# A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks

Hidehisa Nakayama, *Member, IEEE*, Satoshi Kurosawa, Abbas Jamalipour, *Fellow, IEEE*, Yoshiaki Nemoto, *Senior Member, IEEE*, and Nei Kato, *Senior Member, IEEE*

***Abstract*—Mobile ad hoc networks (MANETs) are usually formed without any major infrastructure. As a result, they are relatively vulnerable to malicious network attacks, and therefore, security is a more significant issue than infrastructure-based wireless networks. In MANETs, it is difficult to identify malicious hosts as the topology of the network dynamically changes. A malicious host can easily interrupt a route for which it is one of the forming nodes in the communication path. In the literature, there are several proposals to detect such malicious hosts inside the network. In those methods, a baseline profile, which is defined as per static training data, is usually used to verify the identity and the topology of the network, thus preventing any malicious host from joining the network. Since the topology of a MANET dynamically changes, the mere use of a static baseline profile is not efficient. In this paper, we propose a new anomaly-detection scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals. Our dynamic learning process involves calculating the projection distances based on multidimensional statistics using weighted coefficients and a forgetting curve. We use the network simulator 2 (ns-2) system to conduct the MANET simulations and consider scenarios for detecting five types of attacks. The simulation results involving two different networks in size show the effectiveness of the proposed techniques.**

***Index Terms*—Ad hoc on-demand distance vector (AODV), anomaly detection, dynamic learning, forgetting curve, malicious attacks, mobile ad hoc networks (MANETs), projection distance.**

## I. Introduction

INCREASINGLY, mobile ad hoc networks (MANETs) are receiving more attention as part of the next-generation network technologies. These networks are usually constructed by using mobile and wireless hosts with minimum or no central control point of attachment, such as a base station. These networks can be useful in a variety of applications, such as one-off meeting networks, disaster and military applications, and the entertainment industry. Because the network topology of MANETs frequently changes, and there is no central management entity, all of the routing operations must be performed by the individual nodes in a collaborative fashion. Consequently, it is unrealistic to introduce an authentication server that can employ conventional cryptographic schemes to secure the network against attacks from malicious hosts. The typical types of attacks in MANETs include eavesdropping, address spoofing, forged packets, denial of service (DoS), etc. [1].

Secure routing protocols [2]–[4] in which key-based cryptographic technologies [5], [6] are applied have been suggested to meet the increasing demands for MANET security. However, besides the topology issue, these methods cannot protect the network from attacks by a malicious node that has managed to acquire the network key. Therefore, other security methods that can detect attacks from malicious hosts are required. If a well-known attack in the TCP/IP protocol stack is launched in a MANET, then it is possible to protect the network by using conventional security techniques [7]. However, if the attacker maliciously uses the specific routing protocol of the MANET, prevention becomes remarkably difficult [8]. In such a case, it is almost impossible to recognize where and when the malicious node appears. Thus, the attack detection at each node becomes necessary [9].

The techniques for detecting the malicious attacks are usually classified into two categories, namely, misuse detection and anomaly detection. In misuse detection, the method of using a signature-based analysis is widely implemented. In this method, the attacks are identified by comparing the input traffic signature with the signatures extracted from the known attacks at the network routers. An anomaly detection is a technique that quantitatively defines the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. It is rather easy to detect an attack, the traffic signature of which is identifiable by using misuse detection. However, for those attacks, the type or traffic signatures of which are hard to identify by misuse detection, the method is rather inadequate. In such cases, those attacks can only be detected by using anomaly detection methods. In anomaly detection, even when the traffic signature is unknown, if the baseline profile of a network is delineated *a priori*, then the abnormality can be recognized. In [10], the effectiveness of such a detection method in wired networks has been demonstrated. In this method, the baseline profile is preextracted and then applied to the same network. However, for MANETs, since the network conditions are likely to change, the preextracted

Manuscript received April 16, 2008; revised August 30, 2008. First published November 25, 2008; current version published May 11, 2009. The review of this paper was coordinated by Prof. X. (S). Shen.

H. Nakayama was with the Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan. He is now with the Department of Electronics and Intelligent Systems, Tohoku Institute of Technology, Sendai 982-8577, Japan (e-mail: hidehisa@m.ieice.org).

S. Kurosawa was with the Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan. He is now with the Information Technology R&D Center, Mitsubishi Electric Corporation, Kamakura 247-8501, Japan (e-mail: Kurosawa.Satoshi@cw.MitsubishiElectric.co.jp).

A. Jamalipour is with the School of Electrical Information Engineering, University of Sydney, Sydney NSW 2006, Australia (e-mail: a.jamalipour@ieee.org).

Y. Nemoto and N. Kato are with the Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan (e-mail: nemoto@nemoto.ecei.tohoku.ac.jp; kato@it.ecei.tohoku.ac.jp).

Digital Object Identifier 10.1109/TVT.2008.2010049

network state may not correctly represent the state of the current network. This problem indeed influences the accuracy of the anomaly detection method.

Due to the fact that the MANET environment dynamically keeps evolving, envisioning a robust anomaly detection method becomes imperative to thwart the malicious attacks against it. In this paper, we propose a new anomaly detection scheme based on a dynamic learning method. The MANET hosts are mobile on their own so that the MANET environment is dynamically changing. Our dynamic learning method is based on a statistical decision theory that calculates the multidimensional projection distance between the current and normal states of the targeted host. We propose to use weighted coefficients with a forgetting curve as its mathematical property has been proved [11], [12] to suit our requirements. We conduct network simulations with five types of attacks in [13]–[15] as a case study that concerns one of the most popular MANET routing protocols, i.e., the ad hoc on-demand distance vector (AODV) [16]. The simulation results of the network simulator 2 (ns-2) [17] demonstrate the effectiveness of the proposed technique, regardless of the number of nodes in the considered MANET.

The remainder of this paper is organized as follows. In Section II, we present the problems of conventional detection schemes in attacks against MANETs. In Section III, we present an overview of AODV. Section IV describes the proposed detection scheme and the derivation of the essential parameters. In Section V, the simulation results concerning the performance of the proposed scheme are provided. Section VI presents the conclusions and future research scopes.

