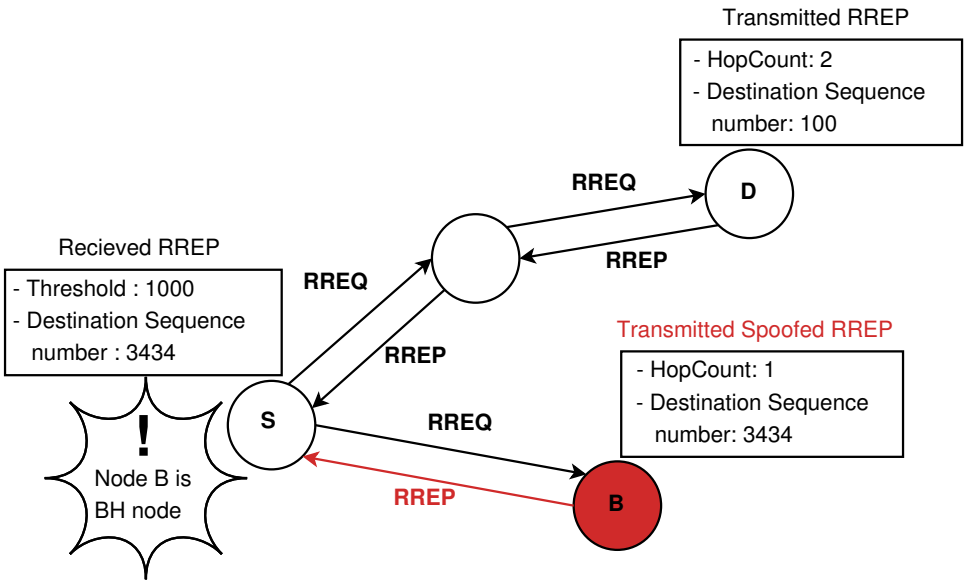

Figure 3: Threshold-based defense method.

we conducted experiments on a network subjected to a collaborative attack using a smart BH node and a *spy node*. While the smart BH node behaves as described in the previous section, the spy node objective is to collect as much RREQ information as possible from nodes across the network and transmit the collected information to the smart BH. The smart BH node can use the collected information from the spy node and itself to better estimate the threshold values. In addition to collecting and transmitting information to the smart BH node, a spy node behaves like a legitimate node and transmits regular RREQ and RREP messages as any other node. While defense mechanisms may target behaviors specific to BH nodes, they might not target the behavior of a spy node, making this node harder to detect. In our evaluations, the smart BH node and the spy node start at opposite corners of the network and slowly move towards the network center where they meet (Figure 4). Evaluations involving such attacks are further discussed in Section 5.

4 The Collaborative Defense Method

Our proposed defense method uses the sequence number and creation time (timestamp) described by the RREPs coming from the destination node. The approximate sequence number was predicted using the least-squares method to set the threshold value. To improve the threshold approximation accuracy, the source node uses extra sequence numbers and timestamp information from neighboring nodes added to the RREP packet specification. With this information, the node that initiated the RREQ (source node) can judge whether a BH node inserted itself into the route.

4.1 Sequence numbers and timestamp information

The collected information by the collaborative defense method can be divided in two categories:

- Regular information collected from the RREP packet specification.
- Extra information inserted into RREP that describes information from neighboring nodes.

The first information can be obtained from regular AODV RREP packets without changing its implementation because a node retrieves the destination node address and destination sequence number from the received RREP packet. Concerning the second type of information, it is necessary to change the implementation of AODV to share information from neighboring nodes. Part of our

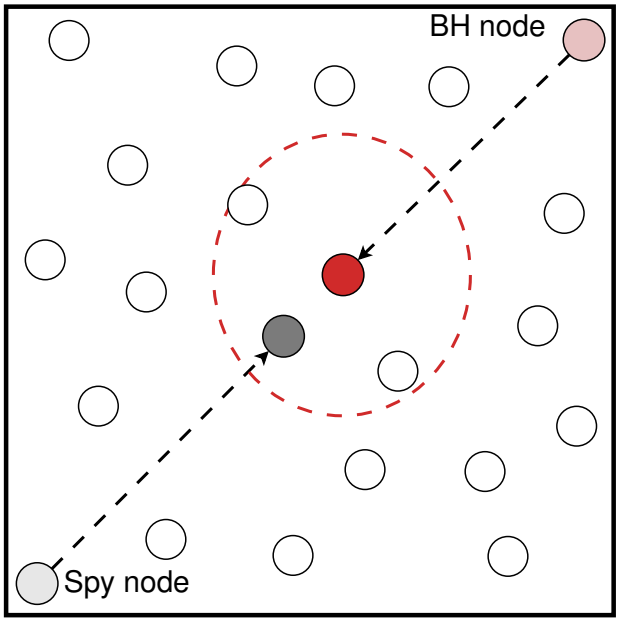

Figure 4: A collaborative BH node attack assisted by a spy node.

proposal in this study involves this second method. By adding information to the RREP packet (Table 3) from the original (Table 2), it is possible to share additional information held by the neighboring nodes with the source node.

Table 3: Modified RREP specification.

Packet Type	Reserved	Hop Count
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Lifetime		
Creation Time		
Previous Creation Time 1		
Previous Destination Sequence Number 1		
.....		
Previous Creation Time n		
Previous Destination Sequence Number n		
Hop 1	Hop 2	Hop3
Last Relay Time 1	Last Relay Time 2	Last Relay Time 3

Our modified RREP adds five new elements: *creation time of the RREP packet, previous creation time, previous destination sequence number, hop and last relay time.* A relay node inserts its last known sequence number into the *previous destination sequence number* field in the RREP. That is, the previous destination sequence number is an item to be written when the sequence number of the destination node was last acquired from an RREP that was received and forwarded in the past. A relay node inserts the time it acquire the sequence number information into the *creation time* field of the RREP. Our modified RREP also include the creation time and sequence number from previous sequence number acquisitions. Therefore, to make our defense method work, all nodes must hold the destination sequence number value of the RREP received in the past and the creation time information of the RREP. A single RREP can hold a variable number of previous creation time and previous destination sequence number pairs (max 3). The last two elements in the modified

RREP, *Hop* and *Last Relay Time*, collect RREP relay information from the first three nodes that relayed the RREP. This information is later used by the source node to compare the relay frequency of RREP packets from nodes involved in the route. The inclusion of this information into RREP packets increases the RREP overhead, but the extra information is valuable for detecting BH nodes. This RREP overhead is further discussed at the end of Section 5.

