network

MDPI

Article

Preventing Black Hole Attacks in AODV Using RREQ Packets

Yujin Nakano * and Tomofumi Matsuzawa

Department of Information Sciences, Tokyo University of Science, Chiba 278-8510, Japan; t-matsu@is.noda.tus.ac.jp

* Correspondence: yu2000u119@gmail.com

Abstract: Ad hoc networks, formed by multiple wireless communication devices without any connection to wired or intermediary devices such as by access points, are widely used in various situations to construct flexible networks that are not restricted by communication facilities. Ad hoc networks can rarely use existing infrastructure, and no authentication infrastructure is included in these networks as a trusted third party. Hence, distinguishing between ordinary and malicious terminals can be challenging. As a result, black hole attacks are among the most serious security threats to Ad hoc On-demand Distance Vector (AODV) routing, which is one of the most popular routing protocols in mobile ad hoc networks. In this study, we propose a defense method against black hole attacks in which malicious nodes are actively detected to prevent attacks. We applied the proposed method to a network containing nodes engaging in black hole attacks, confirming that the network's performance is dramatically improved compared to a network without the proposed method.

Keywords: network security; routing protocol; ad hoc network

Citation: Nakano, Y.; Matsuzawa, T. Preventing Black Hole Attacks in AODV Using RREQ Packets. *Network* **2023**, *3*, 469–481. https://doi.org/10.3390/network3040020

Academic Editors: Thomas M. Chen and Alexey Vinel

Received: 6 June 2023
Revised: 14 August 2023
Accepted: 1 October 2023
Published: 7 October 2023

1. Introduction

Internet of Things (IoT) technologies and devices, in which various devices that were not previously connected to the internet connect to a network and exchange information with each other, have attracted increasing attention recently. According to IHS Technology, the number of IoT devices shipped in 2018 reached neary 10 billion units per year, with a cumulative installed base of 30 billion units. The forecast for 2025 is just over 20 billion units shipped annually, with a cumulative installed base of 80 billion units. IoT devices communicate wirelessly, and in many cases connect to base stations called access points to achieve internet connectivity. However, the increase in the number of wireless communication devices has increased the load on access points; accordingly, the degradation of communication quality due to congestion has become a major concern. Mobile ad hoc networks are a representative technology for infrastructure-less communication that does not involve base stations such as access points. Consequently, ad hoc networks are expected to be implemented under various situations, and have become a topic of active research recently [1]. For example, by applying this network technology to automobiles, information on traffic congestion, accidents, and nearby vehicles can be shared between vehicles. Examples include vehicular ad hoc networks (VANETs) [2], which can improve transportation, off-grid rescue, and disaster support operations [3]. Thus far, various protocols derived from this routing protocol have been proposed.

Numerous Mobile Ad Hoc Network (MANET) routing protocols have been proposed recently. The routing used in such applications primarily includes flat routing protocols; however proactive, reactive, and hybrid protocols have been considered as well, depending on the implemented routing table management methods [4]. A proactive protocol is a method in which a route table is created even before a communication request is initiated. Although communication can start as soon as a communication request is made, packets are exchanged with neighboring nodes to keep the route list up-to-date, which may result in excessive use of bandwidth and radio waves. In a reactive protocol, on the other

hand, the route is created when a communication request occurs. Although starting a communication is time-consuming when using this approach, it is effective in networks that include battery-powered mobile devices, as there is no need to use extra bandwidth or radio waves.

One of the most potent reactive routing protocols is the so-called Ad hoc On-demand Distance Vector (AODV) routing [5,6]. Experiments comparing the performance of AODV, DSR, and DSDV have concluded that AODV is the best protocol in terms of throughput and performance when there are large numbers of implemented nodes in an environment where data is exchanged regularly [7].

Ad hoc networks can rarely use existing infrastructure. Because there is no authentication infrastructure that functions as a trusted third party, distinguishing between malicious terminals and other terminals is not possible. As a result, there is a risk of unauthorized participation in the network by malicious terminals, leading to unauthorized reception or falsification of data. Such security problems are an important barrier to the development of ad hoc networks [8,9]. In the AODV protocol, black hole attacks have been reported to take advantage of this vulnerability [10,11] In such attacks, an unauthorized terminal impersonates a real destination for packets that are used by the source to route destinations. As a result, data are absorbed and discarded as if they had fallen into a "black hole" in the network. Consequently, the performance of such networks can degrade considerably. Black hole attacks make it impossible for vehicles to communicate with each other though VANETs, underlining the danger of inducing potential accidents if the network consists of fully-automated vehicles, and in a disaster relief network can induce significant delays in communicating information to disaster victims. In this study, we focus on the characteristics of black hole attacks that can spoof any destination address as if it were its own destination. We implement and evaluate an opinion-based decision function that actively detects malicious nodes and excludes them from the network. Moreover, we discuss how the proposed method can improve security in a simple way for AODV and corresponding derived routing protocols.