## II. Related Works

### A. Secure Schemes for Routing Procedures

Secure ad hoc routing protocols have been proposed as a technique to enhance the security in MANETs. For example, the secure AODV (SAODV) [18], which uses signed routing messages, is proposed to add security to AODV [16]. A-SAODV [19], [20] is a mild implementation of SAODV that uses the RSA [21] as an asymmetric cryptographic algorithm and the SHA1 [22] as a hash algorithm. The survey conducted by Yih-Chun and Perrig [23] overviewed the various secure routing protocols and pointed out their drawbacks and advantages. They also proposed a secure on-demand ad hoc network routing protocol (Ariadne) [24], which prevents the compromised nodes from tampering with the uncompromised routes, and the secure efficient ad hoc distance (SEAD) [25], which is a secure routing protocol, using efficient one-way hashing functions and not using asymmetric cryptographic operations. In addition, Zhou and Haas proposed a distributed certification authority mechanism in which the authentication uses threshold cryptography [2]. In [26], a MANET is divided into clusters, and a certification authority is appointed to each cluster. In [27], a method called key predistribution (KPD) scheme is applied. In [28], the authenticated routing for ad hoc networks (ARAN) is proposed by using public-key cryptographic mechanisms based on the AODV. These methods can only guard against external attacks. However, the internal attacks mounted by the malicious or compromised hosts may still have a severe impact on the network performance, as well as on the connectivity among the nodes in the targeted MANET.

Deng *et al.* [29] proposed an approach that requires the intermediate nodes to send a route reply (RREP) packet with the next hop information. When a source node receives the RREP packet from an intermediate node, it sends a "Further Request" packet to the next hop to verify that it has a route to the intermediate node and a route to the destination. As a response to this request, the intermediate node will send another RREP packet. When the next hop receives a "Further Request" packet, it sends a "Further Reply" packet that includes the verified result to the source node. Based on the information in the "Further Reply" packet, the source node judges the validity of the route. Again, the method in [30] requires the intermediate node to send the route confirmation request (CREQ) to the next hop node toward the destination, and then, the next hop node receives the CREQ and looks into its cache for a route to the destination. If it has such a route to the destination, then it sends a route confirmation reply (CREP) message to the 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 routing protocol has to be modified. These modifications may increase the routing overheads, which results in the performance degradation of the bandwidth-limited MANETs.

### B. Network Monitoring-Based Attack Detection

In addition to the aforementioned techniques, an attack detection by network monitoring, which can detect attacks from inside MANETs, has also been proposed. For instance, Kachirski and Guha [31] proposed a method that detects attacks by employing distributed mobile agents. Network monitoring nodes are selected to be able to collect all the packets within a cluster, and the decision agents in the nodes are used to detect and classify the security violations. The concern of this method is that the monitoring nodes will consume a large amount of energy. Vigna *et al.* [32] detect attacks by placing AODV-based State Transition Analysis Technique (AODVSTAT) sensors within the network and by either observing solely contiguous nodes or trading information with other sensors. However, it is necessary to deploy a large number of AODVSTAT sensors on the nodes for detecting a varied range of attacks. In addition, a large number of UPDATE messages may cause an overwhelming congestion in the network. Tseng *et al.* [33] introduced a method that places a network monitor (NM) inside the network. In this method, the NM constantly monitors the packet flow in the network within a certain range to detect any attacks. However, placing effective detectors, i.e., mobile agents, sensors, or NMs, is considered to be difficult when the MANET topology dynamically changes. One solution to this problem is to observe the packet flow on each node and to detect any potential attack.

### C. Anomaly Detection

Huang *et al.* [34] proposed a method in which the packet flow is observed at each node. In this method, 141 features that

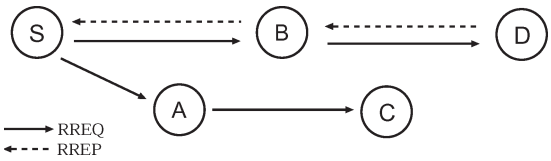


Fig. 1. Route-discovery process on AODV.

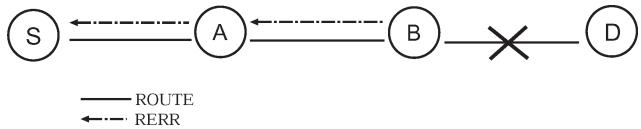


Fig. 2. Transferring RERR messages on AODV.

are both traffic and topology related are defined. Huang *et al.* suggested an anomaly detection mechanism with interrelation between features. Moreover, in [35], they constructed an extended finite-state automaton (EFSA) according to the specification of the AODV routing protocol, envisioned normal condition modeling, and detected attacks with both specification-based and anomaly-based detection schemes. In specification-based detection, the attacks were detected as deviant packets from the conditions defined by EFSA. In addition, in anomaly detection, the normal conditions are defined as the baseline with which the condition of EFSA and also the amounts of transition statistics are compared. The deviations from those conditions are then used to detect the potential attacks. For determining the baseline profiles, in both methods, the training data are extracted beforehand from the same network environment where the test data are applied. However, we note that the MANET topology can rather easily be changed, and the differences in network states grow larger with time. Furthermore, these methods cannot be applied to a network where the learning phase has been conducted in another network.

Sun *et al.* [36] proposed an anomaly detection method in which mobility is considered. This method computes the recent link change rate $(LCR_{\mathrm{recent}})$ and can select the training data, the link change rates of which have the smallest Euclidean distance to $LCR_{\mathrm{recent}}$. However, the change of network states can be caused not only by mobility; it may also occur due to the sudden participation and disappearance of nodes in a MANET. When the nodes in the current MANET differ from those in the training data, the defined baseline profile cannot express the current network state. As a result, these methods are rendered inadequate and considered difficult in a MANET environment.

To solve this problem, a normal state needs to be defined by 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 doing so, the attack detection can adaptively be conducted even in a changing network scenario.

## III. Attacks on AODV Protocol

### A. Overview of AODV Protocol

The AODV [16] is a reactive routing protocol in which the network generates routes at the start of communication. Each node has its own sequence number, and this number increases whenever a link changes. According to its sequence number, each node judges whether the channel information is recent. Fig. 1 illustrates the route-discovery process of the AODV. In this figure, node $S$ attempts to establish a connection to destination $D$. First, the source node $S$ refers to the route map at the start of communication. In the case where there is no route to destination node $D$, it sends a route request (RREQ) message by using broadcasting. The RREQ ID increases by one every time node $S$ sends an RREQ message. Nodes $A$ and $B$, which have received the RREQ message, generate and renew the route to its previous hop. They also evaluate if this is a repeated RREQ message and accordingly discard it. If $A$ and $B$ have a valid route to the destination $D$, then they send an RREP message to node $S$. In the case where the node has no valid route, they send an RREQ message using broadcasting. The exchange of route information will be repeated until an RREQ message reaches node $D$. When node $D$ receives the RREQ, it sends an RREP message to node $S$. When node $S$ receives the RREP message, a route is established. In case of multiple RREPs received, a node selects an RREP message, the Destination Sequence number (Dst_Seq) of which is the largest among all the previously received RREPs. However, if the Dst_Seqs were the same, then it will select the RREP message whose hop count is the smallest.