4.2 RREP construction and collection

BH nodes present some behaviors that can be exploited in their detection. For instance, the BH nodes immediately respond with an RREP upon receiving any RREQ. Furthermore, BH nodes do not re-transmit RREQ or REPPs from other nodes. Some malicious attacks can re-transmit RREQ and RREP (e.g. gray hole attacks [14]), however, these types of attacks have a different impact on the network to BH attacks and require different detection methods. The current work focus on BH attacks exclusively. In this paper, we analyze and exploit some AODV behaviors to detect BH nodes. For example, in the AODV operation example shown in Figure 5, the last RREP packet received by node A contains an *IP hdr source* $= E$ and in the RREP header *Src IP Address* $= B$. This indicates that the received RREP originated in a node that is not one hop away, and therefore, it was re-transmitted by node B. With this information, the source node can infer that node B is a legitimate node because it re-transmits an RREP. This process is used by the collaborative defense method to identify legitimate nodes that are one hop away from the source node.

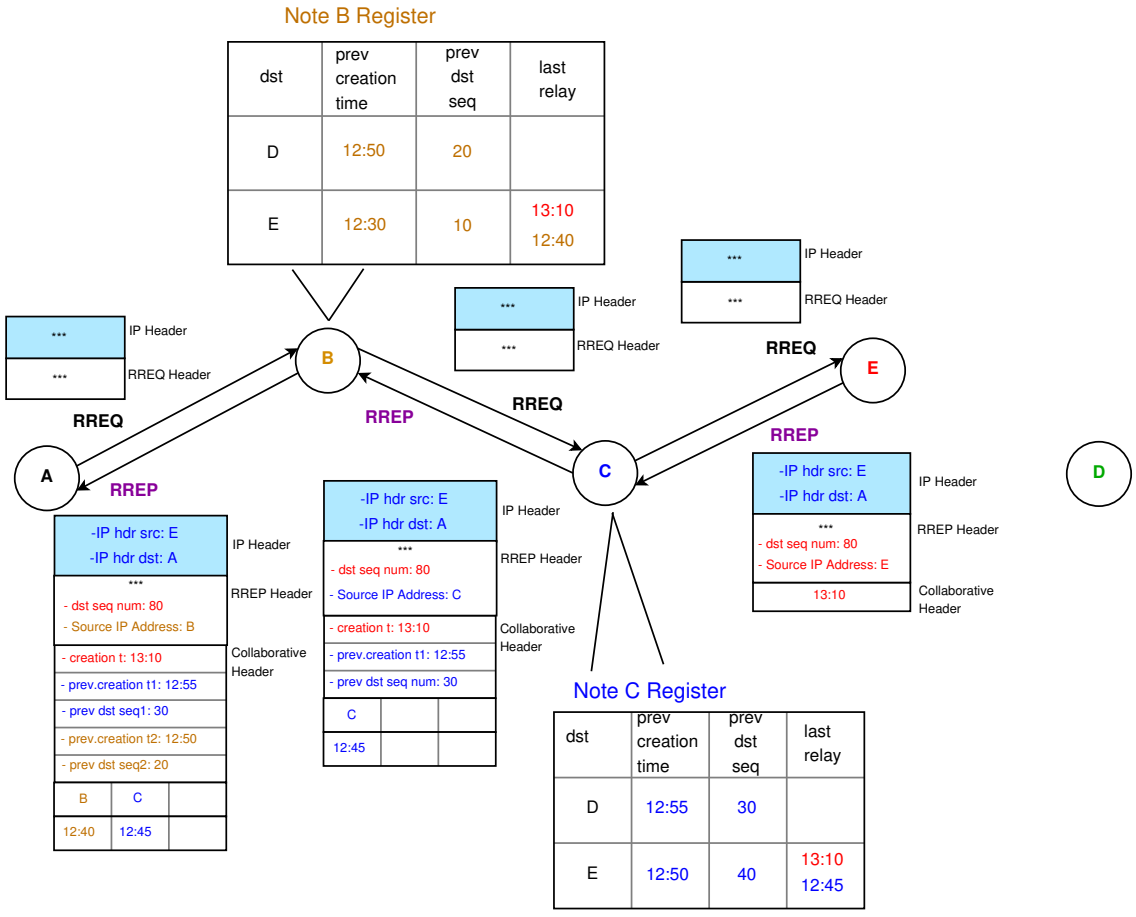

Figure 5: Collaborative defense method information collection and RREP relay.

In the collaborative defense method, each node keeps a *node register* where it keeps the information from neighboring nodes concerning the previous relayed RREP (creation time and destination

sequence number). Figure 5 shows the collection of information used by AODV with a collaborative defense method activated. In this Figure, node A wishes to transmit a data packet to node D, but it does not have a route to it. For this reason, node A broadcasts an RREQ. Node B is a neighbor of node A and receives the RREQ broadcast. This node also does not have a route for node D; therefore, it rebroadcasts the RREQ. Finally, node E received RREQ. Node E has the route to node D and reply with RREP containing the creation time of this RREP. When node C receives this RREP, it registers the creation time in the *last relay* field of its node register. Then, node C adds the last registered prev creation time, sequence number, and last relay time to the RREP and forwards it to node B. The registered prev creation time and sequence number come from an old RREP from node D. The last relay time information comes from an old RREP from node E. The process repeats when sending the information from node B to node A. When the last RREP is received by node A, this node now possesses information from the route between E and A. Node A (source of the first RREQ), uses the collected last relay times to calculate the frequency of RREPs coming from node E. Since BH nodes are frequent senders of RREPs, the collected information is used to determine whether E is a legitimate node. The *Hop* field serves as evidence that a relay was performed (BH does not relay RREP); therefore, ensuring the legitimacy of nodes B and C. Finally, the collected creation times and sequence numbers are used in the creation of the threshold.

