Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method

Satoshi Kurosawa[1], Hidehisa Nakayama[1], Nei Kato[1], Abbas Jamalipour[2], and Yoshiaki Nemoto[1]
(Corresponding author: Hidehisa Nakayama)

Graduate School of Information Sciences, Tohoku University[1]
Aoba 6–3–09, Aramaki, Aoba-ku, Sendai, Miyagi 980–8579, Japan. (Email: hidehisa@it.ecei.tohoku.ac.jp)
School of Electrical and Information Engineering, The University of Sydney, Sydney NSW 2006,Australia[2]

(Received Dec. 19, 2005; revised and accepted Jan. 27 & Mar. 3, 2006)

Abstract

This paper analyzes the blackhole attack which is one of the possible attacks in ad hoc networks. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. In this paper, we propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. The simulation results show the effectiveness of our scheme compared with conventional scheme.

Keywords: AODV, anomaly detection, blackhole attack, MANET

1 Introduction

Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. The applications of MANET range from a one-off meeting network, emergency operations such as disaster recovery to military applications due to their easy deployment. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks.

Blackhole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route REPly (RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. By comparing the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the most recent routing information and selects the route contained in that RREP packet. In case the sequence numbers are equal it selects the route with the smallest hop count. If the attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than the real destination node to the source node, the data traffic will flow toward the attacker. Therefore, source and destination nodes became unable to communicate with each other. In [14], the authors investigated the effect of blackhole attack when movement velocity and a number connection toward the victim node are changed, and proposed the detection technique at the destination node. However, we can effectively avoid the attack for example by selecting the detour route during route reconstruction which achieved by detecting the attack at the source node rather than at the destination node. Thus, taking into account the detection at the source node is indispensable.

Regarding the detection of blackhole attack at the source node, [6, 7] have proposed methods in which still they are using the same training data to define the normal state. However, in MANET where the network state changes frequently, the pre-defined normal state may not accurately reflect the present network state. Therefore, using this normal state may degrade the detection accuracy.

In this paper, we use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing [11] for analysis of the effect of the blackhole attack when the destination sequence number are changed via simulation. Then, we select features in order to define the

normal state from the characteristic of blackhole attack. Finally, we present a new training method for high accuracy detection by updating the training data in every given time intervals and adaptively defining the normal state according to the changing network environment.

The rest of this paper is organized as follows. In Section 2, we discuss the related work. Section 3 provides the background on the AODV protocol and describes the characteristic of the blackhole attack. Section 4 analyzes the blackhole attack through simulations. In Section 5, we propose the detection scheme of the attack, and evaluate its effectiveness. Section 6 concludes the paper.

2 Related Works

2.1 Secure Routing

Secure ad hoc routing protocol has been proposed as a technique to enhance the security in MANET. In [3], Hu et al. proposed a common key encryption system for Dynamic Source Routing (DSR) [8]. In Secure AODV (SAOV) [15] and Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [4], secure routing protocol using hash functions have been proposed. In [12], Authenticated Routing for Ad hoc Networks (ARAN), an AODV-based secure routing protocol using public key encryption system is proposed. Hu and Perrig [5] survey the weakness and strength of various secure routing protocols. The above mentioned secure protocols can only guard against external attacks. However, for the internal attacks coming from compromised hosts could still have severe impacts on network performance and its connectivity. Therefore, detecting the internal attack launching from these compromised hosts is indispensable.

2.2 IDS Approaches for MANET

To protect against the blackhole attack, five methods have been proposed. In [2], the method requires the intermediate node to send a RREP packet with next hop information. When a source node receives the RREP packet from an intermediate node, it sends a Further Request to the next hop to verify that it has a route to the intermediate node who sends back the RREP packet, and that it has a route to the destination. When the next hop receives Further Request, it sends Further Reply which includes check result to source node. Based on information in Further Reply, the source node judges the validity of the route. In [9], the method requires the intermediate node to send Route Confirmation Request (CREQ) to next hop node toward the destination. Then, next hop node receives CREQ, and look up its cache for a route the destination. If it has one, it sends Route Confirmation Reply (CREP) to source node with its route information. The source judges whether the path in RREP is valid by comparing the information with CREP. In these methods, the operation is added to routing protocol. This operation can increase the routing overhead resulting in performance degradation of MANET which is bandwidth-constrained. In [13], source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. In ad hoc networks, the redundant paths in most of the time have some shared hops or nodes. When source node receives RREPs, if routes to destination shared hops, source node can recognize the safe route to destination. But, this method can cause the routing delay. Since a node has to wait for RREP packet to arrive from more than two nodes. Therefore, a method that can prevent the attack without increasing the routing overhead and the routing delay is required.