In Fig. 2, when node $B$ detects a disconnection of route, it generates route error (RERR) messages and puts the invalidated address of node $D$ into its list and then sends RERR to node $A$. When node $A$ receives the RERR message, it refers to its route map and the current list of RERR messages. If there was a route to the 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 an RERR message to node $S$. This way, the RERR message can finally be sent to the source node $S$.

### B. Classification of Attacks

According to the aforementioned features, the malicious nodes can misuse the AODV by forging source IP addresses, destination IP addresses, RREQ IDs, hop counts, Destination Sequence numbers (Dst_Seqs), Source Sequence numbers (Src_Seqs), and also by flooding the network with routing packets. According to prior works (e.g., [13]–[15]), we can classify the attacks against AODV into *routing disruption attacks* and *resource consumption attacks*.

1) *Routing Disruption Attacks:* These attacks interrupt the establishment of a route or destroy an existing route. The most common attacks of this type are the modification of RREP (same as the Blackhole Attack) and the modification of RREQ.
2) *Resource Consumption Attack:* This attack wastes resources of a specific node and the network as a whole. The most common attack of this type is malicious flooding.

A short explanation of the preceding three attacks is given here.

1) Modification of RREP: The Dst_Seq represents the freshness of routing information in the network. When a source node receives multiple RREP messages, it selects the node that has the largest Dst_Seq value and accordingly constructs a route. Therefore, a malicious node may

intentionally attempt to modify the RREP packet and increase the Dst_Seq value of the RREP message. As a result, a false route will be established, and the legitimate data traffic will be interrupted. In addition, the victim nodes will further spread the false routing information to others, and thus, the damage will propagate throughout the network. In this case, we can consider two types of forged packets. In the first type, the source and destination IP addresses are spoofed or forged to the destination node. In the second type, the destination IP address is forged to the destination node, and the source IP address is spoofed to a randomly selected node. We call the "Modification of RREP (1)" as an attack that uses the first packet type and the "Modification of RREP (2)" as an attack that uses the second packet type.

2) Modification of RREQ: The RREQ ID represents the freshness of an RREQ message in the network. Based on the RREQ ID, each node decides whether to forward an RREQ message. Therefore, a malicious node attempts to intentionally increase the RREQ ID when an RREQ packet is received. Additionally, when a forged packet with a false source address in the IP header is sent, the route will never be established.
3) Malicious Flooding: Generally, the RREQ messages are broadcasted to select new routes. If a malicious node sends an excess number of RREQ messages, then the network will become congested with a huge amount of RREQ traffic. In our preliminary experimental results, when a malicious node sends more than 20 RREQ packets per second, the congestion occurs, which leads to significant unnecessary delays and packet drops. In this case, we can consider two forged packet types. In the first type, the source IP address is forged to a randomly selected node. In the second type, the source IP address is forged to a destination node, and the RREQ ID is intentionally increased at the same time. We define the "Malicious Flooding (1)" as an attack that uses the first packet type and the "Malicious Flooding (2)" as an attack that uses the second packet type.

See [13]–[15] for detailed information on these attacks.

## IV. Dynamic Anomaly Detection

In this section, we first introduce the *features* that are essential for our envisioned anomaly detection scheme, and then delineate the module of the detection scheme based on the *projection distances*.

### A. Definition of Features

Each node observes its own traffic and uses a time slot to record the number of packets (messages) according to their types (see Fig. 3). In time slot $\Delta\tau$, the instantaneous value of the network state is expressed by a $p$-dimension vector $\boldsymbol{x} = [x_1, x_2, \ldots, x_p]^T$, where each feature $x_k$ $(k = 1, \ldots, p)$ is measured. In this paper, we define nine features related to path finding, four features related to path abnormality, and one feature related to a major characteristic of AODV. Therefore,

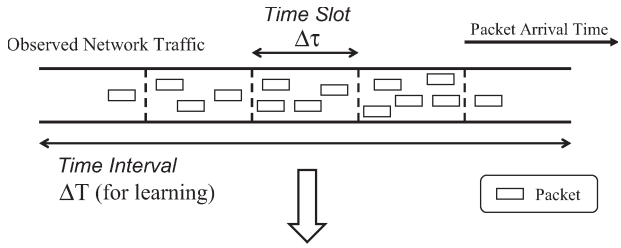


Fig. 3. Feature definition. The traffic features in a time slot are expressed by the elements of the $p$-dimensional vector $\boldsymbol{x}$.

we obtain $p = 14$. According to [10], [34], and [35], a small value for the time slot is preferred, and therefore, $\Delta\tau$ is set to a constant small value of 5 s.

Furthermore, in the learning process shown in Fig. 3, a time interval $\Delta T$ is defined. It contains several time slots. In other words, the number of time slots is equal to the number of all training samples at a given time interval. Note that if we use a shorter time interval $\Delta T$, the data sets contained in one time interval will decrease. On the other hand, a larger value of $\Delta T$ slows down the learning process.

The statistics for a time interval define a state in the network, and a further explanation about the statistics is described in Section IV-B.

*1) Path Finding Features (Nine Dimensions):* The path finding features comprise the following:

1) number of received RREQ messages (three types);
2) number of forwarded RREQ messages;
3) number of outbound RREQ messages;
4) number of outbound RREP messages (two types);
5) 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 addresses, messages with their own destination IP addresses, and messages with neither source nor destination IP addresses of their own. When counting the number of received RREP messages, the packets with a matching destination IP address, source IP address, RREQ ID, or Src_Seq in the training data are recorded once for each time slot. Similarly, the number of outbound RREP messages includes two types, for which the destination node is itself, and for which it holds the path toward the destination node. The number of received RREP messages includes two types: the first type is a packet, both source and destination addresses of which exist in the training data. All of the other packets are classified as the second type (with either one or no matching features). As an example, when a node is under attack by the "Malicious flooding," it receives a tremendous amount of RREQ messages, and therefore, the number of received RREQ messages increases. This indicates the presence of anomaly in the network.

