Proceedings of the Federated Conference on Computer Science and Information Systems pp. 797–802 DOI: 10.15439/2017F101 ISSN 2300-5963 ACSIS, Vol. 11

# Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks

Taku Noguchi
College of Information Science and Engineering,
Ritsumeikan University, Shiga, Japan
Email: noguchi@is.ritsumei.ac.jp

Takaya Yamamoto
College of Information Science and Engineering,
Ritsumeikan University, Shiga, Japan

***Abstract*—A mobile ad hoc network (MANET) is a collection of mobile nodes that do not need to rely on a pre-existing network infrastructure or centralized administration. Securing MANETs is a serious concern as current research on MANETs continues to progress. Each node in a MANET acts as a router, forwarding data packets for other nodes and exchanging routing information between nodes. It is this intrinsic nature that introduces the serious security issues to routing protocols. A black hole attack is one of the well-known security threats for MANETs. A black hole is a security attack in w hich a malicious node absorbs all data packets by sending fake routing information and drops them without forwarding them. In order to defend against a black hole attack, in this paper we propose a new threshold-based black hole attack prevention method. To investigate the performance of the proposed method, we compared it with existing methods. Our simulation results show that the proposed method outperforms existing methods from the standpoints of black hole node detection rate, throughput, and packet delivery rate.**

## I. Introduction

WITH the popularity of mobile devices and the development of wireless communication technology, mobile ad hoc networks (MANETs) have recently attracted attention. MANETs can be constructed by mobile nodes without a pre-existing network infrastructure or centralized administration and can be set up at any time and place. MANETs are useful in a variety of applications, such as emergency communications at disaster sites and vehicle-to-vehicle communications for driver assistance and safety. These types of applications require highly secure communications between mobile nodes because they handle vital information concerning human life and safety. However, MANETs are more vulnerable than conventional networks using fixed infrastructure to attacks such as data modification, identity spoofing, intentional packet dropping, and unauthorized packet reception because the third party nodes act as routers and forward unrelated packets between source and destination nodes.

A *black hole attack* is one of the well-known serious security threats in MANETs [1], [2]. A black hole attack is a security attack in which a malicious node, called a *black hole node*, can absorb all data packets by sending fake routing information, untruthfully claiming a new or fresher route to the destination, and then drops them without forwarding them to the destination. This type of attack significantly degrades network performance, such as packet delivery rate and throughput, because of their repeated packet drops and the routing load due to frequent route reconstructions. AODV [3], one of the principal routing protocols used in MANETs, is significantly threatened by a black hole attack because a black hole node can easily make the source node believe that the path through the black hole node is the best (shortest) path by sending a Route REPly (RREP) packet with a highest sequence number and a small number of hops to the source node.

In this paper, we propose a method of defense against a black hole attack in AODV. The proposed method classifies nodes into two different classes, either normal node or black hole node, by using a dynamically updated sequence number threshold. This threshold is calculated from the total number of active nodes and the time elapsed from the reception of the last routing control packet. In the proposed method, each node checks whether the received RREP sequence number is higher than a dynamically updated threshold value. If it is higher than the threshold value, then the source node of the RREP is considered to be a black hole node and is blacklisted. The proposed method establishes a secure route by excluding the blacklisted nodes. Blacklists maintained by nodes are checked and updated by flooding a dummy Route REQuest (RREQ) packet periodically to avoid misjudgment of black hole nodes. To investigate the performance of the proposed method, it was compared with an existing secure AODV protocol. Our simulation results show that the proposed method outperforms the existing protocol from the standpoints of black hole node detection rate, packet delivery rate, and throughput.

The rest of this paper is structured as follows.

We provide a short introduction to the AODV protocol in Section II and describe the characteristics of a black hole attack in Section III. In Section IV, we provide a detailed description of the proposed method. We study the performance of the proposed method and compare it with the existing protocol through detailed simulation in Section V. Finally, Section VI concludes the paper.