Huang et al. [6] propose a method in which the packet flow is observed at each node. In this method, they define a total of 141 features with traffic related and topology-related, and suggest anomaly detection means with inter-relation between features. In [7], Huang et al. construct an Extended Finite State Automaton (EFSA) according to the specification of AODV routing protocol; modelize normal state; and detect attacks with both specification-based detection and anomaly detection. In specification based detection, they simply detect attacks as deviant packet from condition defined by EFSA. Also, in anomaly detection, they define normal state and compare it with condition of EFSA and amount of statistic of transition, and then detect attacks as a deviation from those states.

From the characteristics of the blackhole attack, we need to take a destination sequence number into account. In [6], feature related to the destination sequence number has not been taken into account as the feature to define the normal state. In [7], the threshold is used and the feature is defined as the number of time that the destination sequence number is greater than the threshold. However, since a destination sequence number changed depending on the network environment, up to a threshold it may be difficult to successfully discriminate between the normal state and the state where blackhole attack took place. And hence cause degradation in detection accuracy.

Except the destination sequence number issue, the above mentioned approaches use static training data to define the normal state. However, we note that the MANET topology can be changed easily, and the difference in network state becomes larger by time. Furthermore, these methods cannot be applied to a network while the training has been done in another network. As a result, these methods are considered difficult in a MANET environment. To solve this problem, normal state needs to be defined using the data reflecting the trend of current situation and this leads to the idea of updating the training process within a time interval. By so doing, attack detection can be adaptively conducted even in a changing network environment.

3 Problem Statement

3.1 Overview on AODV

AODV is a reactive routing protocol [11] in which the network generates routes at the start of communication. Each node has its own sequence number and this number increases when links change. Each node judges whether the channel information is new according to sequence numbers. Figure 1 illustrates the route discovery process in AODV. In this figure, node S is trying to establish a connection to destination D. First, the source node S refers to the route map at the start of communication. In case where there is no route to destination node D, it sends a Route Request (RREQ) message using broadcasting. RREQ ID increases one every time node S sends a RREQ. Node A and B which have received RREQ generate and renew the route to its previous hop. They also judge if this is a repeated RREQ. If such RREQ is received, it will be discarded. If A and B has a valid route to the destination D, they send a RREP message to node S. By contrast, in case where the node has no valid route, they send a RREQ using broadcasting. The exchange of route information will be repeated until a RREQ reaches at node D. When node D receives the RREQ, it sends a RREP to node S. When node S receives the RREP, then a route is established. In case a node receives multiple RREPs, it will select a RREP whose the destination sequence number (Dst_Seq) is the largest amongst all previously received RREPs. But if Dst_Seq were same, it will select the RREP whose hop count is the smallest.

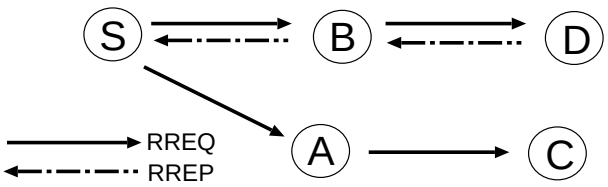


Figure 1: Route discovery process

In Figure 2, when node B detects disconnection of route, it generates Route Error (RERR) messages and puts the invalidated address of node D into list, then sends it to the node A. When node A receives the RERR, it refers to its route map and the current list of RERR messages. If there was a route to destination for node D included in its map, and the next hop in the routing table is a neighboring node B, it invalidates the route and sends a RERR message to node S. In this way, the RERR message can be finally sent to the source node S.

3.2 Description of Blackhole Attack

In AODV, Dst_Seq is used to determine the freshness of routing information contained in the message from originating node. When generating a RREP message, a destination node compares its current sequence number, and

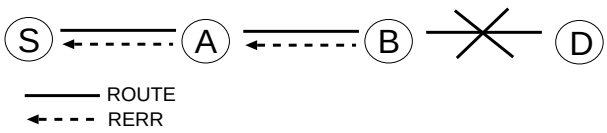


Figure 2: Transferring route error messages

Dst_Seq in the RREQ packet plus one, and then selects the larger one as RREP's Dst_Seq. Upon receiving a number of RREP, a source node selects the one with greatest Dst_Seq in order to construct a route. To succeed in the blackhole attack the attacker must generate its RREP with Dst_Seq greater than the Dst_Seq of the destination node. It is possible for the attacker to find out Dst_Seq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's Dst_Seq base on the received RREQ's Dst_Seq. However, this RREQ's Dst_Seq may not present the current Dst_Seq of the destination node. Figure 3 shows an example of the blackhole attack. The value of RREQ and RREP using in the attack are shown in Table 1.