*2) Path Abnormality Features (Four Dimensions):* The path abnormality features comprise the following:

1) number of received RERR messages;
2) number of outbound RERR messages;
3) number of dropped RREQ messages;
4) number of dropped RREP messages.

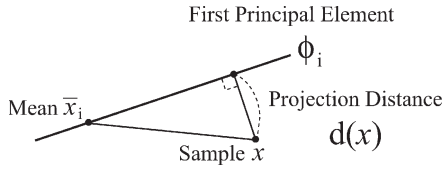


Fig. 4. Distance of sample $x$ to the first principal element $\phi_i$. $d(\boldsymbol{x})$ is the projection distance.

When counting the number of received RREQ messages, the packets with the same destination IP address and Dst_Seq are recorded only once for each time slot. As an example, when a node is under attack of the "Modification of RREQ" messages caused by packets with a forged source address in the IP header, a large number of RREP messages will not successfully be able to be sent out. As a result, the number of dropped RREP messages will increase, and this acts as a sign of abnormality in the network.

*3) AODV Characteristic Feature (One Dimension):* The AODV characteristic feature comprise the average of the differences 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 an RREQ message, each node keeps the destination IP address and the Dst_Seq in its list. When an RREP message is received, the node looks over the list to see if there is the 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 the ad hoc networks, sometimes the 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. In a normal state, the Dst_Seq increases in a relatively stable pace. On the contrary, when a node is receiving "Modification of RREP" attacks, this value drastically changes, and thus, we may recognize this particular abnormality.

### *B. Detection Module by Projection Distance*

In pattern recognition, based on statistical decision theory, the distance measure is an effective way to formulate the different types of categories because the same category is distributed in the close area in a multidimensional feature space [37]. Here, the normal and attack states as two different categories can be considered. In this section, we describe the detection module by using the projection distance (see Fig. 4).

Let us consider a training data set $\boldsymbol{D}_i = \{\boldsymbol{x}\}$ collected by each node $i$ $(i = 1, \ldots, N)$, where $N$ is the number of all nodes participating in MANET, and the current time interval consists of $D_i$ time slots $(D_i = |\boldsymbol{D}_i|$, in case of using all training samples). First, we calculate the mean vector and the covariance matrix at node $i$ as

$$\bar{\boldsymbol{x}}_i = \frac{1}{D_i} \sum_{\boldsymbol{x} \in \boldsymbol{D}_i} \boldsymbol{x}. \tag{1}$$

$$\boldsymbol{\Sigma}_i = \frac{1}{D_i} \sum_{\boldsymbol{x} \in \boldsymbol{D}_i} (\boldsymbol{x} - \bar{\boldsymbol{x}}_i)(\boldsymbol{x} - \bar{\boldsymbol{x}}_i)^T. \tag{2}$$

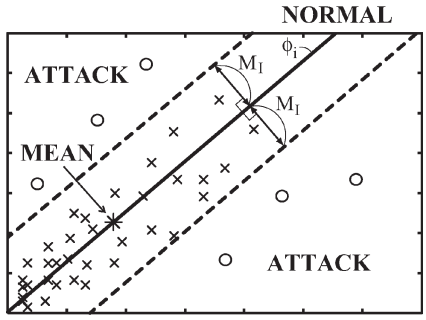


Fig. 5. Example of the division by using the projection distance.

From (1) and (2), we use the principal component analysis (PCA) [37] to analyze the statistical nature of the current time interval. The PCA is the method that explores the correlations between each feature and finds the most important axis to express the scattering of data. Here, the most important axis denotes the baseline profile of network activity. When an attack takes place, it generates the deviation sample from this axis. By using PCA, the first principal element $\boldsymbol{\phi}_i$, which reflects the approximate distribution of the training data sets, is calculated. Here, we consider the projection distance of an input data sample $\boldsymbol{x}$ as

$$d(\boldsymbol{x}; \boldsymbol{D}_i) = \|\boldsymbol{x} - \bar{\boldsymbol{x}}_i\|^2 - \boldsymbol{\phi}_i^T (\boldsymbol{x} - \bar{\boldsymbol{x}}_i). \tag{3}$$

When the projection distance is larger than the threshold $M_I$, it is evaluated as

$$\begin{cases} d(\boldsymbol{x}; \boldsymbol{D}_i) > M_I & : \text{attack} \\ d(\boldsymbol{x}; \boldsymbol{D}_i) \leq M_I & : \text{normal.} \end{cases} \tag{4}$$

Here, when $M_i$ is the maximum value of projection distance for node $i$ in the training data sets $\boldsymbol{D}_i$, the suffix $I$ of $M_I$ is extracted from all the nodes $(N)$ as

$$I = \arg \max_{i=1,\ldots,N} M_i$$

where

$$M_i = \max_{\boldsymbol{x} \in \boldsymbol{D}_i} d(\boldsymbol{x}; \boldsymbol{D}_i). \tag{5}$$

Fig. 5 shows a rough image of determining the normal or attack states by using the projection distances in two dimensions.

### *C. Proposal of Dynamic Anomaly Detection*

Since the network topology easily changes in MANET, the current state may not appropriately be expressed over time. Therefore, by only using the method described in Section IV-B to define the normal state, it is rather insufficient to reflect the changing situation of MANET, and a learning method that can follow these changes is indispensable. We explain the idea of dynamically updating the training data sets in the remainder of this section.

Let $T_0$ be the current time interval, and let $T_1$ be the first time interval. By using the data collected in $T_1$, initially, the first principal element is calculated, and then the calculated first principal element is used in the following time interval $T_0$ for anomaly detection. If the state in $T_0$ is judged as normal, then

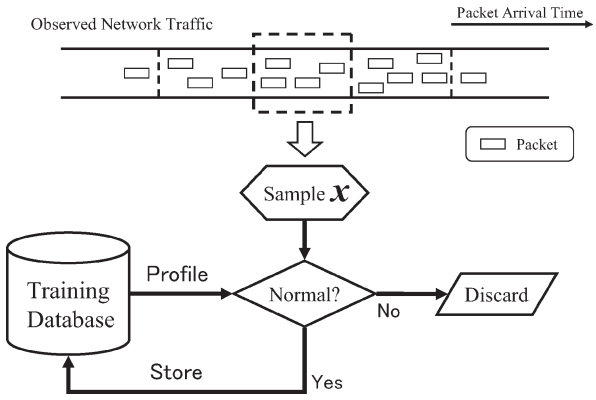


Fig. 6. Flow chart of the proposed method for learning and evaluation.

the corresponding data set will be used as the training data set. Otherwise, it will be treated as the data including attack, and it will consequently be discarded. This way, we keep on learning the normal states of the network. This procedure is shown in Fig. 6.