## II. AODV

The Ad Hoc On-Demand Distance Vector (AODV) routing[3] is a protocol widely used in MANETs. AODV establishes a route between the source and destination nodes only when it is desired by the source node, using RREQ and

<table>
<tr><td>Pkt Type</td><td>Reserved</td><td>Hop Count</td></tr>
<tr><td colspan="3">RREQ ID</td></tr>
<tr><td colspan="3">Destination IP Address</td></tr>
<tr><td colspan="3">Destination Sequence Number</td></tr>
<tr><td colspan="3">Source IP Address</td></tr>
<tr><td colspan="3">Source Sequence Number</td></tr>
</table>

(a) RREQ

<table>
<tr><td>Pkt Type</td><td>Reserved</td><td>Hop Count</td></tr>
<tr><td colspan="3">Destination IP Address</td></tr>
<tr><td colspan="3">Destination Sequence Number</td></tr>
<tr><td colspan="3">Source IP Address</td></tr>
<tr><td colspan="3">Lifetime</td></tr>
</table>

(b) RREP

Fig. 1. AODV packet formats.

RREP packets. AODV uses a destination sequence number ($DSN$) to determine an up-to-date path to the destination. A node updates its path information only if the $DSN$ of the current packet received is greater than the last $DSN$ stored at the node. The route discovery process in AODV is as follows:

1) The source node broadcasts a RREQ to its neighbors.
2) The node receiving the RREQ checks whether there is an entry for the destination node in its routing table. It rebroadcasts the RREQ only if there is an old entry or no entry for the destination in its routing table.
3) If the node that received the RREQ is the destination node or an intermediate node that has a fresh enough entry for the destination in its routing table, the destination/intermediate node responds by unicasting a RREP packet back to the source node.
4) The RREP packet is routed back to the source node along the reverse path that is set up when the RREQ is forwarded.
5) A bidirectional path between the source and destination nodes is established through steps 1–4. If the source node receives multiple RREP packets via different paths, it selects a fresher (having a higher $DSN$) and shorter (having a smaller hop count) path from among them as an optimal route.

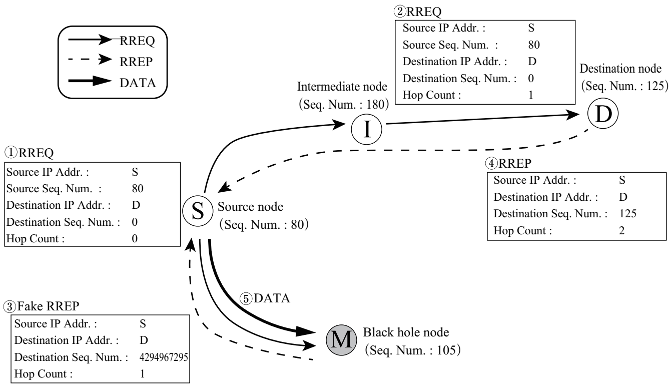

Fig. 2. Black hole attack in AODV.

Figure 1 shows the packet formats for RREQ and RREP. Pkt Type indicates the packet type (“1” for RREQ or “2” for RREP). Hop Count is the number of hops from the source node to the node currently processing the packet. RREQ ID is a sequence number uniquely identifying the particular RREQ originated by a given node. Destination IP Address and Destination Sequence Number are the IP address of the destination node and the last known sequence number of the destination node, respectively. Source IP Address and Source Sequence Number are the IP address of the node that originated the RREQ and the current sequence number associated with the source node, respectively. Lifetime is the time for which nodes receiving the RREP consider the route to be valid.

## III. Black hole attack

A black hole attack is a kind of denial of service where a black hole node can absorb all data packets by sending a fake RREP, untruthfully claiming a new or fresher route to the destination, and then drops them without forwarding them to the destination. Upon receiving a RREQ packet, a black hole node creates a fake RREP packet with a smaller hop count and a spoofed destination sequence number, which is a relatively high destination sequence number in order to pretend that it has a short and fresh route. Once the source node receives the fake RREP packet from the black hole node, it incorrectly recognizes the path through the black hole node as a best path and routes its data packets along that path. Figure 2 shows an example of a black hole attack in AODV. As shown in this figure, the destination node D and the black hole node M receive the RREQ sent from the source node S (①, ②). D sends a RREP packet that contains its sequence number back to S (④). On the other hand, M sends a fake RREP packet that contains a spoofed (large) destination sequence number back to S (③). Although S receives both the legitimate RREP and the fake RREP, it selects the path through D because of the spoofed sequence number and sends data packets to M (⑤). A black hole node absorbs all the data packets and does not forward them to the destination node; therefore, packet delivery rate and throughput are significantly degraded. Additionally, a large amount of control traffic generated by a retransmission control mechanism of the destination node may have a negative impact on the entire network.

