A Self-adaptive Intrusion Detection Method for AODV-based Mobile Ad Hoc Networks

Satoshi Kurosawa[†], Hidehisa Nakayama[†], Nei Kato[†], Abbas Jamalipour[‡], and Yoshiaki Nemoto[†]
[†]Graduate School of Information Sciences, Tohoku University
Aoba 6–3–09, Aramaki, Aoba-ku, Sendai, Miyagi, 980–8579 Japan
[‡]School of Electrical and Information Engineering, The University of Sydney, Sydney NSW 2006,Australia
kuro@it.ecei.tohoku.ac.jp

Abstract

Mobile ad hoc networks (MANET) are usually formed without any major infrastructure. As a result, they are relatively vulnerable to malicious network attacks and therefore the security is a more significant issue than in infrastructure-type wireless networks. In these networks, it is difficult to identify malicious hosts, as the topology of the network changes dynamically. A malicious host can easily interrupt a route for which the malicious host is one of the forming nodes in the communication path. In the literature, there are several proposals to detect such malicious host inside the network. In those methods usually a baseline profile is defined in accordance to static training data and then they are used to verify the identity and the topology of the network, thus avoiding any malicious host to be joined in the network. Since the topology of a MANET is dynamically changing, use of a static profile is not efficient. In this paper, we propose a new intrusion detection scheme based on a learning process, so that the training data can be updated at particular time intervals. The simulation results show the effectiveness of the proposed technique compared to conventional schemes.

1 INTRODUCTION

Mobile ad hoc networks (MANET) recently have received particular attention as part of next generation network technologies. These networks are usually constructed using mobile and wireless host with minimum or no central control or point of attachment such as a base station. These networks could be useful in a variety of applications from a one-off meeting network, to disaster and military applications, and to the entertainment industry.

Because in a MANET the network topology is changing frequently and there is no central management unit, all routing management are performed by individual nodes in a collaborative way. Consequently, there would be no authentication server that can use conventional cryptographic schemes to secure the network against attacks from malicious host. Typical types of attacks in MANET include: eavesdropping, spoofing, forged packets, denial of service (DoS), and so on.

Secure routing protocol [1],[2] in which cryptographic technologies are applied have been suggested as a means for increasing the security in MANET. However, these methods cannot protect the network from attacks of a harmful node who has acquired the network key. Therefore other security methods which can detect attacks from malicious hosts are required.

If a well-known attack in TCP/IP protocol stack is assumed in a MANET, it is possible to protect the network by using conventional security techniques. But if the attacker maliciously uses the specific routing protocol of the MANET, the prevention becomes remarkably difficult. In such a case it is almost impossible to recognize where and when the malicious node exists. Thus the attack detection at each node becomes necessary.

Techniques for detecting malicious attacks are usually classified into two categories of misuse detection and anomaly detection [3]. In misuse detection, a means that uses traffic pattern is widely implemented. In this method, attacks are identified by comparing the aggregated input traffic pattern with the output patterns in routers of the network. Anomaly detection is a technique that defines quantitatively the baseline profile of normal system activity with any deviation from the baseline is treated as a possible system intrusion.

It is rather easy to detect an attack whose traffic pattern is identifiable by using misuse detection. However for those attacks whose type or traffic patterns are hard to identify by the misuse detection, the method is inefficient. In such cases, those attacks can be detected

0-7803-9466-6/05/$20.00 ©2005 IEEE

only by using the anomaly detection.

In anomaly detection method, even when the traffic pattern is unknown, if we can extract the normal state of a network, then the abnormality can be recognizable. In reference [4], the effectiveness of such kind of detection method in wired networks has been shown. In this method, the normal state is pre-extracted and then it is applied to the same network. For MANET since the network conditions can change heavily, the pre-extracted network state may not reflect the present network state correctly. This problem influences the detection accuracy in the anomaly detection method.