2. Black Hole Attack

2.1. Summary

In a black hole attack, an attacking node impersonates a destination node or an intermediate node in order to illegally receive and discard data flowing in the network.

2.2. Construction

Before describing the behavior of a black hole attack, we discuss how AODV is routed. In AODV, the sender issues what is called a route request (RREQ) packet at the timing of sending data to the destination, flooding all nodes within the transmission range of the source node. This RREQ packet contains the IP address of the destination node; the node that receives this packet can verify whether it is the destination. If a relay node determines that it is not the destination node, it floods the RREQ packet again, and the process repeats. Finally, the RREQ packet reaches the destination node, which sends an RREP packet to the source node back along the same route that the RREQ packet followed. Thus, a route is established when the RREP packet reaches the source node.

Next, the behavior of black hole attacks is described. An attacking node that receives an RREQ packets broadcast to the network (hereinafter called a black hole node), then forges and route replay packets (RREP) with a large sequence number and a small hop value and sends them back to the source node. In AODV, the priority of a route is evaluated based on the sequence number of the packet and the hop value. Therefore, when a black hole node receives an RREP packet returned by a black hole node, it misidentifies the route through the black hole node as the latest route to the destination. Figure 1 shows an example of a black hole attack. The nodes are indicated as follows: S is the source node, A is the relay node, D is the destination node, and BH is the black hole attacker. The solid line shows the flow of RREQ packets, and the dashed line shows the flow of RREP packets. In

this example, before the RREQ packet reaches the destination node D via the relay node A, the black hole node BH near the source node S sends a forged RREP packet back to the source node S. As a result, the source node S mistakenly believes that the black hole node BH is the route to the destination node D and establishes a route. All data packets sent after the establishment of the route are relayed to the black hole node BH, and the black hole node discards all data received. This causes a situation where the route is established, but the data do not reach the destination. Even if the source node S tries to establish the route again, it will end up in the same situation as long as the black hole node BH is present.

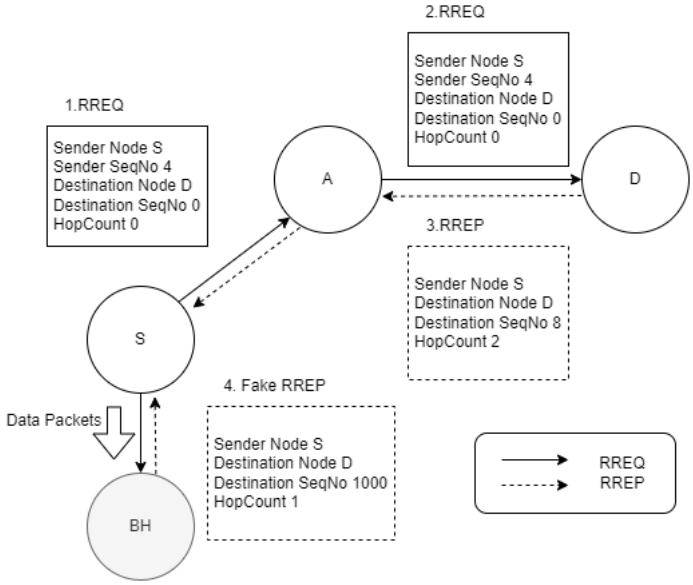


Figure 1. Black hole attack.

2.3. Methods of Defense against Black Hole Attacks

Existing studies of preventing black hole attacks can be divided into two main categories, namely, methods based on opinion and methods based on sequence numbers. Opinion-based defense methods focus on the characteristics of black hole node behavior. A typical example is called Statistical Ad hoc On-demand Distance Vector (SAODV) routing [12]. In SAODV, a given node has an appropriate asymmetric signature–key pair, which provides integrity, authentication, and non-repudiation security features to the route discovery mechanism via digital signature and hash chain mechanisms. Sequence number-based defense methods focus on unnatural sequence numbers set by black hole nodes when they receive packets, and use a threshold value to defend against black hole nodes. One typical example is called Secure Route Discovery for the AODV protocol (SRD-AODV) routing [13]. Sequence number-based methods sometimes identify a normal node as a black hole node. Therefore, hybrid methods that can restore normal nodes to the network by applying an opinion-based redecision mechanism have been developed as well. In a study employing this method, Noguchi et al. [14] applied a dynamic sequence number threshold to RREP packets received by a node to determine whether the sender of the RREP packet is a black hole node. Other studies have aimed to establish secure routes without focusing on the behavior of black hole attacks or sequence numbers. Using a genetic algorithm, Iram et al. proposed ETSAODV, which calculates a confidence value from the previously collected distances between neighboring nodes and determines the routing destination based on this value [15,16] Other studies have aimed to extend the route establishment process of AODV to select a more secure route. Slw-Aodv, proposed by Krishna et al., extends AODV to establish three routes by implementing a route confirmation process with Route Confirm packets and using challenge–response authentication. Slw-Aodv extends AODV by implementing a route confirmation process using Route Confirm packets and then using challenge–response authentication [17].