## IV. Black hole attack prevention method using dynamic threshold

A black hole node advertises a spoofed destination sequence number to the source node. To prevent a black hole attack, various methods have been proposed [4], [5], [6], [7], [8], [9]. Threshold-based methods [7], [8], [9] detect a black hole node by checking whether the destination sequence number of the RREP is higher than a threshold value. An important

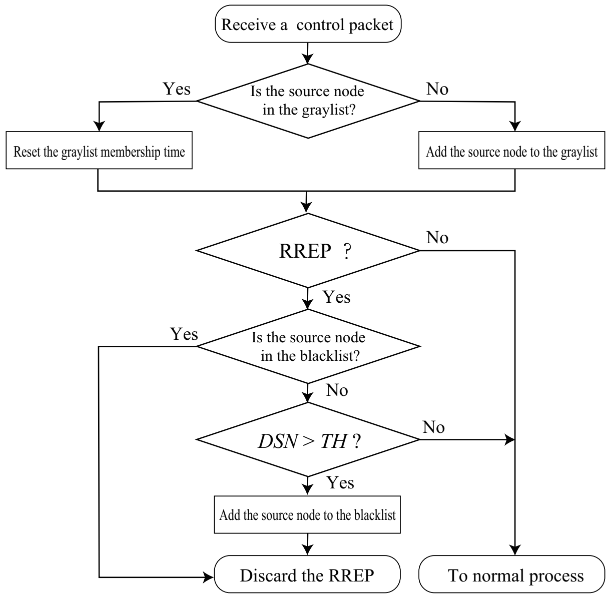
Receive a control packet
Is the source node in the graylist?
Yes
No
Reset the graylist membership time
Add the source node to the graylist
RREP ?
No
Yes
Is the source node in the blacklist?
Yes
No
DSN > TH ?
No
Yes
Add the source node to the blacklist
Discard the RREP
To normal process

Fig. 3. Black hole node detection flow chart.

technical issue in threshold-based methods is to calculate an appropriate threshold to achieve a lower false detection rate and a higher true detection rate. In this paper, we propose a new threshold-based method in which the threshold value is dynamically updated by each intermediate node based on the total number of active nodes in the network and the time elapsed after it knows the last sequence number of the destination node. Additionally, the proposed method rejudges black hole (blacklisted) nodes periodically by using a dummy RREQ packet. The proposed method aims to improve the true detection rate while reducing the false detection rate by using both a threshold-based detection mechanism and a dummy RREP–based mechanism.

### A. *Blacklist construction*

Upon receipt of a RREQ or RREP packet from its neighbors, each node adds the source node of the received packet to its graylist. A graylist entry has four information fields: 1) node address, 2) RREQ flag, 3) RREP flag, and 4) membership time. The node address is the address of the source node of the RREQ/RREP packet. When a node receives a RREQ/RREP packet and then adds an entry to its graylist, it sets the RREQ/RREP flag to 1. The membership time is the lifetime of the graylist membership; the entry is deleted from the graylist after the membership time has elapsed.

When a node I receives a RREP packet, it also checks whether the source node of the RREP packet is in its blacklist. A blacklist entry has two information fields: 1) node address and 2) membership time. If the source node of the RREP packet is blacklisted, I drops the received RREP packet. Otherwise, I checks whether the destination sequence number $DSN$ is higher than the threshold $TH$. If $DSN > TH$, then the source node is blacklisted; otherwise, I processes the RREP packet in the normal way. Figure 3 shows the flow chart of the black hole node detection process.