As a case study in this paper, we will use one of the most popular MANET routing protocols, i.e., the Ad hoc On-demand Distance Vector (AODV) routing [5]. In this paper, a new learning method is proposed in which the network state is updated in given intervals. This method can automatically adapt to the changing network environment, and thus preventing degradation of the detection accuracy. We evaluate the effectiveness of the proposed method by simulation using the Network Simulator, NS2 [6].

The remainder of the paper is organized as follows. In Section 2, we present the problems of conventional detection schemes in attacks against MANET. Next in Section 3, we presents an overview of AODV. Section 4 proposes our detection scheme. In Section 5, a simulation model and parameters are introduced and some numerical results on the performance of proposed detection scheme are provided. Section 6 gives conclusions and future works.

2 RELATED WORKS

2.1 Attack detection in individual nodes

Secure ad hoc routing protocols have been proposed as a technique to enhance the security in MANET. In [2], Y.C. Hu *et.al.* proposed a common key encryptosystem to Dynamic Source Routing (DSR) [7]. Secure AODV (SAODV) [1] and Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [8] are examples of the secure routing protocols using hash-based functions. In [9], Authenticated Routing for Ad hoc Networks (ARAN) is proposed using public-key cryptographic mechanisms based on AODV. Hu and Perrig [10] survey the weakness and strength of various secure routing protocols. In [11], a distributed certification authority mechanism is proposed, in which the authentication uses threshold cryptography. In [12], MANET is divided into clusters and a certification authority is appointed in each cluster. In [13], a method called key pre-distribution scheme (KPD) is applied. These methods can only guard against external attacks. But the internal attacks coming from malicious hosts could still have severe impacts on network performance and its connectivity.

Therefore, other techniques which can detect attacks in MANET are later proposed. For instance, Kachirski and Guha [14] proposed a method that detects attacks by distributed mobile agents. Vinga *et al.* [15] detect attacks by placing AODVSTAT sensors within the network and observing solely contiguous nodes, or trading information with other sensors. Tseng *et al.* [16] method places a Network Monitor (NM) inside the network. In this method, the NM is constantly monitoring the packet flow in network within a certain range and then detects any attack. But placing effective sensors and NM for detection is thought to be difficult when the MANET topology is dynamically changing. One solution is to observe the packet flow on each node and detect any potential attack.

2.2 Dynamic anomaly detection method

Huang, *et al.* [17] 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 interrelation between features. In [18] Huang and Lee construct an Extended Finite State Automaton (EFSA) according to the specification of AODV routing protocol; make normal condition modeling; 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 condition and compare it with condition of EFSA and amount of statistic of transition, and then detect attacks as a deviation from those conditions. For defining the normal state, in both methods, learning data are extracted beforehand from the same network environment where the test data are applied. 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 where the learning 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 the current situation and this leads to the idea of updating the learning process within a time interval. By so doing, attack detection can be adaptively conducted even in a changing network environment.

3 OVERVIEW ON AODV

AODV is a reactive routing protocol [5] 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. When a node wants to find a route to a destination node, it broadcasts a Route Request (RREQ) message with a unique RREQ ID to all its neighbors. When a node receives a RREQ message, it updates the sequence number of source node and sets up reverse routes to the source node in the routing tables. If the node is the destination or the node has a valid route to the destination, it unicasts a route reply (RREP) back to the source node. The source node or the intermediate nodes that receives RREP will update its forward route to destination in the routing tables. Otherwise, it continues broadcasting the RREQ. If a node receives a RREQ message that has already processed, it discards the RREQ and does not forward it.

When a link is broken, route error packets (RERR) are propagated to the source node along the reverse route and all intermediate nodes will erase the entry in their routing tables.

4 PROPOSAL OF ADAPTIVE INTRUSION DETECTION

4.1 Feature selection

For expressing network state at each node, multi-dimensional feature vector is defined. Each dimension is counted up on every time slot. In this paper, 14 features including nine features related to path finding and four features related to path abnormality and one feature related characteristics of AODV are taken into consideration.