4.3 Threshold creation

The source node predicts the sequence number using the least-squares method with its own information and information collected from its neighboring nodes. Through preliminary experiments, we confirmed that the sequence number increased proportionally over time. Therefore, the least-squares method involves using two pairs of data: the destination sequence number and the acquisition time of the sequence number. For example, let $T_1, T_2, T_3, ..., X_n$ be a sequence of acquisition times of a destination sequence number for a given destination IP address, and $S_1, S_2, S_3, ..., S_n$ be the destination sequence numbers corresponding to each acquisition time. Using these values, we calculate the elapsed times X_n between the reception of the first sequence number and the subsequent sequence numbers, $(X_n = T_n - T_1)$. By using these datasets, $(X = X_1, X_2, X_3, ..., X_n$ and $Y = S_1, S_2, S_3, ..., S_n)$, it is possible to calculate the equation of a straight line, whose slope and intercept are, respectively, given by the following equations:

$$slope : A = \frac{Cov(X,Y)}{\sigma_X^2} \tag{1}$$

$$intercept : B = \overline{Y} - A\overline{X} \tag{2}$$

where $\overline{X}$ represents the average of X, σ_X represents the standard deviation of X, $\overline{Y}$ is the average of Y, and $COV(X,Y)$ represents the covariance between X and Y. For example, suppose that the datasets (X,Y) are (2, 4), (3, 5), (10, 18), and (13, 29). In this case, $x = 7$, $y = 14$, $\sigma_X = \sqrt{\frac{43}{2}}$, $Cov(X,Y) = 47$, $slope : A = \frac{94}{43}$, and $intercept : B = -\frac{56}{43}$. Therefore, the standard equation of a line can be derived as $y = \frac{94}{43}x - \frac{56}{43}$. For example, when $x = 3$ is substituted into this equation, $y = \frac{226}{43} \approx 5.2558$, which approximately matches the data of (3, 5). With this standard equation, the actual sequence number value is calculated (predicted) at any given time, and the threshold can be defined. To decrease the false detection rate (FDR), that is, the ratio of the number of normal nodes considered falsely as BH nodes to the total number of normal nodes, the threshold must be slightly higher than the actual sequence number value. Thus, the threshold value is defined by the following expression:

$$Th = Seq_a + \alpha \tag{3}$$

where Th represents the threshold, Seq_a represents the approximated actual sequence number, and α is a safety margin parameter for preventing the false detection of a BH node. Depending on the

value of α, performance can change significantly. A smaller value of α increases the detection rate of BH nodes and, increases the FDR. A larger value of α decreases the FDR and decreases the detection rate of BH nodes.

5 Performance evaluation

5.1 Simulation environment

We evaluated the performance of the proposed BH-attack defense method using the ns2 network simulator [3]. The simulation environment is presented in Table 4. We implemented a smart BH attack and a defense method against this attack. In addition to the defense method proposed in this study, we also evaluated and compared a BH-attack prevention method using a dynamic threshold in MANETs [11]. This method classifies nodes as either normal or BH using a dynamically updated sequence number threshold. The threshold is calculated from the total number of active nodes and the time elapsed from the reception of the last routing control packet. Evaluating these methods, the number of nodes was changed from 20 to 50, and the number of trials was set to 30 for each number of nodes. The results are given as an average of 30 observations. The AODV protocol was used as the routing protocol in all our experiments. We evaluated the defense methods from three perspectives: packet delivery rate (PDR), attack success rate (ASR), and FDR (Equations 4, 5, and 6).

$$PDR = \frac{N_{recv}}{N_{sent}} \times 100 \tag{4}$$

where PDR represents the amount of data sent from the source node to the destination node, N_{recv} is the number of data packets received by the destination node, and N_{sent} is the number of data packets transmitted by the source node.

$$ASR = \frac{NF_{selected}}{NF_{recv}} \times 100 \tag{5}$$

where the ASR represents how much the BH node is able to guide data packets to itself against the number of attacks, $NF_{selected}$ is the number of times a route through a BH node is selected according to the spoofed RREPs whose sequence numbers are smaller than the threshold, and NF_{recv} is the number of spoofed RREPs created by a BH node and received by the source node.

$$FDR = \frac{N\_TH_{over}}{NT_{recv}} \times 100 \tag{6}$$

where FDR denotes the number of normal nodes treated as BH nodes, N_TH_{over} is the number of unspoofed RREPs whose sequence numbers are larger than the threshold, and NT_{recv} is the number of unspoofed RREPs created by a normal node and received by the source node.

Table 4: Simulation Environment

Simulation Time	500[s]
Network Area	800[m]×800[m]
Number of Nodes	20, 30, 40, 50
Malicious Nodes	1 or 2
Mobility Model	Random Waypoint
Routing Protocol	AODV

In [3], RREQ exploitation methods were investigated. In our previous study, we demonstrated that it is possible to implement a simple attack that cleverly predicts the sequence number and successfully degrades the PDR performance of existing defense methods. Contrarily, we implemented a defense method against these types of attacks in our present study [3].

5.2 Smart BH attack evaluation

In the first round of evaluation, we tested the performance of the proposed defense method when a smart BH node exists in the network. In these experiments, we fixed the value of α to 4. As previously explained in Section 4.3 (Equation 3), α is used in the calculation of the predicted sequence number threshold value and represents a safety margin for preventing the false detection of BH nodes. Preliminary experiments indicated that 4 was the optimal α value; therefore, we used this value through our experiments with a single BH node. Experiments with different α values are further discussed in Subsection 5.4.

5.2.1 Packet delivery rate (PDR)

Figure 6 shows the PDR results. As the number of nodes increases, the PDR tends to increase. This is because it became possible to establish stable links as the node number increased. In other words, more routes become available to a destination at any given time. The collaborative method (proposed method) has a higher packet delivery rate than the existing threshold-based method. The collaborative method achieves a 71% PDR. This represents a 31% PDR increase when compared to the threshold-based method. Note that the PDR of the collaborative method increased by approximately 44% when compared to a scenario with no defense method. The collaborative defense method benefits more from the increase of nodes. In our experiments, the PDR increases as the node number increases. This is because when the node number increases, the collaborative method can collect more RREP information from neighboring nodes and calculate better estimate thresholds.