As mentioned earlier, when updating the database, it is possible to use the most recent data set. However, since the most recent data set is easily affected by the sudden change in the network, it is necessary to take the time series model into consideration to keep the database from being too sensitive to the changes in the network topology. Here, we use the forgetting curve [11], [12] as the weighting function to adjust the degree of importance of the time slot. The forgetting curve aims at reducing the weight when the data become old and of less significance.

Suppose using $m_i$ data sets as the training data. Fig. 7 shows how to weigh the data sets while learning. $\lambda_i(t)$, $t = 1, 2, \ldots, m_i$, are the forgetting coefficients that correspond to each training data set, respectively. As shown in Fig. 8, the forgetting curve is expressed as

$$\begin{aligned}\lambda_i(t) &= \lambda_i(0) e^{-a_i T_t} \\ &= \lambda_i(0) \cdot \exp(-a_i \Delta T \cdot t), \quad i = 1, \ldots, N \end{aligned} \tag{6}$$

where the current coefficient $\lambda_i(0)$ and the common time interval $\Delta T$ are constants. $\lambda_i(t)$ are constrained by

$$1 = \sum_{t=1}^{m_i} \lambda_i(t), \quad i = 1, \ldots, N. \tag{7}$$

Additionally, we describe the derivation algorithm of determining the parameters $m_i, a_i$ in Section IV-D. Using the number of data sets $m_i$ and the forgetting coefficients $\lambda_i(t)$, the statistics of the current state "0" can be calculated from (1) and (2) as

$$\begin{aligned}\bar{\boldsymbol{x}}_i(0) &= \sum_{t=1}^{m_i} \lambda_i(t) \bar{\boldsymbol{x}}_i(t) \\ &= \sum_{t=1}^{m_i} \frac{\lambda_i(t)}{D_i(t)} \sum_{\boldsymbol{x}(t) \in \boldsymbol{D}_i} \boldsymbol{x}(t) \end{aligned} \tag{8}$$

$$\begin{aligned}\boldsymbol{\Sigma}_i(0) &= \sum_{t=1}^{m_i} \lambda_i(t) \boldsymbol{\Sigma}_i(t) \\ &= \sum_{t=1}^{m_i} \frac{\lambda_i(t)}{D_i(t)} \sum_{\boldsymbol{x}(t) \in \boldsymbol{D}_i} (\boldsymbol{x}(t) - \bar{\boldsymbol{x}}_i(t)) (\boldsymbol{x}(t) - \bar{\boldsymbol{x}}_i(t))^T . \end{aligned} \tag{9}$$

Here, we consider all the training data sets

$$\boldsymbol{U}_i = \{\boldsymbol{D}_i(1) \cup \boldsymbol{D}_i(2) \cup \cdots \cup \boldsymbol{D}_i(m_i)\} . \tag{10}$$

By using PCA, the first principal element $\boldsymbol{\phi}_i(0)$ is calculated. As a general scheme, the distance $d(\boldsymbol{x}; \boldsymbol{U}_i)$ of the input data sample $\boldsymbol{x}$ can be computed from (3) and then evaluated as

$$\begin{cases} d(\boldsymbol{x}; \boldsymbol{U}_i) > M_I & : \text{attack} \\ d(\boldsymbol{x}; \boldsymbol{U}_i) \le M_I & : \text{normal.} \end{cases} \tag{11}$$

Here, when $M_i$ is a maximum value of the projection distance for node $i$ in all the training data sets $\boldsymbol{U}_i$, the suffix $I$ of $M_I$ is extracted from all the nodes $(N)$ as

$$I = \arg \max_{i=1,\ldots,N} M_i$$

where

$$M_i = \max_{\boldsymbol{x}(0) \in \boldsymbol{U}_i} d(\boldsymbol{x}(0); \boldsymbol{U}_i) . \tag{12}$$

### D. Derivation Algorithm of Parameters

According to [38], the mobility metric of the MANETs is expressed by using the number of neighbor nodes. Using the number of neighbors, the number of training data sets $m_i$ used in the learning process and the parameter $a_i$ in (6) can dynamically be determined. Assume that for a given node $i$, at time $t$, its neighbor set is $\boldsymbol{S}_i(t)$, $t = 0, 1, 2, \ldots, m_i, m_{i+1}$. If $\boldsymbol{S}_i(0) \cap \boldsymbol{S}_i(m_i + 1) = \emptyset$, then we can recognize that the network state has considerably changed, and then $m_i$ is determined as the number of training data sets. Next, we consider $a_i$ in (6). $a_i$ represents the change in the size of the considered network. The change in size of a network is expressed by the change in the number of its neighboring nodes. Assume that for a given node, at the first time interval $(t = 1)$, its neighbor set is $\boldsymbol{S}_i(1)$. $|\boldsymbol{S}_i(0) - \boldsymbol{S}_i(1)|$ is the number of new neighbors during $\Delta T$, and $|\boldsymbol{S}_i(1) - \boldsymbol{S}_i(0)|$ is the number of neighbors that moved away. Then, $a_i$ can be calculated as

$$a_i = \frac{|\boldsymbol{S}_i(0) - \boldsymbol{S}_i(1)|}{N} + \frac{|\boldsymbol{S}_i(1) - \boldsymbol{S}_i(0)|}{N}. \tag{13}$$

Here, $a_i$ is normalized by $N$ (the number of all nodes participating in MANET). Next, we give an example of the simulation data. Fig. 9 shows the changes of the number of training data sets $m_i$. We can see that $m_i$ dynamically varies as the time elapsed.

## V. Performance Evaluation

In this section, we describe the details to evaluate the proposed method.