Path finding related features (nine dimensions)

- Number of received RREQ messages (three types)
- Number of forwarded RREQ messages
- Number of sent out RREQ messages
- Number of sent out RREP messages (two types)
- Number of received RREP messages (two types)

For each node, the number of received RREQ messages includes three types, i.e., messages with their own source IP address, messages with their own destination IP address, and messages with neither source nor destination IP address of their own. When counting the number of received RREP messages, packets with same destination IP address, source IP address, RREQ ID, and Src_Seq are counted only once for each time slot. Similarly, the number of sent out RREP messages includes two types for which the destination node is itself, and for which it holds the path towards the destination node. The number of received RREP messages includes two types: the first type is a packet whose source address and destination address are the same, and the other is the case excluding the first type.

Path abnormality features (four dimensions)

- Number of received RERR messages
- Number of sent out RERR messages
- Number of dropped RREQ messages
- Number of dropped RREP messages

When counting the number of received RREQ messages, packet with the same destination IP address and Dst_Seq are counted only once for each time slot.

AODV characteristic feature (one dimensions)

- The average of difference of Dst_Seq in each time slot between the number of received RREP messages and the one held in the list.

When sending or forwarding a RREQ message, each node keeps 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. Due to the link error in ad hoc networks, sometimes nodes might receive an old RREP message. In this case, the newly received Dst_Seq in RREP is smaller than the one already kept in the list. When this happens, the calculation is excluded.

4.2 Discrimination module of anomaly detection

Each node observes the traffic of its own, uses a time slot to count up the traffic according to its kinds. A time interval consists of several time slots. In time slot i, the network state is expressed by a k-dimension vector $\boldsymbol{x_i}$. Suppose there are learning data of N time slots in data set $\boldsymbol{D}$, we calculate from Eqs. (1) and (2) the average of $\bar{\boldsymbol{x}}^{\boldsymbol{D}}$ and covariance matrix $\boldsymbol{\Sigma}^{\boldsymbol{D}}$ as follows.

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

$$\boldsymbol{\Sigma}^{D} = \frac{1}{N}\sum_{i=1}^{N}(\boldsymbol{x_i} - \bar{\boldsymbol{x}}^{\boldsymbol{D}})(\boldsymbol{x_i} - \bar{\boldsymbol{x}}^{\boldsymbol{D}})^T \tag{2}$$

where $\boldsymbol{x_i}$ denotes the i-th learning data sample, $\boldsymbol{x_i} = (\boldsymbol{x_{i1}}, \boldsymbol{x_{i2}}, \boldsymbol{x_{i3}}, \ldots, \boldsymbol{x_{ik}})$. From $\bar{\boldsymbol{x}}^{\boldsymbol{D}}$ and $\boldsymbol{\Sigma}^{\boldsymbol{D}}$, we use the Principal Component Analysis (PCA) [19] to analyze the statistical nature of the current time interval. PCA is the method that explores the correlations between each feature and find the most important axis to express the scattering of data. Here, the most important axis denotes the normal state of network activity, and when a attack takes place, it generally deviates from this axis.

Using PCA, the first principal element $\boldsymbol{\phi}$ which reflects the approximate distribution of the learning data sets is calculated. Here, we consider the projection distance of input data sample $\boldsymbol{x}$ as defined by Eq. (3).