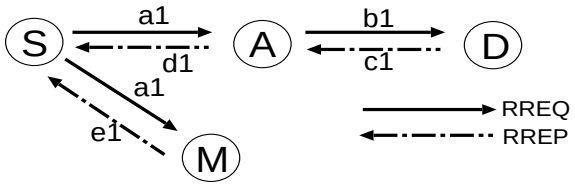


Figure 3: Blackhole attack

Table 1: Values of RREQ and RREP

	RREQ		RREP		
	a1	b1	c1	d1	e1
IP.Src	S	A	D	A	D (MD)
AODV.Dst	D		D		D (MD)
Dst_Seq	60		61		65
AODV.Src	S		-		-

In Table 1, IP.Src indicates the node which generate or forward a RREQ or RREP, AODV.Dst indicates the destination node and AODV.Src indicates the source node. Here, we assume that the destination node D has no connections with other nodes. The source node S constructs a route in order to communicate with destination node D. Let the destination node D's Dst_Seq that the source node S has is 60. Hence, source node S sets its RREQ(a1) and broadcasts as shown in Table 1. Upon receiving RREQ(a1), node A forwards RREQ(b1) since it is not the destination node. To impersonate the destination node, the attacker M sends spoofed RREP(e1) shown in Table 1 with IP.Src, AODV.Dst the same with D and increased Dst_Seq (in this case 65 as) to source node S. At the same time, the destination node D which

received RREQ(b1) sends RREP(c1) with Dst_Seq incremented by one to node S. Although, the source node S receive two RREP, base on Dst_Seq the RREP(e1) from the attacker M is judged to be the most recent routing information and the route to node M is established. As a result, the traffic from the source node to the destination node is deprived by node M.

Next, we consider the case shown in Figure 4. The value of RREQ and RREP using in Figure 4 are shown in Table 2. Similar to Figure 3, source node S attempts to construct a route to destination node D. However, unlike the environment in Figure 3, in this case node B, C and E are also constructing a route to D. Therefore, the destination node D's Dst_Seq that the source node has is significantly different from the current Dst_Seq of node D. Since the most recent Dst_Seq from D that node S has is 60, it set RREQ(a2) as shown in Table 2 and broadcasts. Upon receiving RREQ(a2) ,base on information contained in RREQ(a2) node M sends a spoofed RREP(e2) with Dst_Seq 65 the same with previous situation to the source node. Upon receiving RREQ(b2) node D sends RREP(c2) to the source node. However, this time, since node D constructed route with other nodes, we assume that the Dst_Seq is increased to 70. Then, This RREP(d2) is forwarded by node A. Upon receiving two RREP, node S selects the route to destination node D since the Dst_Seq of node D is the larger one. As a result, the attack is not succeeded.For this reason, the attacker need to set Dst_Seq large enough to overcome significantly changes of the Dst_Seq which differed depending on the traffic condition of the destination node.

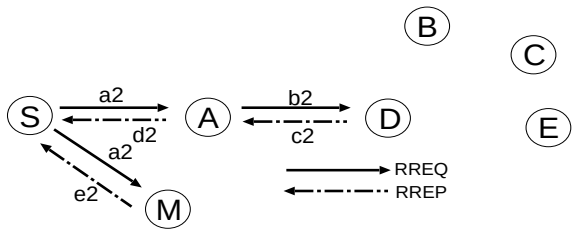


Figure 4: Blackhole attack in some connections to node D

Table 2: Values of RREQ and RREP

	RREQ		RREP		
	a2	b2	c2	d2	e2
IP.Src	S	A	D	A	D (MD)
AODV.Dst	D		D		D (MD)
Dst_Seq	60		70		65
AODV.Src	S		-		-

4 Investigation of Blackhole Attack

In this section, we investigate the effects of the blackhole attack in MANET using NS2 in our simulation. Depending on the traffic involving in a destination node, its Dst_Seq may change. As the recent, in the blackhole attack, the effect of the attack may also change depending on the increased amount of Dst_Seq. Here, we specifically investigate the effects of the attack when the number of connections to the destination and the number of connection from the destination are changed.