### B. *Threshold calculation*

In the proposed method, each node calculates $TH$ dynamically based on the total number of active nodes in the network and the time elapsed after it knows the last sequence number of the destination node. We performed preliminary experiments to find appropriate calculation methods for $TH$. Because of space constraints, we omit the details of the preliminary experiments. It was found that a destination sequence number is approximately proportional to both the total number of active nodes and time. Based on this observation, we define the following equation for $TH$:

$$TH = (\alpha N + \beta)t + DSN_{\text{known}} \qquad (1)$$

Here, $\alpha$ and $\beta$ are positive constants to reflect the growth trend of sequence numbers of active nodes. $N$ is the estimated number of active nodes in the network. We use the number of graylist entries as the value for $N$. $DSN_{\text{known}}$ is the last destination sequence number known to the calculating node. If the calculating node does not know the destination sequence number, then $DSN_{\text{known}}$ is set to 0. $t$ is the time elapsed after the calculating node obtains $DSN_{\text{known}}$. If $DSN_{\text{known}} = 0$, the time elapsed since the AODV protocol was started at the node is used as the value for $t$.

### C. *Black hole node rejudgment*

The proposed method uses a blacklist membership time for each blacklisted node in order so that nodes blacklisted falsely, i.e., nodes that are not true black hole nodes but have been mistakenly added to a blacklist, are not blacklisted permanently. At every expiration of blacklist membership, each node rejudges its blacklisted nodes and determines whether to delete from its blacklist the blacklisted node whose blacklist membership has expired, or to reset the time. The remaining time of the blacklist membership is stored as the membership time filed with the blacklist entry. Each node creates a dummy RREQ packet destined for a randomly generated address and broadcasts it whenever a blacklist membership in its blacklist expires. Only a black hole node will respond to the dummy RREQ by sending a RREP packet back to the RREQ source node without checking the destination address of the dummy RREQ. If the node receives a RREP, it adds the source node of the RREP to its blacklist. If the source node of the RREP is already in its blacklist, it resets the blacklist membership time of the source node. Figure 4 shows the flow chart of the black hole node rejudgment process.

## V. Performance evaluation

In this section, we describe our investigation of the performance of the proposed method by comparing it with that of an existing method. For our simulations, we used the network simulator ns-2 [10].

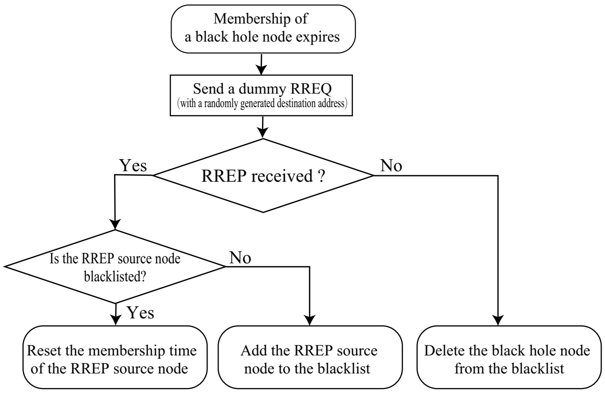

Fig. 4. Black hole node rejudgment flow chart.

TABLE I
SIMULATION PARAMETERS.

| Parameter | Value |
|---|---|
| Simulation time | 200 [s] |
| Number of nodes | 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 |
| Network area | 800 ÃŮ 800 [m] |
| Mobility model | Random Waypoint |
| Transport layer protocol | UDP |
| Application type | CBR |
| Number of black hole nodes | 5 |
| Parameters $\alpha, \beta$ | $\alpha = 0.002, \beta = 0.1$ |
| Blacklist/Graylist membership time | 30 [s] |

## A. Simulation model

In our simulations, 50% of non–black hole nodes try to send their data packets to destination nodes randomly selected from among non–black hole nodes. We assume that black hole nodes always respond to all received RREQs by sending fake RREPs with spoofed destination sequence numbers. The spoofed destination sequence number in a fake RREP is one and a half times as large as the true destination sequence number. AODV with/without a black hole attack and SRD-AODV [9], one of the threshold-based secure AODV protocols, were used as the targets for comparison. Each simulation was run 20 times independently, and the results are an average of the 20 observations. Other simulation assumptions are listed in Table I.