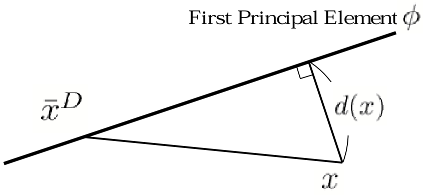


Figure 1. Projection distance

$$d(\boldsymbol{x}) = ||\boldsymbol{x} - \bar{\boldsymbol{x}}^{\boldsymbol{D}}||^2 - \boldsymbol{\phi}^T(\boldsymbol{x} - \bar{\boldsymbol{x}}^{\boldsymbol{D}}) \qquad (3)$$

When the projection distance is larger than the threshold T_h, (which means it is out of the range as normal traffic) it will be judged as attack (Eq. (4)).

$$\begin{cases} d(\boldsymbol{x}) > T_h & : \text{attack} \\ d(\boldsymbol{x}) \leq T_h & : \text{normal} \end{cases} \qquad (4)$$

Here, the projection distance with maximum value is extracted as T_h from the learning data set (Eq. (5)):

$$\begin{cases} I = \arg\max_{i} \max_{\boldsymbol{x_i} \in \boldsymbol{D}} d(\boldsymbol{x_i}) \\ T_h = d(\boldsymbol{x_I}) \end{cases} \qquad (5)$$

Figure 2 gives an rough image of judging the normal or abnormal state by projection distance in the two dimensions.

4.3 Proposal of adaptive anomaly detection

Since the network topology changes easily in MANET, the present state cannot be expressed appropriately when time is elapsing. Therefore, by using only the method described in section 4.2 to define the normal state it would be insufficient to reflect the changing situation, a learning method that can follow the changes of MANET is indispensable. Next, we explain the idea of dynamically updating the learning data sets.

Let ΔT_0 be the first time interval for a node participating in MANET. By using data collected in this time interval, initially the first principal element is calculated, then the calculated first principal element will be used in the following time interval ΔT for anomaly detection. 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 Fig. 3.

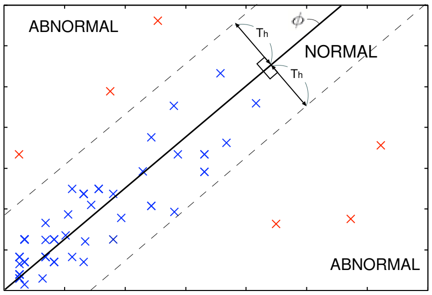


Figure 2. Dividing projection distance into two states

When updating the database, it might be possible to use the very recent data set too, but since the most recent data set is easily affected by the sudden change of the network, it is necessary to take the time series model into consideration to avoid the database from being too sensitive to a change in the network topology. Here, we use the forgetting curve [20] as the weighting function to adjust the degree of importance of the time slot. The forgetting curve aims at reducing the weight when data are getting old.

Suppose using m data sets as learning data sets, Fig. 4 shows how to weigh the data sets in learning. In Fig. 4, $\lambda_1, \lambda_2, \ldots, \lambda_m$ are forgetting coefficients corresponding to each training data set respectively. The forgetting curve is expressed as Eq. (6).

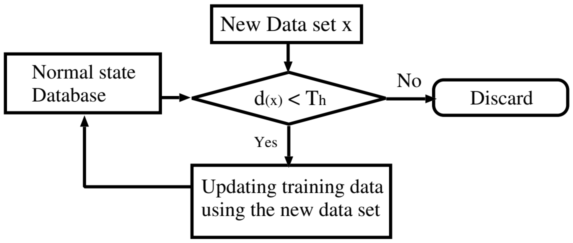


Figure 3. Learning flow chart of proposed method

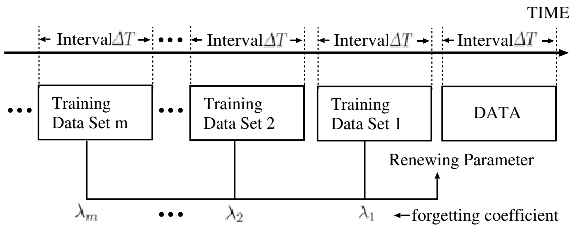


Figure 4. Renewing training data using forgetting coefficient

$$\lambda_j = \lambda_0 \cdot \exp(-a \cdot j\Delta T) \quad (j = 1, 2, \dots, m) \tag{6}$$

where a and λ_0 are constants. $\lambda_1, \lambda_2, \dots, \lambda_m$ are constrained by Eq. (7):