4.1 Simulation Environment

For simulation, we set the parameter as shown in Table 3. Random Waypoint Model (RWP) [1] is used as the mobility model of each node. In this model, each node chooses a random destination within the simulation area and a node moves to this destination with a random velocity.

Table 3: Simulation parameters

Simulator	ns-2(ver.2.27)
Simulation time	600(s)
Number of mobile nodes	30
Topology	1000m × 1000m
Transmission Range	250m
Routing Protocol	AODV
Maximum Bandwidth	2Mbps
Traffic	Constant bit rate
Maximum Speed	5(m/s)
pause time	10(s)

Here, we assume that the blackhole attack take place after the attacking node received RREQ for the destination node that it is going to impersonate. Upon receiving RREQ, the attacker set the Dst_Seq of RREP to RREQ's Dst_Seq + x. Here, x is an integer range form 1 to 30.

The node number of each node among 30 nodes in the simulation is given from 0 to 29. We assume that the communication started from a source node to a destination node and the node numbers of the source node, destination node and attacking node are 0, 1 and 29, respectively, as shown in Figure 5.

4.2 Simulation Result of Blackhole Attack

First, we investigate the delivery ratio of packet from source node 0 to destination node 1 in case there are connections from other nodes to the destination node. For the experiment, in Figure 6, nodes which are selected randomly from 2 to 28 (except the source node, destination node, and attacking node) generate traffic toward the destination node. Here, we perform experiment by changing the number of nodes generating the traffic from one to

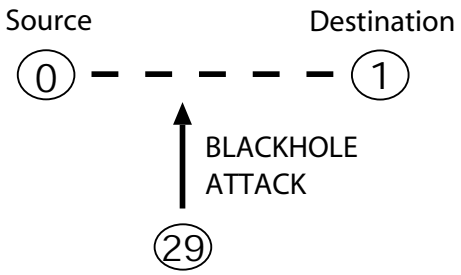


Figure 5: Node descriptions

nine. This experiment is performed repeatedly five times. Figure 7 shows the packet delivery ratio from node 0 to node 1.

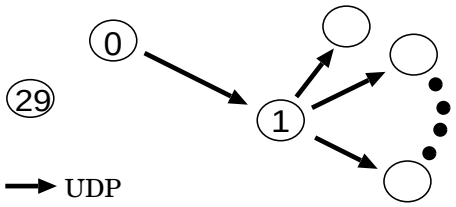


Figure 6: Simulation pattern

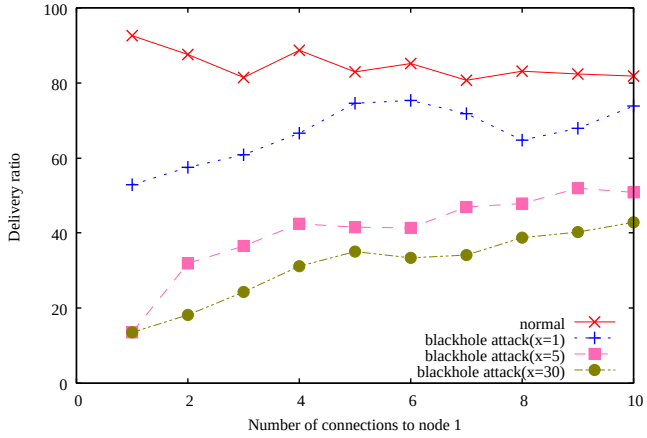


Figure 7: The delivery ratio versus the number of connections to node 1

From Figure 7, we can see that when the number of connection is 1, the more Dst_Seq is increased in blackhole attack the more packet delivery ratio drops. However, when the number of connections increases, the packet ratio increases even when blackhole attack took place. This is because the destination node's Dst_Seq tends to be higher than the attacker's Dst_Seq, since attacker set the Dst_Seq based on the Dst_Seq contained in RREQ coming from the source node. We can see that the more the attacker increase the Dst_Seq, the lower the packet delivery rate is.

Next, we investigate the packet delivery ratio from node 0 to node 1 when destination node 1 generates traffic to other nodes. We assume that destination node 1 generates traffic toward other nodes which their node numbers are randomly selected from 2 to 28 as shown in Figure 6. The experiment is performed by changing the number of selected nodes from one to ten and this experiment is repeated five times. Figure 8 shows the packet delivery ratio from node 0 to node 1.