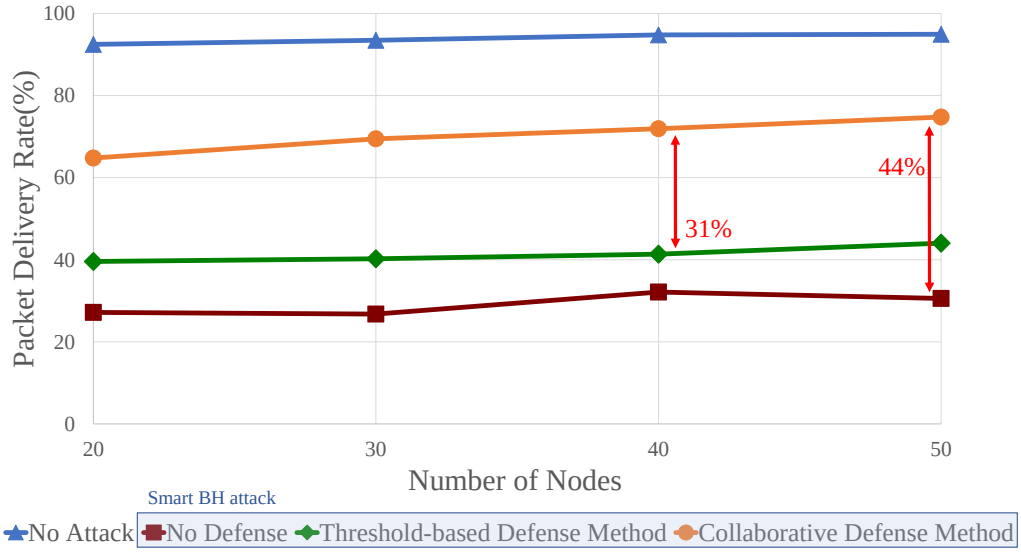

Figure 6: Packet delivery rate: Single smart BH node.

5.2.2 Attack success rate

Figure 7 shows the results of the ASR. When the collaborative method was used, the ASR remain under 13%. In the collaborative method, the source node can accurately predict the sequence number and set a suitable threshold. In comparison, the ASR reached 47% when using the existing threshold-based method. This is almost as high as using no defense method (60% ASR). The threshold-based method can hardly reduce the ASR since the smart BH attack can overcome the method.

5.2.3 False detection rate

Figure 8 shows the FDR results. When compared to the threshold-based method, the collaborative defense method successfully reduced the FDR by 9%. In our experiments, FDR was slightly affected by the number of nodes. Both the threshold-based defense method and the collaborative method are based on the approximation of the threshold value, and this approximation depends on the available information from neighboring nodes. Therefore, when the number of nodes increased, FDR was reduced.

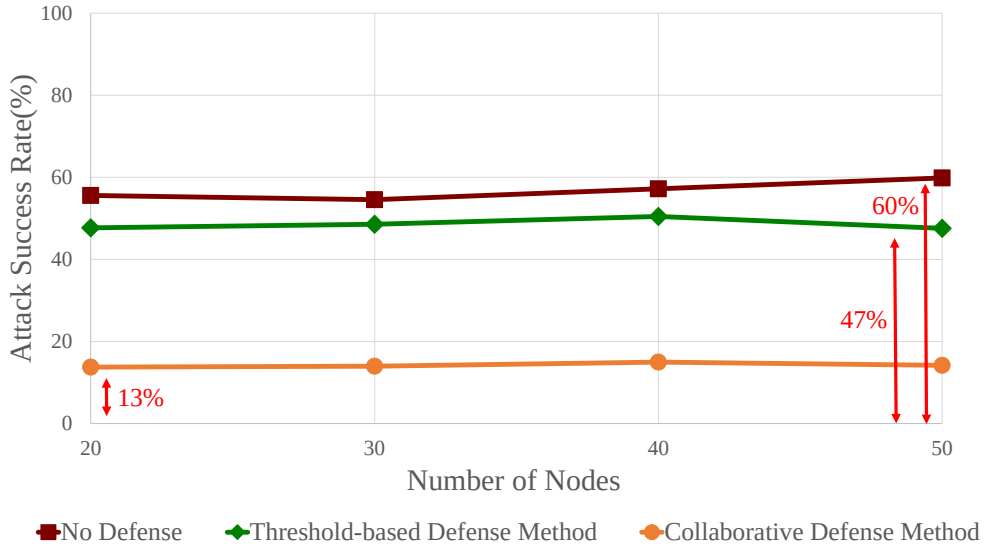

Figure 7: Attack success rate: Single smart BH node.

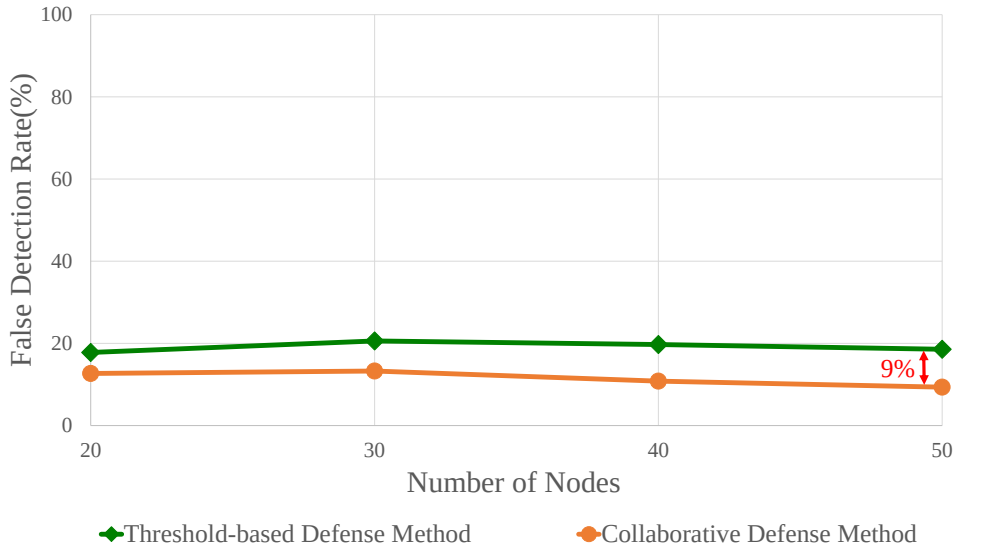

Figure 8: False detection rate: Single smart BH node.