$$1 = \lambda_1 + \lambda_2 + \dots + \lambda_m \tag{7}$$

As for calculating first principal element, first we use Eqs. (1) and (2) to calculate. $\bar{\boldsymbol{x}}^{\boldsymbol{D_1}}, \bar{\boldsymbol{x}}^{\boldsymbol{D_2}}, \dots, \bar{\boldsymbol{x}}^{\boldsymbol{D_m}}$ and covariance matrix $\boldsymbol{\Sigma}^{\boldsymbol{D_1}}, \boldsymbol{\Sigma}^{\boldsymbol{D_2}}, \dots, \boldsymbol{\Sigma}^{\boldsymbol{D_m}}$ from each data set $\boldsymbol{D}_1, \boldsymbol{D}_2, \dots, \boldsymbol{D}_m$. Then using $\lambda_1, \lambda_2, \dots, \lambda_m$ as weighting factors to calculate $\bar{\boldsymbol{x}}^{\boldsymbol{U}}$ and covariance matrix $\boldsymbol{\Sigma}^{\boldsymbol{U}}$ as follows.

$$\bar{\boldsymbol{x}}^{\boldsymbol{U}} = \lambda_1 \bar{\boldsymbol{x}}^{\boldsymbol{D_1}} + \lambda_2 \bar{\boldsymbol{x}}^{\boldsymbol{D_2}} + \dots + \lambda_m \bar{\boldsymbol{x}}^{\boldsymbol{D_m}} \tag{8}$$

$$\boldsymbol{\Sigma}^{\boldsymbol{U}} = \lambda_1 \boldsymbol{\Sigma}^{\boldsymbol{D_1}} + \lambda_2 \boldsymbol{\Sigma}^{\boldsymbol{D_2}} + \dots + \lambda_m \boldsymbol{\Sigma}^{\boldsymbol{D_m}} \tag{9}$$

From $\bar{\boldsymbol{x}}^{\boldsymbol{U}}$ and $\boldsymbol{\Sigma}^{\boldsymbol{U}}$, the new first principal element $\boldsymbol{\phi}^{\boldsymbol{U}}$ is derived and then it will be used to calculate projection distance. The threshold T_h^U will be extracted from all learning data set $\boldsymbol{U} = \{\boldsymbol{D_1} \cup \boldsymbol{D_2} \cup \dots \cup \boldsymbol{D_m}\}$ as described in Eq. (5). By doing this, we update the learning data set gradually, so the new first principal element is always being used in detection.

5 PERFORMANCE EVALUATION

In this section, we use the Network Simulator NS2 [6] to evaluate the proposed method. As for the conventional method, the learning method using the initial set is assumed.

5.1 Attacks used in simulation

Five types of attacks introduced in reference [21],[22],[23] are used in our simulation. Details are as follows.

Modification of RREP-1

Attacks with forged source address in IP header and destination address. The Dst_seq in RREP intentionally increased.

Modification of RREP-2

Attacks with randomly selected source address in IP header and forged destination address. The Dst_seq in RREP is intentionally increased.

Modification of RREQ

Attacks with a intentionally increased the RREQ ID and Src_seq when a RREQ is received. The source address in IP header is false in these attack.

Malicious flooding-1

Attacks with forged source IP address, sending more than 20 packets per second.

Malicious flooding-2

Attacks with fixed IP address and the RREQ ID is intentionally increased, sending more than 20 packets per second.

5.2 Simulation environment

We assume that the simulation network being used is in a place for event, such as that in [17][24]. Various parameters for the simulation are shown in Table 1. For the moving pattern for each node, we use a Random Way-Point model (RWP) [25] in which each node randomly selects destinations in the designated simulation area with random speeds. Figure 5, shows the moving pattern within a certain time period. In this simulation, five types of attacks were randomly executed from 2500(s) to 5000(s), all nodes except the attack node are applied the proposed method to detect the attacks. For starting the learning process, the first normal state, which excludes the attack data, is pre-extracted manually from a learning data. This is because our proposed method detects the possibility of attacks according to the degree which a state deviates from the normal ones. Here, the first time interval is set to 300(s), a period that enough normal state samples can be collected. The time interval of updating is empirically set to 600(s) for this simulation environment. Time slot i is set to 5(s) as in [17][18].