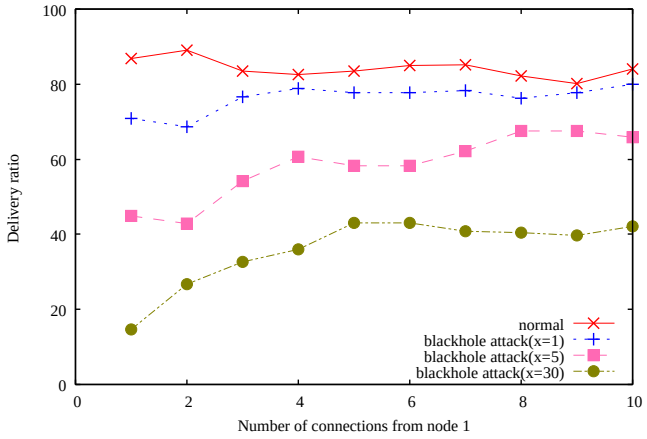


Figure 8: The delivery ratio versus the number of connections from node 1

When the number of connections from node 1 increases, in other words, when node 1 initiates more route discoveries to other nodes, Dst_Seq tends to be increased. For this reason, similar to Figure 7 the packet delivery ratio increases along with the rising of the number of connections. From these results, we can judge that the Dst_Seq of each node change depending on the condition of its traffic.

5 Detecting Blackhole Attack

5.1 Feature Selection

To express state of the network at each node, multidimensional feature vector is defined. Each dimension is counted up on every time slot. In order to detect this attack, the destination sequence number is taken into account. In normal state, each node's sequence number changes depending on its traffic conditions. When the number of connections increases the destination sequence number tends to rise, when there are few connections it tends to be increased monotonically. However, when the attack took place, regardless of the environment the sequence number is increased largely. Also, usually the number of sent out RREQ and the number of received RREP is almost the same. From these reasons we use the following features to express the state of the network.

– Number of sent out RREQ messages

– Number of received RREP messages

– The average of difference of Dst_Seq in each time slot between the sequence number of RREP message and the one held in the list

Here, the average of the difference between the Dst_Seq in RREQ message and the one held in the list are calculated as follows. When sending or forwarding a RREQ message, each node records the destination IP address and the Dst Seq in its list. When a RREP message is received, the node looks over the list to see if there is a same destination IP address. If it does exist, the difference of Dst_Seq is calculated, and this operation is executed for every received RREP message. The average of this difference is finally calculated for each time slot as the feature.

5.2 Discrimination Module of Anomaly Detection

For the traffic that flow across each node, the network state in time slot i is expressed by three-dimension vector $\boldsymbol{x_i} = (\boldsymbol{x_{i1}}, \boldsymbol{x_{i2}}, \boldsymbol{x_{i3}})$. Here, the groups of normal states are considered to be gathered close in feature space. In contrast, the abnormal state is considered to be the scattering data that deviates from the cluster of normal state. According to this, the distribution of network state is shown if Figure 9.

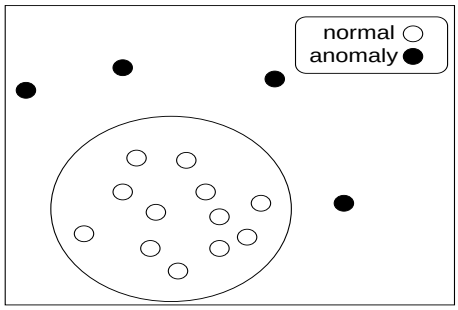


Figure 9: The distribution of network state

From now, we calculate the Mean vector $\bar{\boldsymbol{x}}^{\boldsymbol{D}}$ from Equation (1) using training data set $\boldsymbol{D}$ of N time slots.

$$\bar{\boldsymbol{x}}^{\boldsymbol{D}} = \frac{1}{N}\sum_{i=1}^{N} \boldsymbol{x_i} \tag{1}$$

Next, we calculate the distance from input data sample $\boldsymbol{x}$ to the mean vector $\bar{\boldsymbol{x}}^{\boldsymbol{D}}$ from Equation (2).

$$d(\boldsymbol{x}) = ||\boldsymbol{x} - \bar{\boldsymbol{x}}^{\boldsymbol{D}}||^2 \tag{2}$$

When the distance is larger than the threshold T_h (which means it is out of range as normal traffic), it will be judged as an attack (Equation (3)).