3. Proposed Method

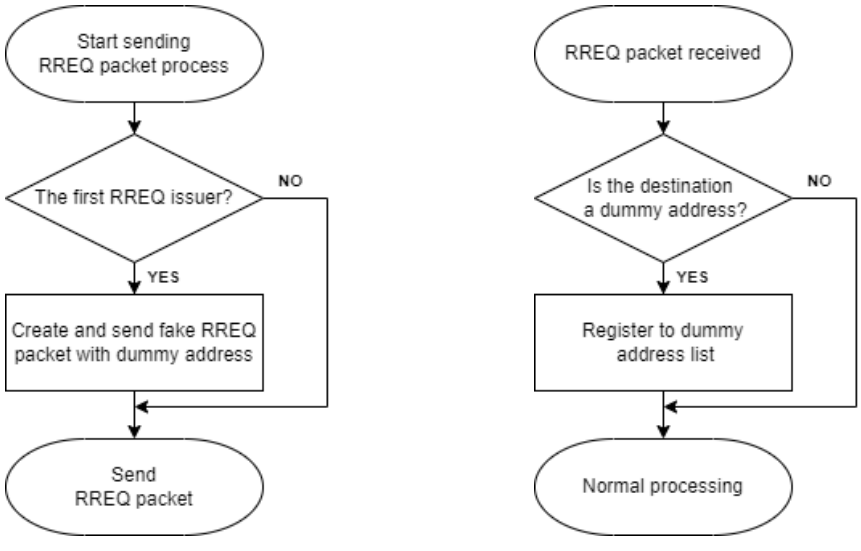
3.1. Summary

MANET devices typically operate with limited CPU processing power, constrained battery life, insufficient bandwidth support, and limited storage. Moreover, the most significant source of energy consumption in MANETs is due to wireless communications, not to computing tasks using the mobile device microprocessor. In fact, the energy consumed by computation is at least 50 percent lower than that consumed by communication [18]. In addition, MANETs lose network connectivity if a node runs out of power; thus, nodes must be able to operate with a limited amount of power for critical operations. Therefore, the communication protocol applied to determine whether a communicating node is a black hole node should be reduced as much as possible to ensure that the amount of required computation is minimal. One problem with existing sequence number-based methods is that the sequence number of RREQ packets flowing through the network tends to increase as the number of nodes in the network increases, which makes misidentification of nodes more likely. To solve this problem, in this paper we consider a mechanism to prevent misidentification. One of the characteristics of a black hole node is that it forges an RREP packet and replies with a forged RREP packet even if it receives an RREQ packet with a destination address that does not exist in the network. Therefore, a normal node can identify a black hole node if it sends back an RREP packet using a forged RREQ packet. In the proposed method, sequence number-based decision mechanisms are not used; instead, a decision mechanism used in related research based on forged RREQ packets for blacklist redecision is incorporated into the transmission of ordinary RREQ packets. This prevents more false positives compared to the standard AODV protocol. Each node corresponding to the proposed method has a dummy address list and a blacklist; these lists consist of entries in which a single unit is a combination of a node's address and time-to-live information.

3.2. Behavior When Processing Control Packets

3.2.1. When Sending/Receiving RREQ Packets

Each node requesting a route issues a forged RREQ packet containing an address that does not exist in the network based on its own address before issuing a normal RREQ packet and then flooding the network. When a node to which the proposed method is applied receives an RREQ packet, it determines whether the packet is forged based on its own address, the source address, and the destination address of the RREQ packet, then registers the packet in the dummy address list if it is determined to be a forged packet. Figure 2 illustrates the process flow when RREQ packets are sent and received.



(**a**) (**b**)

Figure 2. Handling RREQ packets: (**a**) sending RREQ packets and (**b**) receiving RREQ packets.

3.2.2. When Receiving RREP Packets

When a node receives an RREP packet, it first checks its own blacklist. If the address of the source node exists, it deletes the entry related to the source from the route table. Subsequently, it discards the received RREP packet. Next, we consider the case in which the address of the source node is not included in the blacklist. The destination address of the RREP message is checked to verify whether it is stored in the node's dummy address list. If the destination address is included in the dummy address list, the system assumes that the sender is a black hole node and the source address is registered in the blacklist. Finally, the node checks whether a route to the source has been established and discards the route information if it has been established. Then, it issues a route error (RERR) packet and requests the network to delete the route. Finally, the RREP packet is discarded. Figure 3 illustrates the process flow when RREP packets are received.