## B. Performance metrics

We evaluated the performance using the following metrics:

*1) True detection rate $R_{\mathrm{t}}$:* We evaluate the accuracy of detection of a black hole node by the true detection rate $R_{\mathrm{t}}$. $R_{\mathrm{t}}$ is defined by the following equation:

$$R_{\mathrm{t}} = \frac{N_{\mathrm{black}}}{N_{\mathrm{fakeRREP}}} * 100 \qquad (2)$$

Here, $N_{\mathrm{fakeRREP}}$ is the total number of fake RREPs received by non–black hole nodes during the simulation. $N_{\mathrm{black}}$ is the total number of blacklist entries (excluding the entries for the nodes blacklisted falsely) of all non–black hole nodes.

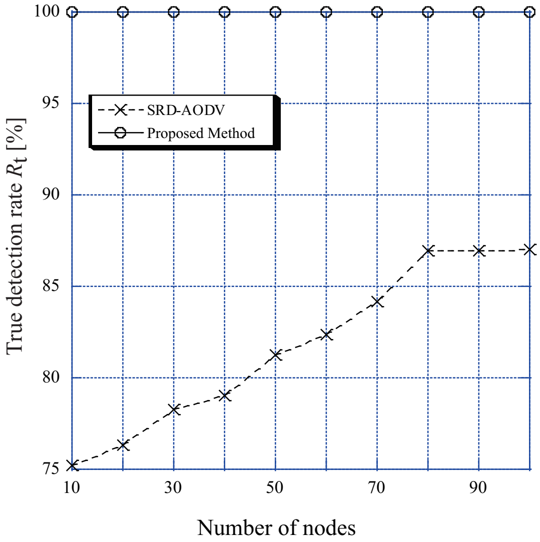

Fig. 5. True detection rate vs. number of nodes.

*2) False detection rate $R_{\mathrm{f}}$:* The inaccuracy of black hole node detection is evaluated by the false detection rate $R_{\mathrm{f}}$. $R_{\mathrm{f}}$ is defined by the following equation:

$$R_{\mathrm{f}} = \frac{N_{\mathrm{discard}}}{N_{\mathrm{RREP}}} * 100 \qquad (3)$$

Here, $N_{\mathrm{RREP}}$ is the total number of legitimate RREPs (not including dummy RREPs and fake RREPs) received by non–black hole nodes during the simulation. $N_{\mathrm{discard}}$ is the total number of legitimate RREPs discarded by non–black hole nodes because of their misidentification.

*3) Throughput:* Throughput is defined by the following equation.

$$\mathit{Throughput} = \frac{\mathit{PktSize} * 8 * N_{\mathrm{recv}}}{T} \qquad (4)$$

Here, $\mathit{PktSize}$ is the data packet size, $N_{\mathrm{recv}}$ is the total number of data packets received by the destination node, and $T$ is the time elapsed from the time the source node receives the first RREP to the end of the simulation.

*4) Packet delivery rate $PDR$:* $PDR$ is the proportion of data packets successfully received by the destination out of all data packets sent by the source node. $PDR$ is defined by the following equation:

$$PDR = \frac{N_{\mathrm{recv}}}{N_{\mathrm{sent}}} * 100 \qquad (5)$$

Here, $N_{\mathrm{sent}}$ is the total number of data packets sent by the source node.

## C. Simulation results

Figure 5 shows the true detection rate characteristics for the proposed method and SRD-AODV. As shown in this figure, the proposed method achieves complete black hole node detection. In the proposed method, the black hole node detection mechanism using both a dynamic threshold and