5.3 Method of deciding the number of data sets in used in learning process and parameter a in Eq.(6)

In reference [26], the mobility metric of MANET in RWP is expressed using the number of neighbor nodes. Using the number of neighbor nodes, the number of data sets used in learning process and parameter a in Eq. (6) can be determined dynamically. Assume that for a given node, at time now, its neighbor set is $\mathbb{N}_0$, and at time ascending to $(m+1)\Delta T$(s), its neighbor set is $\mathbb{N}_{m+1}$. If $\mathbb{N}_0 \cap \mathbb{N}_{m+1} = \emptyset$, we can judge that the

Table 1. Simulation parameter

Simulator	ns-2(ver.2.27)
Simulation time	10000(s)
Number of mobile nodes	50
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	5(m/s)
pause time	10(s)

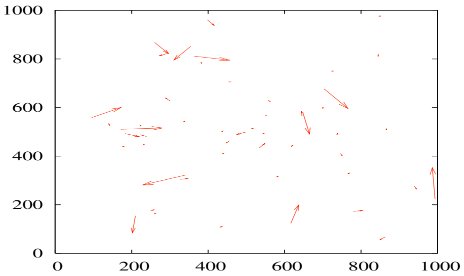


Figure 5. Mobility pattern for random waypoint in five seconds

network state has changed greatly, and m is determined as the number of learning data sets.

a in Eq. (6) is the size of change in network. The size of change in network is expressed by the size of a change in the number of neighbor nodes. Assume that for a given node, at time ascending to $\varDelta T$(s), its neighbor set is $\mathbb{N}_1$, $|\mathbb{N}_0 - \mathbb{N}_1|$ means the number of new neighbors during $\varDelta T$(s), and $|\mathbb{N}_1 - \mathbb{N}_0|$ means the number of neighbors that moved away, a is calculated as Eq. (10).

$$a = \frac{|\mathbb{N}_0 - \mathbb{N}_1|}{ALL\_NODES} + \frac{|\mathbb{N}_1 - \mathbb{N}_0|}{ALL\_NODES} \qquad (10)$$

where a is normalized by ALL_NODES, the number of all nodes in the simulation.

5.4 Results

Figure 6 shows that the number of learning data sets determined dynamically when updating a learning data set. From Fig. 6, we can see that the numbers of data set change according to the change in the network environment.

Figure 7 show the projection distance of the first principal element of a node in the conventional scheme (part a) and in the method using only the recent data set (part b) and proposed method (part c). From these figures we can see that as a general trend, the value of the projection distance increases during the time period of 2500(s) to 5000(s), when the attacks were executed. Especially, in the proposed method the value of the projection distance increases rapidly at 2500(s) and then decreases sharply at 5000(s) as well. On the contrary, for the conventional method the large projection distance is falling at the time with no attacks. This shows the reason why the conventional method has lower detection rates and a large number of false positives. For the method using only the recent data set as the learning data shown in Fig. 7, comparing with the proposed method, the values of the projection distance are small and are scattered in a wide range.