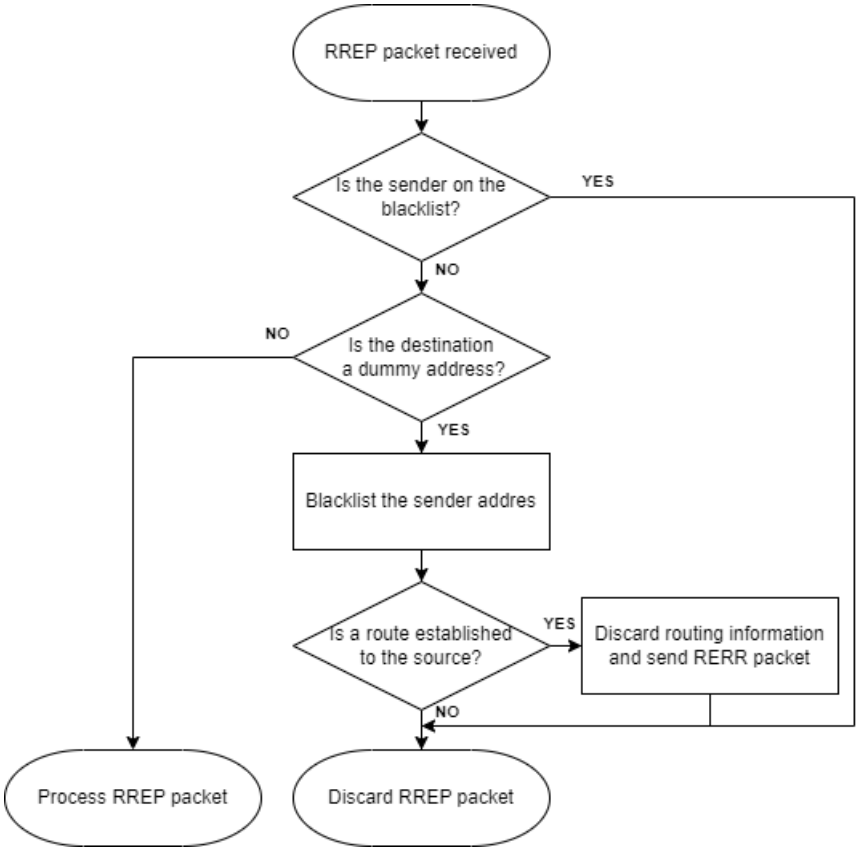


Figure 3. Handling of RREP packets.

4. Preliminary Experiment

4.1. Summary

We experimentally reproduced the proposed method on the ns-3 network simulator; the results verified its validity. We conducted this experiment to verify whether black hole attacks can be reproduced by ns-3, which is a validation of the simulator rather than an experiment to gain new knowledge. Therefore, we prepared an environment in which communication is definitely not possible if there is a black hole node and another in which communication is definitely possible if there is not a black hole node. The simulation time was 10 s, and the source node sent a ping message to the destination node every second. Black hole nodes ware configured to reply to all received RREQ packets with forged RREP packets and to not relay RREQ packets. The arrival rate of packets to the destination node and routing table of each node were verified at the end of the simulation to determine whether the destination node could send data while avoiding black hole nodes.

4.2. Node Deployment

The nodes were arranged in a grid with 250 m intervals, as shown in Figure 4, with 10.0.0.0 as the source node, 10.0.0.2 as the destination node, and 10.0.0.1 as a black hole node. The communication distance of each node was limited to one adjacent node, and the source and destination nodes were adjusted such that they were not adjacent nodes. The dashed circle indicates the communication range of the node. In this experiment, a radius of 250 m was set as the communication range.

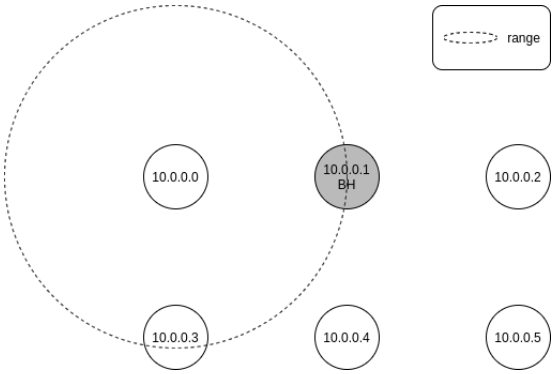


Figure 4. Node placement in preliminary experiment.

4.3. Parameters

The parameter set of the simulator used for this experiment are shown in Table 1. The chosen version of ns-3 was able to apply the program patch for the black hole attack applied in the experiments described below

For the node model, a model considering movement, such as random waypoint or Gauss–Markov, can be used in ns-3. However, if link disconnection occurs owing to the occurrence of movement, it is difficult to distinguish link disconnection due to a black hole attack; thus, a fixed position was used in the preliminary experiment.

Table 1. Parameters used in the preliminary experiment.

Simulator	(ns-3 3.24.1)
Number of normal nodes	5
Number of black hole nodes	1
Transport Protocol	ICMP
Field size	250 × 500 m
Node movement model	fixed position

4.4. Result

4.4.1. Packet Arrival Rate

The packet arrival rate (PAR) is reported in Table 2. AODV (no attack) refers to the result when the black hole node did not attack and simply behaved as a normal node, as reported in Figure 4.

Table 2. Packet arrival rate in the preliminary experiment.