### A. Simulation Environment

The experiments were carried out by using ns-2 (ver. 2.27) [17]. We assume that the simulation network being used is in a place where various events in a MANET can occur [39], [40]. In

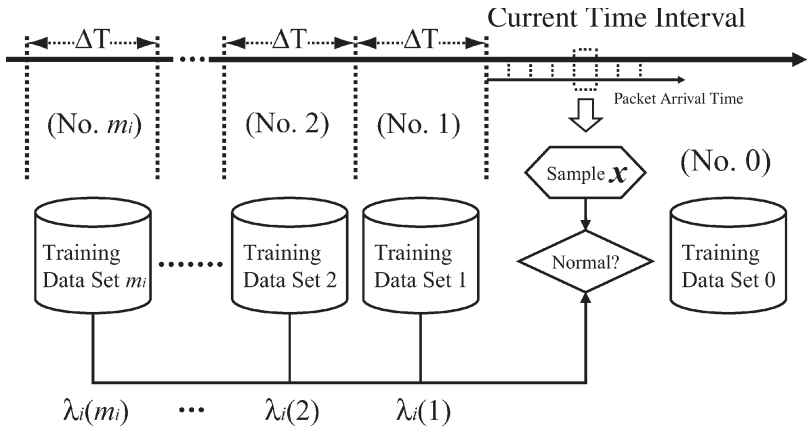


Fig. 7. Renewing training data using the forgetting coefficients.

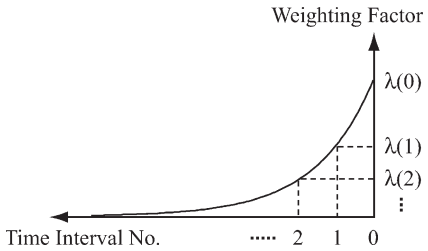


Fig. 8. Ebbinghaus' forgetting curve.

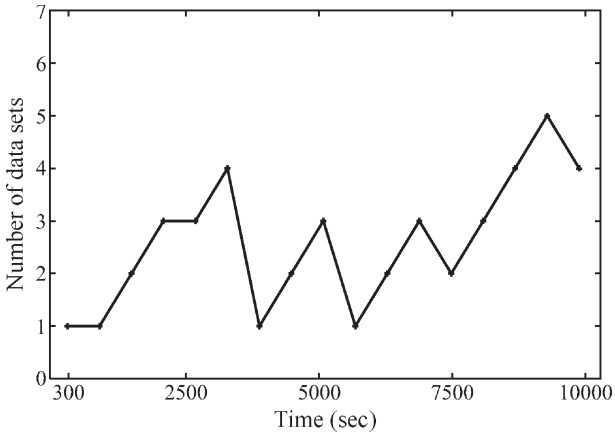


Fig. 9. Example of the number of training data sets, dynamically updated.

this simulation, the run time is 10 000 s, and five types of attacks were randomly executed from 2500 to 5000 s. All of the nodes, except the attack node, employed the proposed method to detect attacks. The simulations were performed for the following two scenarios: 1) a 50-node network with a network topology of 1000 m $\times$ 1000 m and 2) a 100-node network with a network topology of 2000 m $\times$ 2000 m. The traffic loads were constant bit rate flows with a data packet size of 512 B. In 1), the load was varied by using 40 flows (at four packets per second). In 2), the load was varied by using 80 flows (at four packets per second). The 802.11 Media Access Control (MAC) layer was used with a transmission range of 250 m, and it was set for a 2-Mb/s throughput. As for the moving pattern for each node, we use a random waypoint (RWP) model [41] in which each node randomly selects the destinations in the designated simulation area with random speeds. Here, the node velocity was set

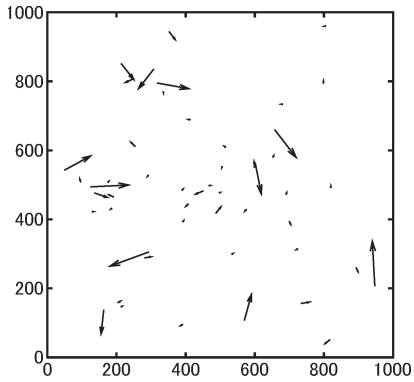


Fig. 10. Mobility pattern for RWP in 5 s.

between 0 and 5 m/s. The pause time was set to 10, 50, 100, 200, and 500 s, respectively. For example, Fig. 10 shows the moving pattern within 5 s.

To start the learning process, the first normal state, which excludes the attack data, was manually preextracted from the training data. This is because our proposed method detects the possibility of attacks according to the degree of which a state deviates from the normal state. Here, the first time interval is set to 300 s. This is a period in which enough normal state samples can be collected. We also deemed that it necessary to shorten the updating interval as the mobility rates increase. However, the shorter the updating interval, the more processing overhead is required. Therefore, more battery power will be consumed. From these facts, it is necessary to take into account the MANET environment and the available battery power to determine the time interval of updating. In our results, the time interval of updating $\Delta T$ was set to 600 s.

### *B. Simulation Results*

To evaluate our proposed methods, we assume the following three ways of using the training data sets:

1) M-1: method of using only the initial training data set;
2) M-2: method of using the most recent training data set at every time interval;
3) M-3: method of using the training data sets dynamically decided at every time interval.

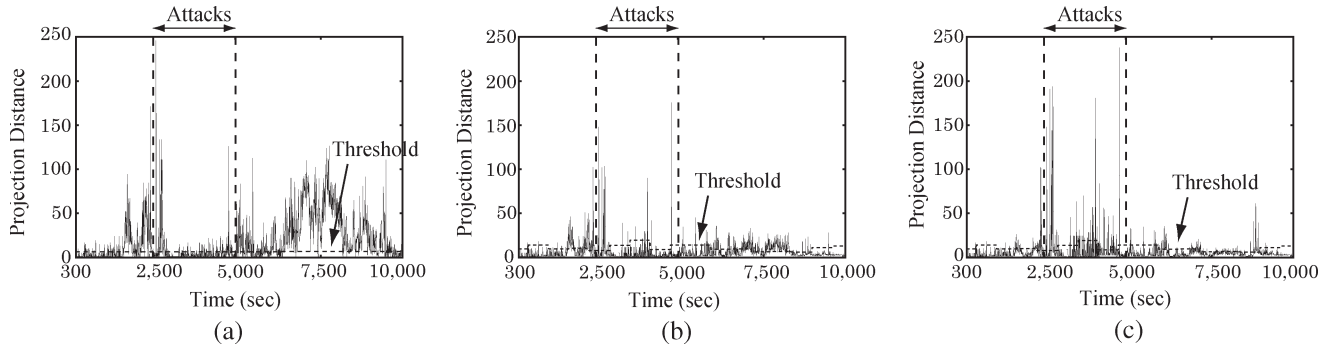


Fig. 11. Detection module by projection distance against modification of RREP(1), $N = 50$. (a) M-1 (conventional method). (b) M-2 (reference method). (c) M-3 (proposed method).