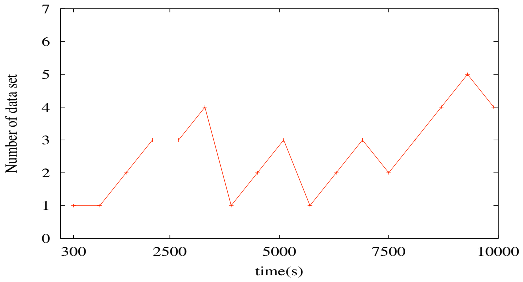


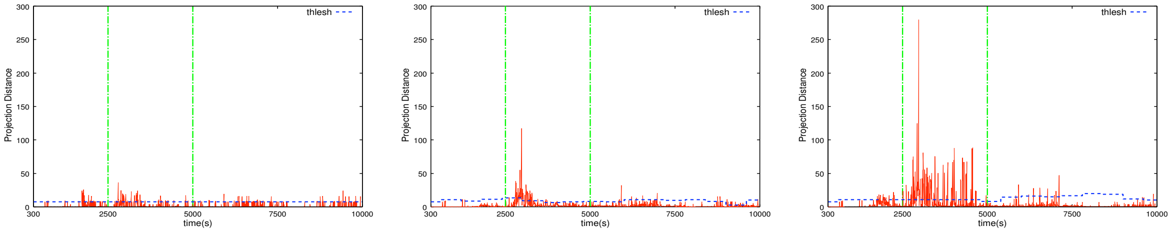
Figure 6. Number of data set in updating learning database

As an example, we can also see that compared to the conventional method with fixed threshold, the proposed method changes its threshold dynamically to fit well with the network traffic. Comparing the method using only the recent data set and proposed method cases, e.g., shown in Fig. 7, we can see that using the forgetting curve can achieve the moderate thresholds.

Table 2 shows the average Detection Rate (DR) and the False Positive Rate (FPR) for the conventional method, the method using only the recent data set and the proposed method. Based on the results shown in this table, we can see that the proposed method provides the highest average detection rate. Compared to the conventional method, the proposed method increases the average DR by more than 54%. Furthermore, the false average FPR is decreased by more than 1%.

6 CONCLUSIONS AND FUTURE WORKS

Vulnerability has been pointed out in MANET against various attacks. For enhancing the security ro-



(a) conventional method

(b) method using only the recent data set

(c) proposed method

Figure 7. Modification of RREP-1 (projection distance)

Table 2. Detection performance

	conventional method		method using only the recent data set		proposed method	
	DR	FPR	DR	FPR	DR	FPR
Modification of RREP(1)	36.65 %	7.93 %	65.51 %	5.27 %	93.54 %	8.73 %
Modification of RREP(2)	48.33 %	6.94 %	60.89 %	4.79 %	95.48 %	8.37 %
Modification of RREQ	55.65 %	16.19 %	77.09 %	9.48 %	97.27 %	13.59 %
Malicious Flooding(1)	40.36 %	9.88 %	80.23 %	4.32 %	99.16 %	6.97 %
Malicious Flooding(2)	32.01 %	9.99 %	83.80 %	3.89 %	100 %	5.38 %

bust learning methods against various attacks are expected. In this paper, we proposed a new detection method based on dynamically updating learning data. The proposed method can adapt easily to the changes within a MANET. Through simulations, the proposed method shows significant effectiveness in detecting various attacks. Compared to the conventional methods which use only static learning data sets, the average detection rate is increased by more than 54% and the average false negative rate is decreased by more than 1%. There results revealed high performance of the proposal method.

Future works will be focused on implementing the algorithm and verifying its effectiveness in a real network environment.

References

[1] M.G. Zapata, “Secure ad hoc on-demand distance vector (SAODV) routing,” IETF Internet Draft,draft-guerrero-manet-saodv-03, March 2005.

[2] H. Yih-Chun, A. Perrig, and D.B. Johnson, “Ariadne:a secure on-demand routing protocol for ad hoc networks,” the Eighth Annual International Conference on Mobile Computing and Networking(MobiCom 2002), pp. 12–23, Sept. 2002.

[3] A. Mishra, K. Nadkarni, and A. Patcha, “Intrusion detection in wireless ad hoc networks,” IEEE Wireless Communications, vol.11, no.1, pp. 48–60, Feb. 2004.