5.3 Collaborative BH attack evaluation

In this section, we discuss our evaluations of a collaborative BH attack where a smart BH attack is assisted by a spy node. The motivations and movement patterns of this attack are briefly discussed in Section 3.3. As in previous evaluations, the safety margin value (α) is fixed at 4. This section evaluates the effectiveness of the collaborative defense method against a collaborative BH attack (the spy-node-assisted BH attack). A spy node only shares information with the smart BH node but does not directly engage in an attack, unlike a BH node. This makes this type of node harder to detect by defense mechanisms, which typically target only the detection of BH nodes.

5.3.1 Packet delivery rate

Figure 9 shows the PDR results of a collaborative BH attack. Similar to the results of a single smart BH attack, when the number of nodes increase the collaborative defense method can collect more information and reduce the impact of the attack. However, the smart BH can also collect more information with the help of the spy node this time and therefore, PDR decreased in all our tests. This proves the effectiveness of the attack assisted by a spy node. Regardless, the collaborative defense method was still able to maintain a 31% increase in performance compared to the threshold-based method and a 37% increase compared to not having a defense method.

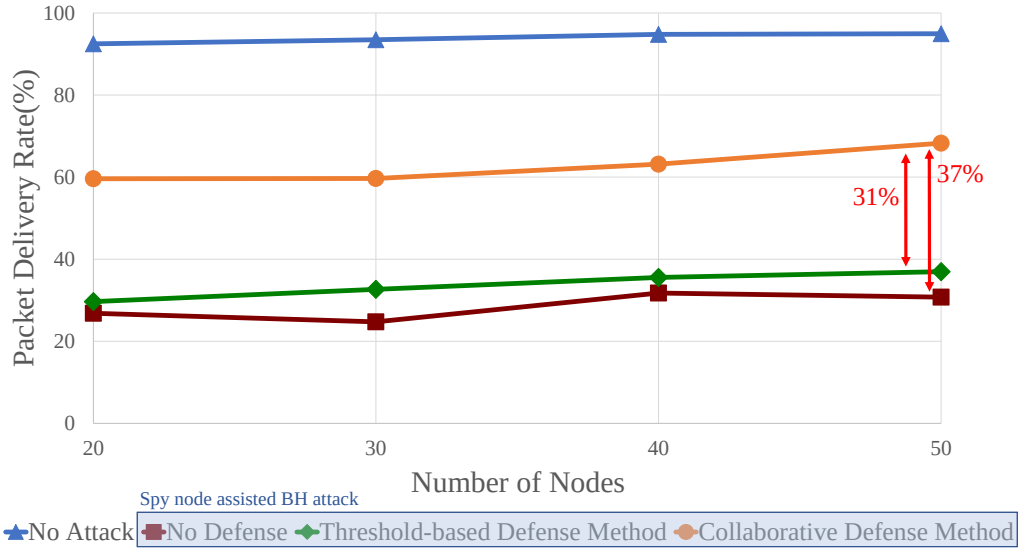

Figure 9: Packet delivery rate: Spy-node-assisted smart BH attack.

5.3.2 Attack success rate

Figure 10 shows the ASR results when a smart BH is assisted by a spy node. In all the cases, the ASR of the collaborative BH attack increased. When a spy node was used, the ASR increased from 13% to 18% in the presence of the collaborative defense method. Similarly, when the threshold-based method was used, the ASR increased from 47% to 53%. Finally, when no defense was present, the ASR increased from 60% to 70%.

5.3.3 False detection rate

Figure 11 shows the FDR results when a smart BH attack is assisted by a spy node. From this figure, we can observe that the collaborative defense method had an FDR increase compared to the threshold-based method. This is because the BH node detection mechanisms that check the legitimacy of nodes (1 hop away check and hop relay confirmation) are designed to assume that only

a single BH node may exist. When more than a single BH node exists, these detection mechanisms cannot be trusted. In these cases, the collaborative defense method must only lean on the dynamic threshold mechanism for the detection of BH nodes. Figure 12 shows a situation where a BH node takes advantage of the existence of a spy node. The collaborative defense method detects BH nodes, however, a spy node may exist between the source and the BH node. The spy node can relay RREP, therefore, it cannot be detected using the aforementioned mechanisms.

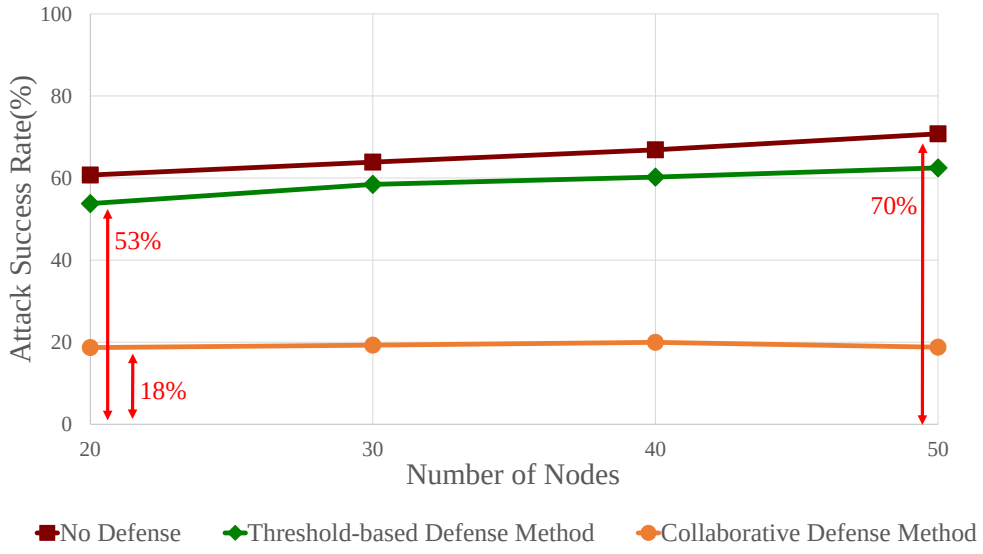

Figure 10: Attack success rate: Spy node assisted smart BH attack.