Protocol	**Packet Arrival Rate**
AODV (no attack)	100%
AODV (attacked)	0%
Proposed method (attacked)	100%

4.4.2. Path at the End of the Simulation

The routing table for each node (excluding broadcast and loopback addresses) at the end of the simulation is reported in Table 3. Each item is described as follows:

NodeNo Unique number assigned to each node
Destination Destination node address
Gateway Gateway of destination node address
Flag Entry state, classified into the following three states:

- UP (frequently used)
- DOWN (not used)
- IN_SEARCH (searching for a path)

Hops Number of hops to the destination node

Table 3. Routing table for each node.

NodeNo	Destination	Gateway	Interface	Flag	Hops
	10.0.0.2	10.0.0.3	10.0.0.0	UP	4
Node0	10.0.0.3	10.0.0.3	10.0.0.0	UP	1
(10.0.0.0)	192.168.19.103	102.102.102.102	102.102.102.102	IN_SEARCH	0
	10.0.0.0	10.0.0.0	10.0.0.1	DOWN	1
Node1(BH)	10.0.0.2	10.0.0.2	10.0.0.1	UP	1
(10.0.0.1)	10.0.0.4	10.0.0.4	10.0.0.1	UP	1
	10.0.0.0	10.0.0.5	10.0.0.2	UP	4
Node2	10.0.0.1	10.0.0.1	10.0.0.2	UP	1
(10.0.0.2)	10.0.0.5	10.0.0.5	10.0.0.2	UP	1
	10.0.0.0	10.0.0.0	10.0.0.3	UP	1
Node3	10.0.0.2	10.0.0.4	10.0.0.3	UP	3
(10.0.0.3)	10.0.0.4	10.0.0.4	10.0.0.3	UP	1
	10.0.0.0	10.0.0.3	10.0.0.4	UP	2
	10.0.0.1	10.0.0.1	10.0.0.4	UP	1
Node4	10.0.0.2	10.0.0.5	10.0.0.4	UP	2
(10.0.0.4)	10.0.0.3	10.0.0.3	10.0.0.4	UP	1
	10.0.0.5	10.0.0.5	10.0.0.4	UP	1
	10.0.0.0	10.0.0.4	10.0.0.5	UP	3
Node5	10.0.0.2	10.0.0.2	10.0.0.5	UP	1
(10.0.0.5)	10.0.0.4	10.0.0.4	10.0.0.5	UP	1

4.5. Considerations

When tracing the route table, no entry for the adjacent black hole node 10.0.0.1 was detected in the routing table for 10.0.0.0; moreover, the route to the destination node 10.0.0.2 was

`10.0.0.0→10.0.0.3→10.0.0.4→10.0.0.5→10.0.0.2.`

Note that the proposed method was appropriately blackened. This shows that the proposed method properly detected the black hole node and constructed the path in such a way as to avoid it.

5. Experiment

5.1. Summary

We simulated a black hole attack (http://mohittahiliani.blogspot.com/2014/12/ns-3-blackhole-attack-simulation-in-ns-3.html (accessed on 10 December 2021)) when using the proposed method on the ns-3 network simulator, then compared the performance of our method with that of the existing AODV protocol. In this experiment, we measured the packet arrival rate and round trip time for the following situations:

- Normal AODV with a black hole node
- The proposed AODV with a black hole node
- Normal AODV without a black hole node.

The simulation time was 100 s, and the source node sent a ping message to the destination node every second. The black hole node replied to all received RREQ packets with forged RREP packets, and did not relay RREQ packets.

The evaluation items are as described in Section 5.3, and the results of ten trials for each item are stated below.

5.2. Node Deployment

The size of the field was 500 × 500 m. A source node was placed at (0 m, 0 m), destination node at (500 m, 500 m), and other normal nodes and black hole nodes were placed at random positions in the field at the simulation start time.

5.3. Parameters

The set of parameters and simulators used are reported in Table 4. In this experiment, in order to verify the AODV routing protocol in a form close to the actual assumed network, we adopted the following parameters for the node movement model.

Table 4. Paramaters.

Simulator	ns-3 (ns-3 3.24.1)
Number of normal nodes	5,10,15,20,25,30,35,40,45
Number of black hole nodes	2
Transport protocol	ICMP
field size	500 × 500 m
Node movement model	RandomWayPoint
Node movement speed	1∼5 m/s

5.4. Valuation Items

The Packet Arrival Rate (PAR) and Round-Trip Time (RTT) were used as the two evaluation items.

The PAR is the ratio (%) of the number of data packets received by the destination node to the number of data packets sent by the source node, and is expressed by the following Equation (1):

$$PAR = \frac{N_{dst\_recv}}{N_{src\_sent}} * 100 \quad (1)$$

where N_{src_sent} is the number of data packets sent by the source node and N_{dst_recv} is the number of data packets received by the destination node.

The RTT is the time (ms) required for the source node to send data to the destination node and for the response to return, which is expressed by the following Equation (2):

$$RTT = T_{src\_recv} - T_{src\_sent} \quad (2)$$

where T_{src_send} is the time at which the source node sent the ping message and T_{src_recv} is the time at which the source node received the ping message returned by the destination node.