$$\begin{cases} d(\boldsymbol{x}) > T_h & : \text{attack} \\ d(\boldsymbol{x}) \leq T_h & : \text{normal} \end{cases} \tag{3}$$

Here, the projection distance with maximum value is extracted as T_h from the learning data set (Equation (4)):

$$T_h = d(\boldsymbol{x_I}), where\ I = \arg\max_i \max_{\boldsymbol{x_i} \in \boldsymbol{D}} d(\boldsymbol{x_i}) \tag{4}$$

Let ΔT_0 be the first time interval for a node participating in MANET. By using data collected in this time interval, the initial mean vector is calculated, then the calculated mean vector will be used to detect the attack in the next period time interval ΔT .If the state in ΔT is judged as normal, then the corresponding data set will be used as learning data set. Otherwise, it will be treated as data including attack and it will be consequently discarded. This way, we keep on learning the normal state of network. The procedure is shown in Figure 10.

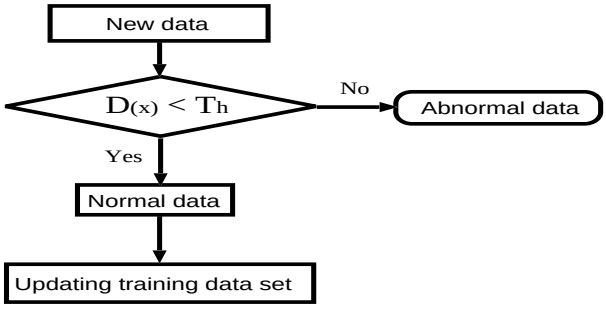


Figure 10: Learning flow chart of proposed method

By doing this, we update the training data set to be used for the next detection. Then, the mean vector which is calculated from this training data set is used for detection of the next data. By repeating this for every time interval ΔT, we can perform anomaly detection which can adapt to MANET environments.

5.3 Simulation Result

Refer to [6, 10], we set the simulation parameter as shown in Table 4.

Table 4: Simulation parameter

Simulator	ns-2(ver.2.27)
Simulation time	10000(s)
Number of mobile nodes	30
Number of malicious node	1
Topology	1000m × 1000m
Transmission Range	250m
Routing Protocol	AODV
Maximum Bandwidth	2Mbps
Traffic	Constant bit rate
Maximum Connection	30
Maximum Speed	1 - 20(m/s)
pause time	10(s)

We assume that initial training data set in time interval ΔT_0 does not contain attack data, this interval is set to 300(s). Refer to [6, 7], we set the time slot i to be 5 (s).

Here, the attacker starts attacking after receiving a RREQ. The Dst_Seq of RREP that the attacker sends is equal to the received RREP's Dst_Seq increased by x, where x is selected randomly from 5 to 30.

From the experiment, the detection rate is shown in Figure 11, and the false positive rate is shown in Figure 12. The horizontal axis shows the mobility rate. Here, *using initial training data only* means that only initial data is used as the training data as in [6, 7]. We do not strictly compare our method to these methods, since some features used in [6] and [7] are different with those used in the proposed method.