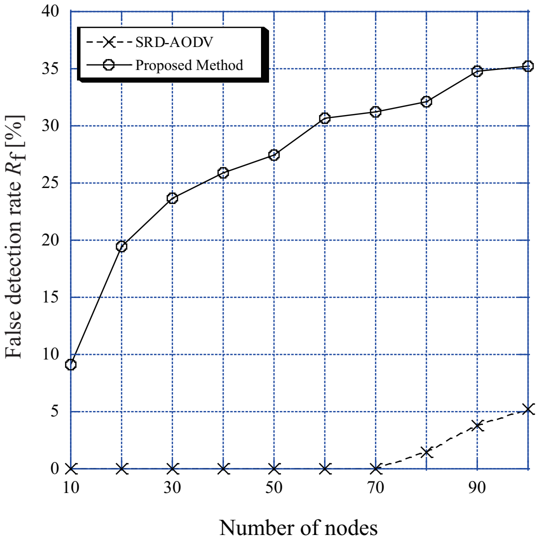

Fig. 6. False detection rate vs. number of nodes.

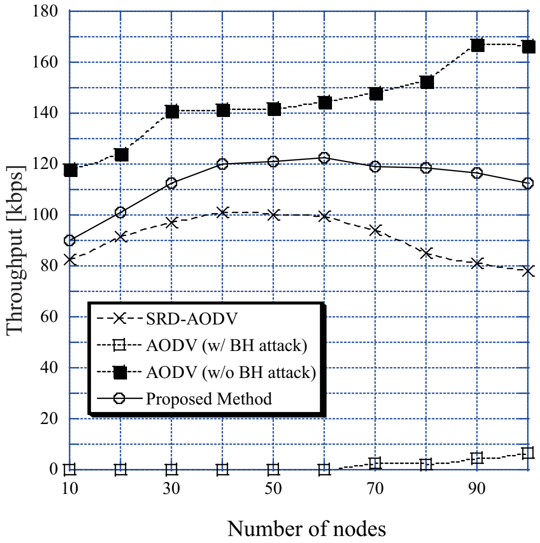

Fig. 7. Throughput vs. number of nodes.

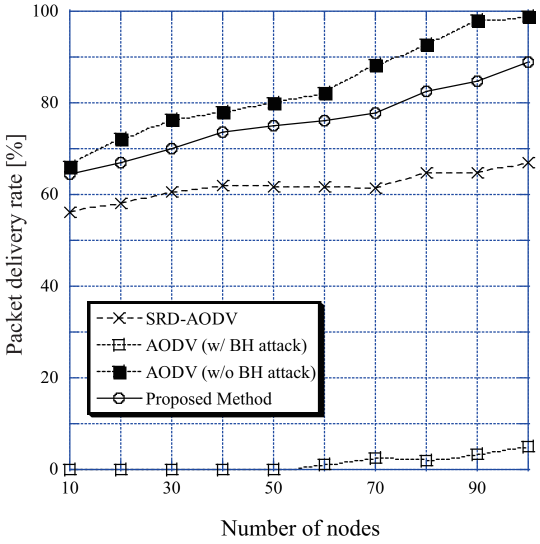

Fig. 8. Packet delivery rate vs. number of nodes.

dummy RREPs contributes to the completeness of the detection. On the other hand, the $R_t$ for SRD-AODV decreases with an increase in the number of nodes. When destination sequence numbers are small, i.e., for a certain period of time after the simulation starts, spoofed destination numbers are also small, and so SRD-AODV cannot detect black hole nodes by using a pre-defined static threshold. SRD-AODV achieves a higher $R_t$ with a larger number of nodes. The reason is that the destination sequence numbers increase quickly with the increase in the number of nodes.

Figure 6 shows the false detection rate characteristics for the proposed method and SRD-AODV. As shown in this figure, SRD-AODV achieves a much lower $R_f$ (less than 5%) than the proposed method. $R_f$ for the proposed method increases with an increase in the number of nodes. The threshold value calculated dynamically using equation (1) is likely to be smaller than the destination sequence numbers when the number of nodes is large, i.e., when the destination sequence numbers are likely to be large. As a result, the false detection rate increases. However, the proposed method was able to delete all the non–black hole nodes from the blacklists by the black hole node rejudgment mechanism with dummy RREPs in our simulations.