5.5. Result

Figure 5 shows the packet arrival rate and Figure 6 shows the round-trip time.

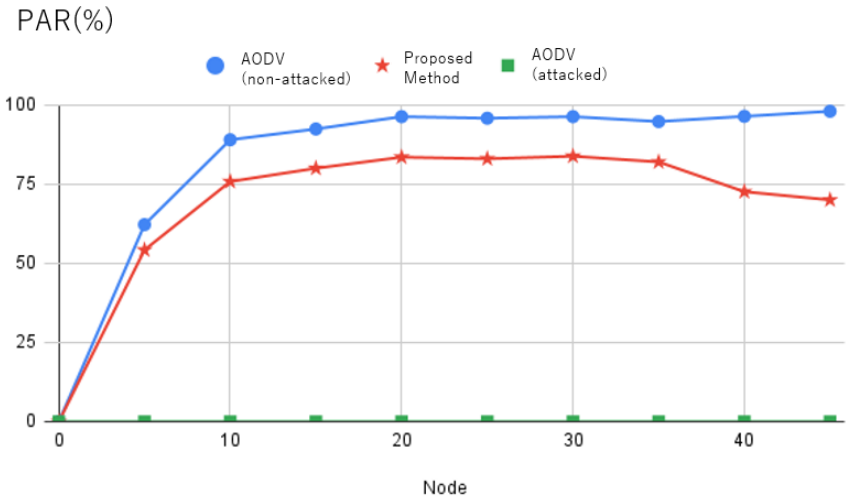


Figure 5. Packet arrival rate (PAR).

The round-trip time of the normal AODV protocol with attacks could not be measured; as shown in Figure 5, the packets did not reach the destination node. Therefore, we measured two AODV points, one indicating the proposed method with attacks and the other indicating the normal AODV protocol without attacks.

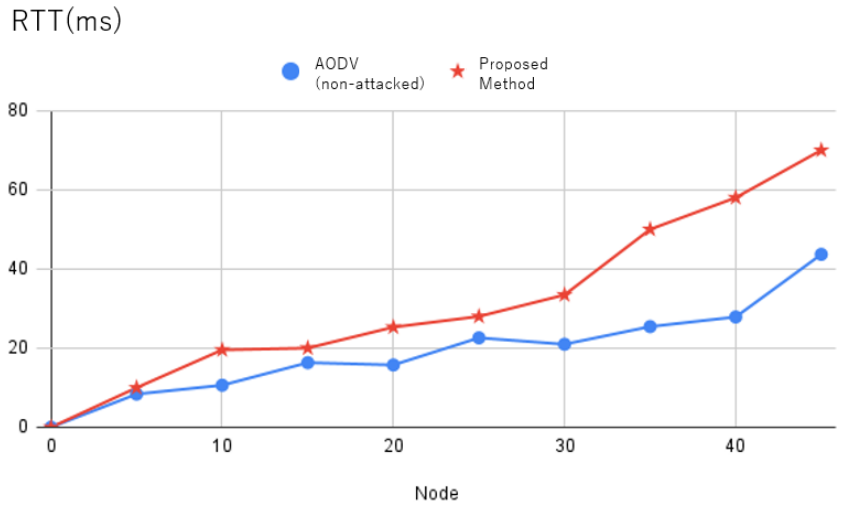


Figure 6. Round-trip time (RTT).

The PAR results show that the network employing the proposed method can efficiently communicate with a network employing the standard AODV routing protocol which is not under attack, although there is a slight degradation of performance compared to the network employing the AODV routing protocol. In contrast, regardless of the number of nodes, the attacked network has a PAR value of zero owing to communication breakdown.

The RTT results show that the performance of the network with fewer nodes is comparable to that of a network with the standard AODV routing protocol that is not under attack; however, the performance slightly degrades as the number of nodes increases.

6. Discussion

First, we discuss the experimental results. With attacks present, the packet arrival rate of the proposed method increases dramatically compared to that of standard AODV. This is because the detection of black hole nodes by dummy RREQ packets and route reconstruction in the proposed method functions well. In contrast, when no attacks are present, the performance of the proposed method is inferior to that of standard AODV.

Without attacks, the round-trip time is higher when using the proposed method, indicating that delays occur in sending and receiving data. The round-trip time is affected by the number of relay nodes along the route. The increase in the round-trip time when using the proposed method is due to the additional time required for processing when a black hole node is detected. From the above, it can be observed that although the proposed method can prevent the occurrence of black hole attacks, it affects performance to a limited extent in terms of both data transmission and reception. In the proposed method, a normal node that detects a black hole node discards its routing information and searches for a new route that does not pass through the black hole node. During this search, no data are transmitted, and the packets that exceed the survival time of the data packet buffer held by the node are discarded. Therefore, such events occur more frequently when the environment in which normal nodes detect black hole nodes becomes more dense, leading to a reduced packet arrival rate in the experiment.