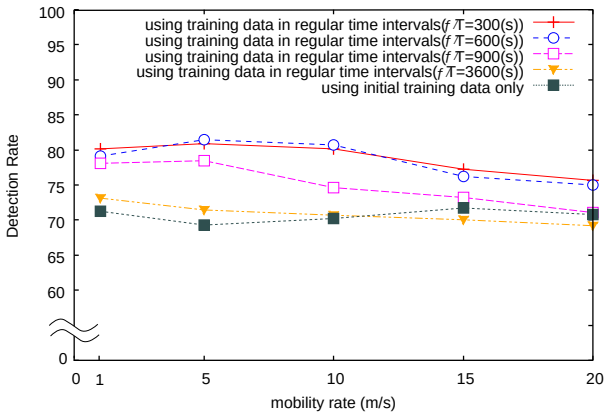


Figure 11: Detection rate versus mobility rate

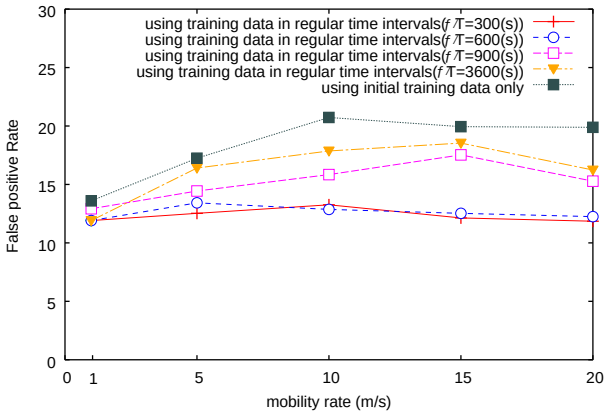


Figure 12: False positive rate versus mobility rate

From these results, we can see that the detection accuracy drops as updating time interval increases. We can also see that it is necessary to shorten the updating interval as the mobility rate become faster. However, the shorter the updating interval is the more processing overhead is needed. Therefore more battery power will be consumed. From these facts, it is necessary to take into account the MANET environment and battery power issue to determine the updating interval. In simulation, even if mobility rate become faster, detection accuracy of the proposed method ($\Delta T = 300$(s)) and ($\Delta T = 600$(s)) are better than the *using initial training data only*. However, the detection accuracy of the proposed method degrades when the updating time interval become longer.

Comparing the proposed method ($\Delta T = 600$(s)) with *using initial training data only*, we found that the average detection rate is increased by more than 8% and the average false positive rate is decreased by more than 6%. From this result, we can see that the detection rate and false positive rate has been improved. In the proposed method, by updating the training data it can adapt to the changing environment in MANET, while *using initial training data only* using only the initial training data can not adapt to the dynamically changing environment. Therefore, we can see that the proposed scheme is effective in anomaly detection.

6 Conclusion

Blackhole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node.

In this paper, we have analyzed the blackhole attack and introduced the feature in order to define the normal state of the network. We have presented a new detection method based on dynamically updated training data. Through the simulation, our method shows significant effectiveness in detecting the blackhole attack.

References

[1] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 257-269, Jul./Sep. 2003.

[2] H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[3] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, pp. 12-23, Sept. 2002.

[4] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *The 4th IEEE Workshop on Mobile Computing Systems & Applications*, pp. 3-13, June 2002.

[5] Y. C. Hu and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 28-39, May/June 2004.

[6] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *The 23rd International Conference on Dis-*

tributed Computing Systems (ICDCS'03), pp. 478-487, May 2003.

[7] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in *The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04)*, pp. 125-145, French Riviera, Sept. 2004.

[8] D. B. Johnson, D. A. Maltz, and Y. C. Hu, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, IETF Internet Draft, draft-ietf-manet-dsr-10, July 2004.

[9] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in *ICPP Workshops*, pp. 73, 2002.

[10] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Personal Communications*, pp. 16-28, Feb. 2001.

[11] C. E. Perkins, E. M. B. Royer, and S. R. Das, *Ad hoc On-Demand Distance Vector (AODV) routing*, RFC 3561, July 2003.

[12] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, "Authenticated routing for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, pp. 598-610, Mar. 2005.

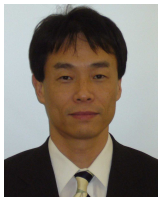
[13] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in *ACM 42nd Southeast Conference (ACMSE'04)*, pp. 96-97, Apr. 2004.

[14] W. Wang, Y. Lu, and B. K. Bhargava, "On vulnerability and protection of ad hoc on-demand distance vector protocol," in *The 10th International Conference on Telecommunications (ICT'03)*, vol. 1, pp. 375-382, French Polynesia, Feb. 2003.

[15] M. G. Zapata, *Secure Ad Hoc on-demand Distance Vector (SAODV) Routing*, IETF Internet Draft,draft-guerrero-manet-saodv-03, Mar. 2005.

Satoshi Kurosawa is currently with the Information Technology R&D Center of Mitsubishi Electric Corporation. He received his B.E. degree from Miyagi University of Education in 2004 and M.S. degree from Tohoku University in 2006. His reserch interests lie in the field of wireless networking, especially ad hoc network securiry. His recent work has focused on ad hoc routing protocols and sensor network security.

Hidehisa Nakayama received his B.E., M.S. and Ph.D. degrees in Information Sciences from Tohoku University in 2000, 2002, 2005, respectively. He is a assistant professor at Tohoku University. He has been engaged in research on computer networking, wireless mobile ad hoc network and pattern recognition and image processing. He is a member of IEEE, the Institute of Electronics, Information and Communication Engineers and the Information Processing Society of Japan. He received the Paper Award for Young Researcher of IPSJ Tohoku Chapter in 2000 and the Best Paper of Pattern Recognition in SCI 2003.