[4] Y. Sato, Y. Waizumi, and Y. Nemoto, “Improving accuracy of network-based anomaly detection using multiple detection modules,” IEICE Technical Report, vol.104, no.354, pp. 45–48, 2004.

[5] C.E. Perkins, E.M. Belding-Royer, and S.R. Das, “Ad hoc on-demand distance vector (AODV) routing,” RFC 3561, July 2003.

[6] UCB/LBNL/VINT: Network Simulator - ns (version 2). `http://www.isi.edu/nsnam/ns/`.

[7] D.B. Johnson, D.A. Maltz, and H. Yih-Chun, “The dynamic source routing protocol for mobile ad hoc networks (DSR),” IETF Internet Draft, draft-ietf-manet-dsr-10, July 2004.

[8] H. Yih-Chun, D.B. Johnson, and A. Perrig, “SEAD:secure efficient distance vector routing for mobile wireless ad hoc networks,” the 4th IEEE Workshop on Mobile Computing Systems & Applications, pp. 3–13, June 2002.

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

[10] H. Yih-Chun, 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.

[11] L. Zhou, and Z.J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol.13, no.6, pp. 24–30, 1999.

[12] M. Bechler, H. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A cluster-based security architecture for ad hoc networks," INFOCOM 2004, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, vol.4, pp. 2393–2403, March 2004.

[13] M. Ramkumar, and N. Memon, "An efficient key predistribution scheme for ad hoc network security," IEEE Journal on Selected Areas in Communications, vol.23, no.3, pp. 611–621, March 2005.

[14] O. Kachirski, and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks," the 36th Annual Hawaii International Conference on System Sciences (HICSS), pp. 57–64, Jan. 2003.

[15] G. Vigna, S. Gwalani, K. Srinivasan, E.M. Belding-Royer, and R.A. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," the 20th Annual Computer Security Applications Conference (ACSAC'04), pp. 16–27, Dec. 2004.

[16] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K.N. Levitt, "A specification-based intrusion detection system for AODV," the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03), pp. 125–134, Fairfax, USA, Oct. 2003.

[17] Y. an Huang, W. Fan, W. Lee, and P.S. Yu, "Cross-Feature Analysis for Detecting Adhoc Routing Anomalies," the 23rd International Conference on Distributed Computing Systems (ICDCS'03), pp. 478–487, May 2003.

[18] Y. an Huang, and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125–145, French Riviera, Sept. 2004.

[19] R.O. Duda, P.E. Hart, and D.G. Stork, Pattern Classification and Scene Analysis, John Wiley & Sons, 1973.

[20] H. Ebbinghaus, Memory : A contribution to experimental psychology, Teachers College Press, 1913.

[21] P. Ning, and K. Sun, "How to misuse aodv: A case study of insider attacks against mobile adhoc routing protocols," the 4th Annual IEEE Information Assurance Workshop, pp. 60–67, June 2003.

[22] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz, "On the effect of node misbehavior in ad hoc networks," the IEEE International Conference on Communications 2004, vol.6, pp. 3759–3763, June 2004.

[23] W. Wang, Y. Lu, and B.K. Bhargava, "On vulnerability and protection of ad hoc on-demand distance vector protocol," the 10th International Conference on Telecommunications 2003 (ICT2003), vol.1, pp. 375–382, French Polynesia, Feb. 2003.

[24] C.E. Perkins, E.M. Royer, S.R. Das, and M.K. Marina, "Performance comparison of two ondemand routing protocols for ad hoc networks," IEEE Personal Communications Magazine special issue on Ad hoc Networking, pp. 16–28, Feb. 2001.

[25] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," IEEE Transaction on Mobile Computing, vol.2, no.3, pp. 257–269, July/Sept. 2003.

[26] J. Tsumochi, K. Masayama, H. Uehara, and M. Yokoyama, "Impact of mobility metric on routing protocols for mobile ad hoe networks," Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on, vol.1, pp. 322–325, Aug. 2003.