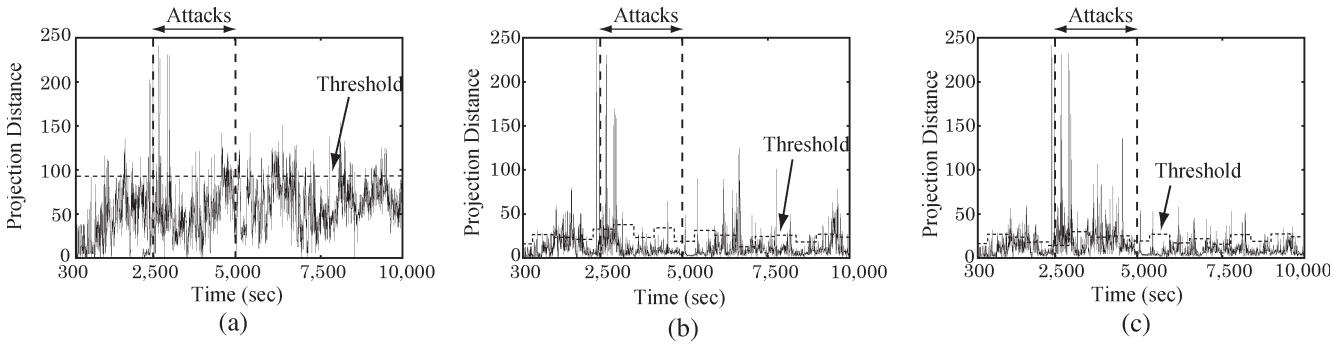


Fig. 12. Detection module by projection distance against modification of RREP(1), $N = 100$. (a) M-1 (conventional method). (b) M-2 (reference method). (c) M-3 (proposed method).

"M-1" is the conventional method, and "M-3" is our proposed method. For reference, we also show the result of "M-2," which is the simplest case of our proposed method.

Figs. 11 and 12 show the projection distances of the first principal element of a node in the conventional scheme "M-1," in the reference method "M-2," and in the proposed method "M-3." From these figures, we can see that, as a general trend, the value of the projection distance increases during the time period of 2500–5000 s, when the attacks were executed. In particular, in the proposed method "M-3," the value of the projection distance rapidly increases at 2500 s and then sharply decreases at 5000 s as well. On the contrary, for the conventional method "M-1," the large projection distances can be found through the whole period, and they do not descend at the time when attacks stop. This is the reason behind the lower detection rates (DRs) and a large number of false positives of the conventional method "M-1." For the method "M-2," comparing with "M-3", the values of the projection distance are relatively small and are scattered in a wide range; the result is better than "M-1" and worse in contrast with "M-3."

As evident from Fig. 11, where the value of $N$ is 50 during the attack period, "M-3" yields a higher projection distance and can detect the current anomaly compared to the other methods. During the normal period, it should be noted that there are many points that exceed the threshold in "M-1" and "M-2." On the other hand, there is a significant peak at around 9000 s, and this peak largely exceeds the threshold in "M-3." Despite being a normal period when there is no attack, because of the rapid changes of network topology, this point is incorrectly evaluated and produces a false positive. As a whole, we can see that, in the proposed method, there are fewer parts where the projection distances exceed the threshold than those in the other methods. This implies that we can obtain a lower number of false detections in the proposed method. Next, from Fig. 12, where $N = 100$, similar to the case of $N = 50$, during the attack period, we can see that the proposed method can detect the anomaly. However, different from the case of $N = 50$, in case of "M-1," the projection distances increase.

This is because, in case of $N = 100$, there are significant changes in the network environment. This causes the predefined baseline profile and the present network state to dramatically differ. Therefore, compared with the case of $N = 50$ during the normal period, we can see that "M-1" produces more false detections. Meanwhile, compared with the case of $N = 50$ in "M-3," we can see that although there is a number of parts that exceed the threshold, it generates less false detection than the other methods. From these facts, we can see that "M-1" cannot adapt with the changing environment. "M-1" does not reflect the whole network state since it only represents the temporary state of the network. For "M-2," by updating the training data set, it can adapt to the changing environment to some extent. Note that, in "M-3," the false detection in the case of $N = 100$ is higher than that of $N = 50$. This is caused by the increase in the RERR packets when the link is disconnected due to the network mobility and size, in addition to the sudden increase of the RREQ packets when a large number of route

TABLE I
PERFORMANCE OF DETECTION MODULE BY PROJECTION DISTANCE: $N = 50$

| | "M-1" | | "M-2" | | "M-3" | |
|---|---|---|---|---|---|---|
| | DR | FPR | DR | FPR | DR | FPR |
| Modification of RREP(1) | 54.79% | 24.90% | 61.62% | 10.40% | 92.88% | 9.47% |
| Modification of RREP(2) | 48.33% | 21.91% | 75.70% | 11.74% | 91.50% | 9.23% |
| Modification of RREQ | 67.19% | 27.06% | 77.09% | 7.77% | 83.39% | 7.52% |
| Malicious Flooding(1) | 51.24% | 18.54% | 76.23% | 12.12% | 95.96% | 9.47% |
| Malicious Flooding(2) | 56.45% | 18.57% | 81.87% | 12.24% | 95.76% | 10.26% |
| *Average* | 55.60% | 22.20% | 74.50% | 10.85% | 91.90% | 9.19% |

TABLE II
PERFORMANCE OF DETECTION MODULE BY PROJECTION DISTANCE: $N = 100$

| | "M-1" | | "M-2" | | "M-3" | |
|---|---|---|---|---|---|---|
| | DR | FPR | DR | FPR | DR | FPR |
| Modification of RREP(1) | 49.75% | 32.57% | 70.76% | 18.48% | 91.77% | 18.89% |
| Modification of RREP(2) | 48.94% | 34.50% | 68.47% | 19.92% | 91.79% | 20.09% |
| Modification of RREQ | 57.81% | 29.14% | 61.66% | 17.08% | 75.74% | 15.95% |
| Malicious Flooding(1) | 53.35% | 36.53% | 71.77% | 18.27% | 84.16% | 17.75% |
| Malicious Flooding(2) | 51.65% | 35.27% | 65.94% | 15.57% | 83.57% | 16.30% |
| *Average* | 52.30% | 33.60% | 67.72% | 17.86% | 85.41% | 17.80% |

requests occur at the same time. These trends become more apparent as the scale of the network becomes larger. Same reasons can be found for the increase of the false positives. Increasing the dimensionality may be effective to reduce these false detections.