Nei Kato received his M.S. and Ph.D. degrees from the Graduate School of Information Sciences, Tohoku University, in 1988 and 1991, respectively. He has been working for Tohoku University since then and is currently a full professor at the Graduate School of Information Sciences. He has been engaged in research on computer networking, wireless mobile communications, image processing, and neural networks. He has served on the technical program and organizing committees of a large number of international conferences and currently he is a technical editor of IEEE Wireless Communications Magazine. He is a member of IEICE, and a senior member of IEEE. He received the IEEE Communications Society Award for Distinguished Contributions to Satellite Communications in 2005.

Abbas Jamalipour has been with the School of Electrical and Information Engineering at the University of Sydney, Australia, since 1998, where he is responsible for teaching and research in wireless data communication networks, wireless IP networks, network security and satellite systems. He is a Fellow Member of the IEEE, a Fellow Member of IEAust, and a Distinguished Lecturer of the IEEE Communications Society. He holds a PhD in Electrical Engineering from Nagoya University, Japan. He is the author for the first technical book on networking aspects of wireless IP, The Wireless Mobile Internet – Architectures, Protocols and Services (Wiley, 2003). In addition, he has authored another book on satellite communication, Low Earth Orbital Satellites for Personal Communication Networks (Artech House, 1998), and coauthored four other technical books on wireless telecommunications. He has authored over 180 papers in major journals and international conferences, and given short courses and tutorials in major international conferences. He is the Editor-in-Chief of the IEEE Wireless Communications, a technical editor of the IEEE Communications Magazine, the Wiley

International Journal of Communication Systems, Journal of Communications and Networks (JCN), the International Journal of Sensor Networks, and the International Journal of Business Data Communications and Networking. He was Chair of the Satellite and Space Communications Technical Committee, and is currently Chair of the Asia Pacific Board, Chapters Coordination Committee, and Vice Chair of the Communication Switching and Routing Technical Committee, IEEE Communications Society. Professor Jamalipour has been the Technical Program Chair for the 2004 International Symposium on Performance Evaluation of Computer and Telecommunication Systems - SPECTS2004, Technical Program Vice Chair of IEEE Wireless Communications and Networking Conference - WCNC2004, WCNC2005, Co-Chair of Symposium on Next Generation Networks for Universal Services, IEEE International Conference on Communications - ICC2005, and Technical Program Vice-Chair IEEE High Performance Switching and Routing Workshop - HPSR 2005, and the Chair of the Wireless Communications Symposium, IEEE GLOBECOM2005. Dr. Jamalipour was also a Technical Program Vice Chair of IEEE WCNC2006, Co-Chair of Symposium on Next Generation Mobile Networks, IEEE International Conference on Communications - ICC2006, Co-Chair of Symposium on Satellite and Space Communications, IEEE GLOBECOM2006, and Co-Chair of Communications QoS, Reliability and Performance Modelling Symposium, IEEE ICC2007.

Yoshiaki Nemoto received his B.E., M.E., and Ph.D. degrees from Tohoku University in 1968, 1970, and 1973, respectively. He is a full professor with the Graduate School of Information Sciences, and served as director of the Information Synergy Center, Tohoku University. He has been engaged in research work on microwave networks, communication systems, computer network systems, image processing, and handwritten character recognition. He is a co-recipient of the 1982 Microwave Prize from the IEEE Microwave Theory and Techniques Society. He is a Fellow Member of IEICE, and a fellow of the Information Processing Society of Japan. He received the IEEE ComSoc Award for Distinguished Contributions to Satellite Communications in 2005.

A mobile ad-hoc network (MANET) is a self-configuring infrastructureless network of mobile devices. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. AODV (Ad-hoc On-demand Distance Vector) is a loop-free routing protocol for ad-hoc networks.Â The credit is initiated in a route discovery phase. Detecting Blackhole Attack. on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method [18]. Black Hole Detection in. MANET Using AODV Routing Protocol [20]. Proposed method is based on. dynamically updated training data. Use of the promiscuous mode of. Mobile Ad-Hoc Network is an autonomous system where two or more wireless devices or terminals that has the capability to communicate with each other without of any centralized administrator or fixed network infrastructure. Mobile nodes can dynamically form a network to exchange information without the help of any central administration.Â Black Hole Attack. Mobile Ad Hoc Network using the AODV protocol faces an attack named Blackhole attack where a malicious node or Blackhole node consumes the network traffic and drops all data packets.Â To detect the blackhole attack the â€œBlackhole Detection Systemâ€ checks the RREPs that come from multiple paths.