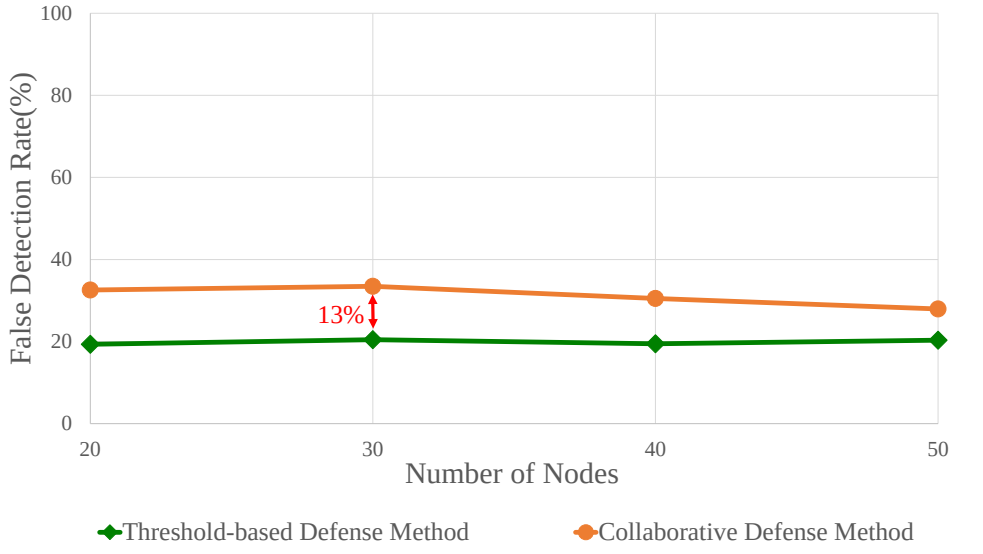

Figure 11: False detection rate: Spy node assisted smart BH attack.

5.4 Dynamically Adaptive Safety Margin

In our previous experiments, we used a fixed value of α to calculate the safety margin used in the threshold calculation. However, this safety margin is fixed and unable to adapt to the RREP

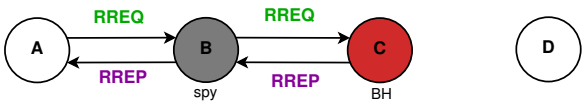

Figure 12: Spy node and BH node collaboration

sequence number increase rate. The safety margin α should be set appropriately according to the increase rate of the node sequence numbers. For this reason, we introduce a *dynamically adaptive safety margin* to be used to calculate the threshold. When the number of nodes in topology is high, the rate at which RREP is produced also increases. Our dynamic margin considers this rate change by taking the number of RREP received and comparing each one of them to the current threshold (Figure 13). Based on the percentage of RREP sequence numbers under or over the current threshold, the value of α is dynamically updated in subsequent threshold calculations.

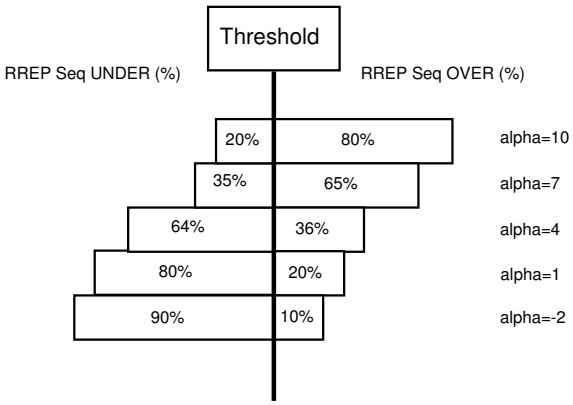

Figure 13: Dynamical Safety Margin.

5.4.1 Packet delivery rate

Figure 14 shows a packet delivery rate comparison between a smart BH attack and smart BH attack assisted by a spy node. In both cases, the difference between using an α dynamic safety margin and a fixed α safety margin is tested. From this figure, we observe that a smart BH node assisted by a spy node is able to reduce the packet delivery rate by 5% when compared to a smart BH node that worked alone. Nevertheless, the collaborative defense method can slightly improve the PDR when the dynamic safety margin is used.

5.4.2 BH attack success rate

Figure 15 shows an attack success rate comparison between a smart BH attack and a smart BH attack assisted by a spy node. From this figure, we observe that the attack success rate effectively increased when a spy node assisted BH attack was used. In some cases, the spy node assisted BH attack increased the ASR up to 5%. This is because the information collected by a spy node made the BH attack a more dangerous threat. Regardless of the collaborative BH attack used, the dynamic safety margin successfully minimized the impact of the attack.

5.4.3 False detection rate

Figure 16 shows the FDR results between a single smart BH attack and a spy node assisted smart BH attack. When the spy node assisted the attack, the dynamic safety margin reduced the FDR by 6% when compared to a fixed safety margin. Likewise, when a single BH attack was used, the dynamic margin reduces the FDR by 2%. This shows that the spy node assisted attack has a small