Figure 7 shows the throughput performance for the proposed method, AODV with/without black hole (BH) attack, and SRD-AODV. In this figure, AODV without BH attack (i.e., with no black hole nodes) represents the target performance. The proposed method achieves better throughput performance than SRD-AODV and AODV with BH attack. In AODV with BH attack, only very few packets are received by destination nodes because of the black hole attacks. Both the proposed method and SRD-AODV achieve a certain level of throughput performance because both methods can establish a secure route by excluding the black hole nodes. The throughput performance of the proposed method is less than that of AODV without BH attack because the dummy RREP traffic generated by the proposed method causes collision with data packets. SRD-AODV cannot detect black hole nodes for a certain period of time after the simulation starts. This results in the degradation of the overall throughput of SRD-AODV. The throughput performances of the proposed method, SRD-AODV, and AODV without BH attack all become worse with a smaller number of nodes. The reason is that frequent path breaks due to node mobility occur between the source and destination nodes when the number of nodes is small.

Figure 8 shows the packet delivery performance for the proposed method, AODV with/without BH attack, and SRD-

AODV. Similar to the results shown in Fig. 7, the proposed method achieves a higher packet delivery rate than SRD-AODV and AODV with BH attack. The packet delivery rates of the proposed method, SRD-AODV, and AODV without BH attack all increase with an increase in the number of nodes. The reason is that path break probability decreases with the increase in the number of nodes.

## VI. Conclusion

In MANETs, all nodes act as routers. This feature is what leads to the security issues in the routing protocols. The black hole attack is one of the well-known security threats in MANETs. In order to defend against a black hole attack in AODV, we have proposed a prevention method, which detects a black hole node by using a dynamically updated sequence number threshold and dummy RREPs. With simulation experiments, we investigated the effectiveness of our proposed method by comparing its performance with that of existing methods. The simulation results show that our proposed method achieves complete black hole detection and improves throughput and packet delivery performance.

Issues for further research are to validate the proposed method on different scenarios with various network sizes and node mobilities, and to decrease the false detection rate of the proposed method. The false detection rate can be improved by optimizing the values of the $\alpha$ and $\beta$ parameters. Therefore, we plan to propose a method for optimizing the parameter values according to network conditions.

## Acknowledgment

This work was supported by JSPS KAKENHI Grant Number 15K00141.

## References

[1] 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*, vol.1, no.1, pp.1-16, Dec. 2011.

[2] A. Sherif, M. Elsabrouty, and A. Shoukry, "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Adhoc Network (MANET)," in *Proc. IEEE International Conference on Computational Science and Engineering*, pp.346-352, http://dx.doi.org/10.1109/CSE.2013.60, Dec. 2013.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Adhoc On-Demand Distance Vector (AODV) Routing," RFC3561, http://dx.doi.org/10.17487/RFC3561, https://www.ietf.org/rfc/rfc3561.txt.

[4] L. Tamilselvan and V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET," in *Proc. IEEE International Conference on Wireless Broadband and Ultra Wideband Communications*, p.21, http://dx.doi.org/10.1109/AUSWIRELESS.2007.61, Aug. 2007.

[5] D. Kshirsagar and A. Patil, "Blackhole Attack Detection and Prevention by Real Time Monitoring," in *Proc. IEEE International Conference on Computing, Communications and Networking Technologies*, pp.1-5, http://dx.doi.org/10.1109/ICCCNT.2013.6726597, July 2013.

[6] S. Jain and A. Khunteta, "Detecting and Overcoming Blackhole Attack in Mobile Adhoc Network," in *Proc. IEEE International Conference on Green Computing and Internet of Things*, pp.225-229, http://dx.doi.org/10.1109/ICGCIoT.2015.7380462, Oct. 2015.

[7] S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour, "Detecting Blackhole Attack on AODV-Based Mobile Adhoc Networks by Dynamic Learning Method," *International Journal of Network Security*, vol.5, no.3, pp.338-346, Nov. 2007.

[8] 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, pp.54-59, Aug. 2009.

[9] 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*, pp.1159-1164, http://dx.doi.org/10.1109/HPCC.and.EUC.2013.164, Nov. 2013.

[10] DARPA, "The Network Simulator - ns-2" (online), available from (http://www.isi.edu/nsnam/ns/) (accessed 2017-04-20).