In addition, in the scenario without attacks, the total amount of control packets circulating in the network when using the proposed method is larger than when using standard AODV, which is due to the dummy RREQ packets used to detect black hole nodes and RERR packets used to reconstruct routes. Clearly, these packets cause collisions and loss of data packets. Therefore, although the proposed method is able to reliably detect black hole nodes, there is room for improvement in terms of ensuring route construction that avoids black hole nodes. Finally, we consider the practical feasibility of our proposed approach. The proposed method often uses existing AODV mechanisms to defend against black hole attacks. For example, the dummy RREQ packets are simply an application of the normal RREQ packet-issuing mechanism, and the process of route destruction and reconstruction when a black hole node appears in the route follows the same process relating to existing RERR packets. The only newly added parts are the list that manages node information and the mechanism that controls communication using this information. Therefore, the proposed method consists of a simple algorithm. The advantage of this design is that the algorithm can be easily incorporated into many AODV-derived routing protocols. If a routing protocol uses RREQ, RREP, or RERR packets for routing, those packets can easily be used in the proposed approach. There is no need to create new packet types to improve security.

Furthermore, the algorithm is backwards-compatible. As mentioned above, the proposed method uses the existing AODV packet mechanism. Therefore, terminals that do not apply the proposed method can process dummy RREQ packets in the same way as when receiving normal RREQ packets. Because no RREP packet is returned for dummy RREQ packets, they are not mistakenly registered in the blacklist. Therefore, the routing process need not vary between the terminals to which the proposed method is applied and those to which it is not, enabling straightforward communication between the two. However, if a black hole node exists in the environment, a terminal could be mistakenly registered in the blacklist. This point is discussed further below.

7. Future Research

In the proposed method, a black hole node can be detected only by neighboring nodes that receive a forged RREP packet from the black hole node. One possible countermeasure is to share this information with the surrounding normal nodes to neutralize to the black hole nodes in the network. There are two timing types to consider for issuing dummy RREQ packets: during initial route discovery, and in response to link breakage. In the latter case, a dummy RREQ packet is sent each time a node is unable to correct a break by itself. This can cause frequent flooding of dummy RREQ packets in an environment with frequent link disconnections, which can increase the network load. Moreover, as the dummy RREQ packet has no destination, it will propagate throughout the network if the time-to-live (TTL) is long enough. This can lead to bandwidth overload, particularly if there are frequent link disconnections. However, adjusting the TTL of dummy RREQ packets to make them smaller means that black hole nodes can only be detected around the source node. Hence,

in order to prevent network congestion, the TTL of dummy RREQ packets should be equal to or greater than that of correct RREQ packets. In networks with frequent link changes, reducing the number of dummy RREQ transmissions may become necessary in order to optimize performance.

One common problem observed in related studies, as well as in the proposed method, is that when using dummy RREQ packets to identify black hole nodes, nodes with plain AODV that are not modified (denoted as NA, for Not Available) may exist between the dummy RREQ packet and the black hole node(s) (i.e., S and BH). In such cases, a node that is NA can be misjudged as a black hole node, as shown in Figure 7.

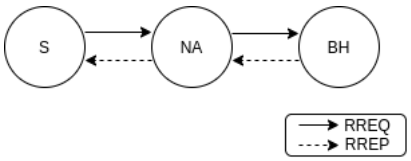


Figure 7. False recognition occurs when an unsupported node exists.

Therefore, to improve the practicality of the dummy RREQ packet-based decision mechanism, nodes must update the hop count of forged RREQ packets at each reception in order to detect only neighboring black hole nodes. The behavior of black hole nodes should be mentioned as well. As a precondition, a black hole node can be detected by the proposed method because it has the characteristic of returning RREQ packets for every RREP packet it receives. However, consider the case where a black hole node behaves as a normal node at certain times and behaves in a malicious manner at others. In this case, the proposed detection approach may not work; accordingly, data cannot be transmitted after the route is established. Although detection can exclude the black hole node from the network when it behaves maliciously during route establishment, this process inevitably decreases network throughput. Extending the above example, consider the case in which a malicious attack occurs outside of the routing phase. For instance, a black hole node may be specified to behave as a normal node during the route establishment phase and to discard data when routing packets for subsequent data communication. After the route is established, the source node repeats routing for route establishment, because it cannot transmit data; however, when routing to establish a route, if this black hole node exists on the route again, it ends up not being able to send data to the destination node. To avoid such loops, a technique is needed to identify nodes that can establish a route but cannot communicate data and to prevent such nodes from being candidates for routes during the routing stage. This technique may additionally be an effective countermeasure against wormhole attacks in MANETs; in such attacks, a wormhole node with a high-speed private channel is installed near the source and destination nodes, and discards data after assigning itself priority as a node on the communication path. As a future work research direction, we plan to evaluate recent related studies and proposed methods in terms of their power consumption, communication volume, and resistance to black hole attacks.