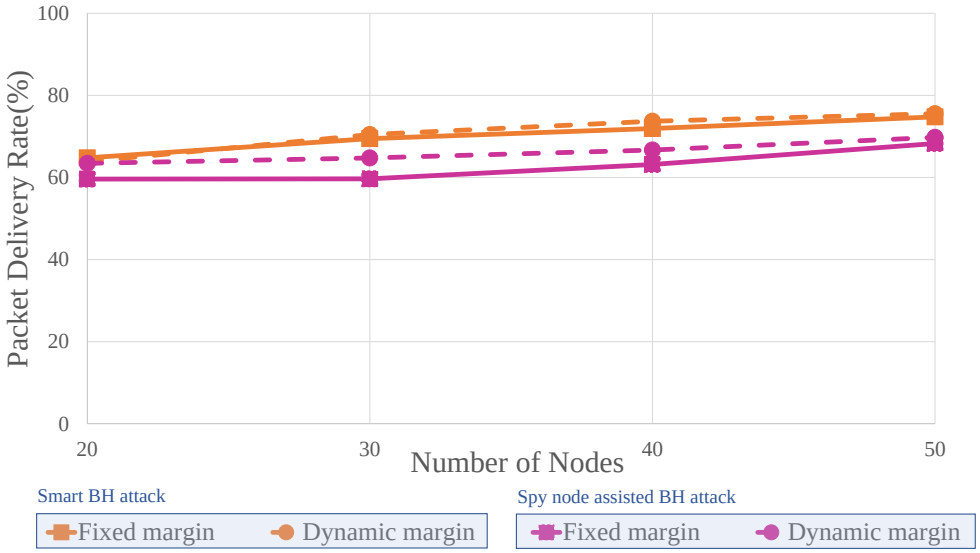

Figure 14: Packet delivery rate: Single smart BH attack V.S. Spy node assisted smart BH attack.

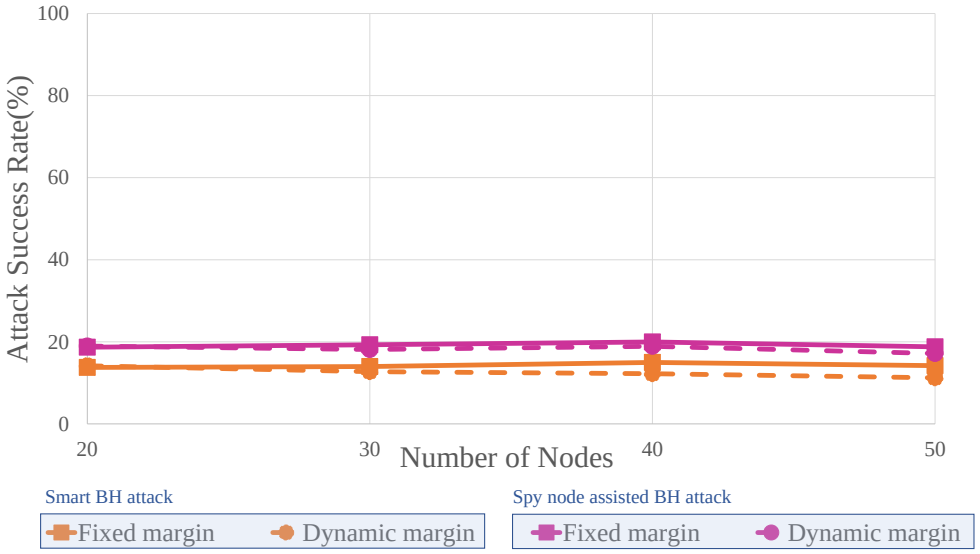

Figure 15: Attack success rate: Single smart BH attack V.S. Spy node assisted smart BH attack.

but noticeable impact on the network performance even when a collaborative defense method is running.

5.4.4 RREP overhead

Figure 17 shows the overhead caused by the modified RREP. We tested two identical networks, one running with the collaborative defense method and one without it. In both cases, no BH nodes exist. The amount of RREP overhead generated by the collaborative defense method was close to 9.3 KB in total. Therefore, we can conclude that, overall, the collaborative defense method has just a small impact when put in the context of information flowing in the network. This is because the number of RREP packets flowing in the network is always smaller than data packets and the RREQ packet, even if the RREP is larger in size.

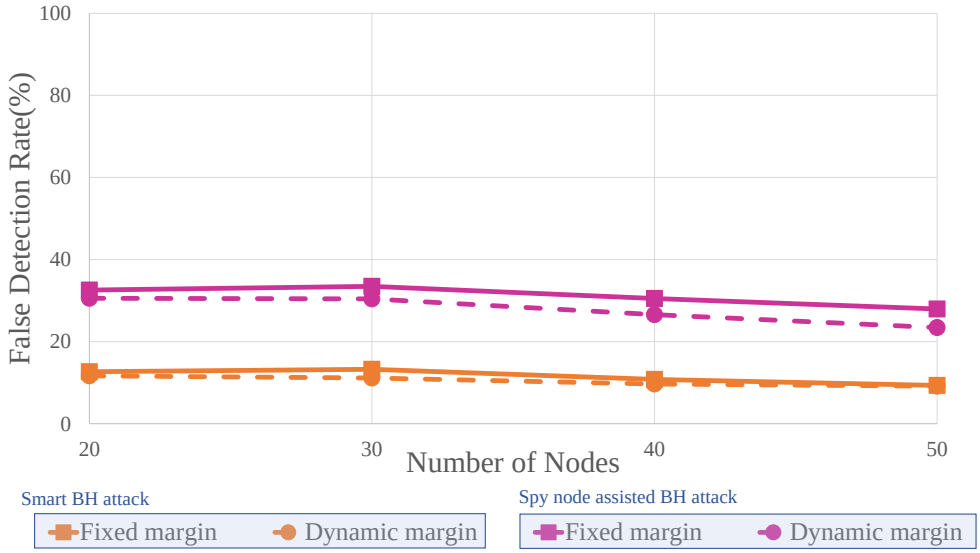

Figure 16: False detection rate: Single smart BH attack V.S. Spy node assisted smart BH attack.

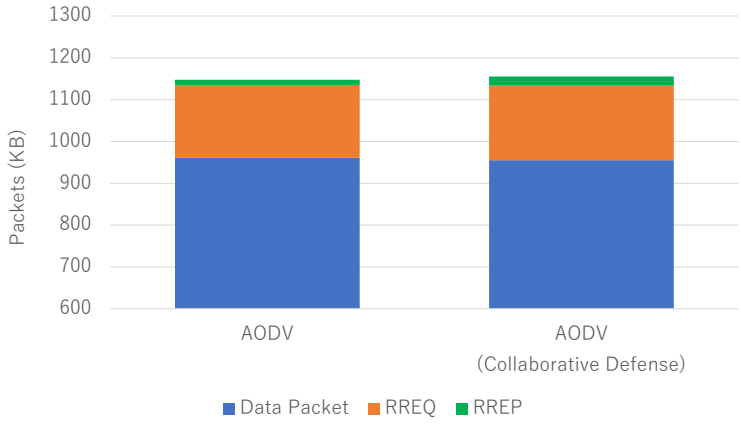

Figure 17: Collaborative defense method RREP overhead

6 Conclusions

In this study, we implemented a defense method that uses the neighboring nodes collaboration to protect a MANET against BH attacks. We tested our defense method against a smart BH attack and a smart BH attack assisted by a spy node. We tested our proposed method performance in three categories: packet delivery rate, attack success rate, and false detection rate. Our experiments showed positive results in all categories when compared to the existing threshold-based defense method. In the spy-node-assisted smart BH attack evaluations, the BH, ASR, and FDR increased while the PDR decreased. To mitigate some of the effects of this collaborative attack, we implemented a dynamic adaptive safety margin to approximate the threshold in our proposed defense method. This dynamically adaptive safety margin confirmed that a more flexible threshold estimation could improve the performance even in the presence of multiple malicious nodes. An optimal approximation of the threshold is an integral part of developing countermeasures against BH attacks. This can only be achieved by collecting enough information from the network while maintaining a low overhead. Future studies will address these issues in more detail.

7 Future work

Our proposed defense was able to improve upon the traditional threshold-based BH detection method. However, collaborative attacks of malicious nodes are difficult to detect and prevent. The present work will be extended to include the detection of multiple malicious nodes in large networks. At the same time, our proposed method introduced an overhead to the RREP specification. We believe that this overhead can be further reduced in future studies.

References

[1] Mishra Ankur, Jaiswal Ranjeet, and Sharma Sanjay. A novel approach for detecting and eliminating cooperative black hole attack using advanced dri table in ad hoc network. *2013 3rd IEEE International Advance Computing Conference (IACC)*, pages 499–504, 2013.

[2] K S Arathy and C N Sminesh. A novel approach for detection of single and collaborative black hole attacks in manet. *Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016)*, pages 264–271, 2016.

[3] DARPA. The network simulator - ns2. https://www.isi.edu/nsnam/ns/.

[4] Texas Instruments. *CC26X2R1 Z-Stack 3.10 User Guide*. Texas Instruments.

[5] Sakshi Jain and Dr. Ajay Khuteta. Detecting and overcoming blackhole attack in mobile adhoc network. *InternationalConference on Green Computing and Internet of Things (ICGCIoT)*, pages 225–229, 2015.

[6] S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour. Detecting blackhole attack on aodv-based mobile adhoc networks bydynamic learning method. *International Journal of Network Security, vol.5, no.3,*, pages 338–346, November 2007.

[7] Khan Moazzam, Amini Fereshteh, Misic Jelena, and B. Mi-sic Vojislav. The cost of security: Performance of zigbee key exchange mechanism in an 802.15.4 beacon enabled cluster. *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pages 876–881, 2006.

[8] Umar Farooq Muhammad, Wang Xingfu, Sajjad Moizza, and Qaisar Sara. Development of protective scheme against collaborative black hole attacks in mobile ad hoc networks. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, 12(3):1330–1347, March 2018.

[9] Sidhu Navjot and Sachdeva Monika. A comprehensive study of routing layer intrusions in zigbee based wireless sensor networks. *International Journal of Advanced Science and Technology*, 29(3):514–524, 2020.

[10] Taku Noguchi and Mayuko Hayakawa. Black hole attack prevention method using multiple rreps in mobile ad-hoc networks. *Proceedings of IEEE Conference on Trust, Security And Privacy In Computing And Communications*, pages 539–544, 2018.

[11] Taku Noguchi and Takaya Yamamoto. Black hole attack prevention method using dynamic threshold in mobile ad-hoc networks. *Preproceedings of the Federated Conference on Computer Science and Information Systems*, pages 813–818, 2017.

[12] C Perkins, E Belding-Royer, and S Das. Ad-hoc on-demand distance vector (aodv)routing, 2003. https://www.rfc-editor.org/rfc/pdfrfc/rfc3561.txt.pdf.

[13] P.N. Raj and P.B. Swadas. “dpraodv: A dynamic learning system against blackhole attack in aodv based manet. *International Journal of Computer Science Issues, vol.2*, pages 54–59, August 2009.

[14] P. Rani, Kavita, S. Verma, and G. N. Nguyen. Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. *IEEE Access*, 8:121755–121764, 2020.

[15] Ken Sajo and Takumi Miyoshi. Defense method to black hole attack on ad hoc network. *The Institute of Electronics, Information and Communication Engineers IEICE Technical Report*, 107(312):21–24, 2007.

[16] Lachdhaf Salim, Mazouzi Mohammed, and Abid Mohamed. Detection and prevention of black hole attack in vanet using secured aodv routing protocol. *Natarajan Meghanathan et al. (Eds) : NeTCoM, CSEIT, GRAPH-HOC, NCS, SIPR - 2017*, pages 25–36, 2017.

[17] S Sarika, A Pravin, A Vijayakumar, and K Selvamani. Security issues in mobile ad hoc networks. *Procedia Computer Science 92*, pages 329–335, 2016.

[18] S Tan and K Kim. Secure route discovery for preventing black hole attacks on aodv-based manets. *in Proc. IEEE International Conference on High Performance Computing and Communications and IEEE International Conference on Embedded and Ubiquitous Computing*, pages 1159–1164, November 2013.

[19] Takeru Terai, Alberto Gallegos, Ramonet, and Taku Noguchi. An implementation of the sequence number prediction based black-hole attack in mobile ad hoc networks. *The Institute of Electronics, Information and Communication Engineers, The 2019 IEICE General Conference, Proceedings of Communication Lectures 2*, pages 368–368, 2019.

[20] F.-H. Tseng, L.-D. Chou, and H.-C. Chao. A survey of black hole attacks in wireless mobile adhoc networks. *Human-centric Computing and Information Science*, 1(1):1–16, 2011.