8. Conclusions

Among the various routing protocols proposed for MANET architectures, AODV is a very powerful option; however, the characteristics of MANETs allow the participation of unauthorized terminals in the network. Thus, a malicious attacker can use AODV to launch a black hole attack, which can significantly degrade network performance. Therefore, in this paper we have proposed a method to defend MANETs using the AODV routing protocol against black hole attacks. The proposed method focuses on the fact that black hole nodes behave differently from normal terminals in order to implement an extended AODV protocol that actively detects black hole nodes using dummy RREQ packets. This enables our approach to prevent black hole attacks in a simple manner and send data to the destination via an accurate route. The proposed method is applicable to small environments with few nodes, as verified by a preliminary experiment, as well as to large

environments with many nodes, as verified by further experimentation. In addition, as expressed in the discussion section, the algorithm has high practical potential owing to its simplicity. As we have demonstrated, the performance of the standard AODV protocol can be significantly improved, and the proposed method can be incorporated into many previously proposed AODV-derived routing protocols to increase their security. In the future, we plan to consider methods to enable more efficient routing in networks with frequent link breakage and networks containing nodes that do not implement the AODV protocol on which the proposed method is based.

Author Contributions: Conceptualization, Y.N. and T.M.; investigation, Y.N.; writing—original draft preparation, Y.N.; writing—review and editing, Y.N. and T.M.; visualization, Y.N.; supervision, T.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Matsui, S. The Application Trends to the Real Systems of an Ad Hoc Network. *J. Reliab. Eng. Assoc. Jpn.* **2012**, *34*, 532–539.
2. Al-shareeda, M.A.; Alazzawi, M.A.; Anbar, M.; Manickam, S.; Al-Ani, A.K. A Comprehensive Survey on Vehicular Ad Hoc Networks (VANETs). In Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA), Maysan, Iraq, 25–26 July 2021; pp. 156–160. [CrossRef]
3. Ramakristanaiah, C.; Sam, R.P. A Survey on MANETs in Disaster Rescue Operations. *Int. J. Sci. Res. (IJSR)* **2015**, *4*, 449–451. [CrossRef]
4. Pandey, K.; Swaroop, A. A Comprehensive Performance Analysis of Proactive, Reactive and Hybrid MANETs Routing Protocols. *IJCSI Int. J. Comput. Sci.* **2011**, *8*. [CrossRef]
5. Perkins, C.; Belding-Royer, E.; Das, S. Adhoc On demand Distance Vector. Internet Engineering Task Force Request for Comments, July **2003**. [CrossRef]
6. Singh, M.; Kumar, S. A Survey: Ad-hoc on Demand Distance Vector (AODV) Protocol. *Int. J. Comput. Appl.* **2017**, *161*, 38–44. [CrossRef]
7. Rajeshkumar, V. Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2. *Int. J. Adv. Res. Comput. Commun. Eng.* **2013**, *2*, 4565–4569.
8. Sarika, S.; Pravin, A.; Vijayakumar, A.; Selvamani, K. Security Issues in Mobile Ad Hoc Networks. *Procedia Comput. Sci.* **2016**, *92*, 329–335. [CrossRef]
9. Alani, M.M. MANET security: A survey. In Proceedings of the 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE 2014), Penang, Malaysia, 28–30 November 2014; pp. 559–564.
10. Tseng, F.H.; Chou, L.D.; Chao, H.C. A survey of black hole attacks in wireless mobile ad hoc networks. *Hum.-Centric Comput. Inf. Sci.* **2011**, *1*, 4. [CrossRef]
11. Golchha, H.K.; Pati, A. Survey on Black Hole Attack in MANET Using AODV. In Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 12–13 October 2018; pp. 361–365.
12. Tamilselvan, L.; Sankaranarayanan, V. Prevention of Blackhole Attack in MANET. In Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), Sydney, NSW, Australia, 27–30 August 2007; p. 21.
13. Tan, S.; Kim, K. Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, China, 13–15 November 2013; pp. 1027–1032.
14. Noguchi, T.; Yamamoto, T. Black hole attack prevention method using dynamic threshold in mobile ad hoc networks. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017; pp. 797–802.
15. Iram, N.; Akhilesh, U. Performance Analysis of Efficiently trusted AODV serving Security in MANET under Blackhole Attack Using Genetic Algorithm. In Proceedings of the 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 27–28 January 2023. [CrossRef]

16. Nausheen, I.; Upadhyay, A. ETSAODV: An Efficient and Trusted Secure AODV with Performance Analysis for MANETS suffering Blackhole Attack. In Proceedings of the 2023 Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 5–6 January 2023. [CrossRef]
17. Murty, M.K.; Rajamani, L. Secure and Light Weight Aodv (Slw-Aodv) Routing Protocol for Resilience Against Blackhole Attack in Manets. *Int. J. Soft Comput. Eng. (IJSCE)* **2023**, *13*, 1–9. [CrossRef]
18. Kanellopoulos, D.; Varun, K.S. Survey on Power-Aware Optimization Solutions for MANETs. *Electronics* **2020**, *9*, 1129. [CrossRef]