In greater detail, Tables I and II display the average of the DR and the false positive rate (FPR) about the projection distance, respectively. Based on the results shown in these two tables, we can see that the proposed method "M-3" provides the highest average DR and the lowest FPR. Compared to the conventional method "M-1," the proposed method "M-3" increases the average DR by more than 25%. In addition, the average FPR is decreased by more than 10% in "M-1." Furthermore, as an effectiveness of dynamic learning, "M-3" increases the average DR by more than 15% compared to "M-2" in our simulation. On the other hand, the FPR of "M-3" is only marginally better than that of "M-2." This is because we approximately fixed the FPR in the range of 10%–20% for clearly understanding the difference of the DR between "M-2" and "M-3."

Now, we evaluate the computational complexities of these three methods. The computational complexity of "M-1" using the initial data is the lowest, and its order is $O(1)$. "M-2" and "M-3" compute the principal elements using PCA, which needs to compute the mean and the covariance. The order is $O(p^2)$ for computing both the mean and covariance, where $p$ is the number of features described in Section IV-A. The order of finding the first principal element depends on the technique of finding the first eigenvalue end eigenvector. For example, the complexity of the power method [42] is $O(k \times p^2)$ for finding the first $k$ eigenvalues and eigenvectors. The "M-2" is $O(p^2)$, where $k = 1$. Because "M-3" has $m_i$ times more learning processes than those of "M-2," the complexity of "M-3" is $O(m_i \times p^2)$ in total. Apparently, there is a tradeoff between the computational complexity and the accuracy of the DRs. We actually tested the computation time of our proposed method by considering $p = 14$. Using a Linux-based computer (Pentium 4, 2.4 GHz), this computation time of "M-3" is below 10 ms. Considering the importance of network security and the increasing power of ad hoc nodes, we believe that our proposed method can be a possible choice for performing anomaly detection in MANETs.

## VI. CONCLUSION

In this paper, a new dynamic anomaly detection system for MANETs has been proposed. For enhancing the security in MANETs, which are vulnerable to attacks, robust learning methods against these attacks are required. To differentiate an attack state from the normal state, we have defined multidimensional features based on the characteristics of these attacks and utilized the projection distance using PCA based on statistical theory. Our proposed system demonstrates an effective performance in terms of high DRs and low FPRs against five simulated attacks, in addition to the scalability of the proposed scheme clarified by the simulation results obtained from two distinct network topologies of varying sizes.

Future works will be focused on the various routing protocols in the MANET architecture. Although AODV is a major routing protocol in MANETs, new protocols are emerging, e.g., dynamic MANET on-demand protocol (DYMO) [43]. We will evaluate these protocols and give an analysis for the additional types of attacks to further improve the accuracy of the overall system. Moreover, in [44] and [45], Yan *et al.* reported an interesting scheme with the context of studies on the intrusion detection system (IDS). The proposed IDS autonomic event analysis system that is represented by description logics allows inferring the attack scenarios and enabling the attack knowledge semantic queries. To cite a case, first, using our proposed system to detect attacks and then rigorously applying this IDS to analyze these attacks may bring about a reliable approach. Our future works will comprise of feasibility studies on these more intelligent detection schemes in MANETs.

## REFERENCES


[1] P. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks," *Commun. Surveys Tuts.*, vol. 7, no. 3, pp. 2–21, Third Quarter, 2005.

[2] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Netw.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[3] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. 3rd ACM Workshop WiSE*, Sep. 2002, pp. 1–10.

[4] P. Papadimitratos and Z. Haas, "Secure data transmission in mobile ad hoc networks," in *Proc. ACM Workshop WiSE*, Sep. 2003, pp. 41–50.

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[6] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996.

[7] J. Edney and W. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access 802.11i*. Upper Saddle River, NJ: Pearson, 2004.

[8] C.-K. Toh, *Ad Hoc Mobile Wireless Networks—Protocol and Systems*. Upper Saddle River, NJ: Pearson, 2002.

[9] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 48–60, Feb. 2004.

[10] Y. Waizumi, Y. Sato, and Y. Nemoto, "A network-based anomaly detection system using multiple network features," in *Proc. 3rd Int. Conf. WEBIST*, Mar. 2007, pp. 410–413.

[11] H. Ebbinghaus, *Memory: A Contribution to Experimental Psychology*. New York: Teachers College, 1913.

[12] I. London, "An ideal equation derived for a class of forgetting curves," *Psychol. Rev.*, vol. 57, no. 5, pp. 295–302, Sep. 1950.

[13] P. Ning and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," in *Proc. 4th Annu. IEEE Inf. Assurance Workshop*, Jun. 2003, pp. 60–67.

[14] W. Wang, Y. Lu, and B. Bhargava, "On vulnerability and protection of ad hoc on-demand distance vector protocol," in *Proc. 10th ICT*, Feb. 2003, pp. 375–382.

[15] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz, "On the effect of node misbehavior in ad hoc networks," in *Proc. IEEE Global Telecommun. Conf. GLOBECOM*, Jun. 2004, pp. 3759–3763.

[16] C. Perkins, E. Belding-Royer, and S. Das, *Ad hoc On-Demand Distance Vector (AODV) Routing*, Jul. 2003. IETF RFC 3561 (Experimental).

[17] *Network Simulator—NS (ver. 2)*. [Online]. Available: http://nsnam.isi.edu/nsnam/

[18] M. Zapata, *Secure ad hoc on-demand distance vector (SAODV) routing*, Sep. 2006. IETF Internet Draft, draft-guerrero-manet-saodv-06.txt.

[19] *A-SAODV Homepage*. [Online]. Available: http://saodv.cefriel.it/

[20] D. Cerri and A. Ghioni, "Securing AODV: the A-SAODV secure routing prototype," *IEEE Commun. Mag.*, vol. 46, no. 2, pp. 120–125, Feb. 2008.

[21] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[22] D. Eastlake, III and P. Jones, *US Secure Hash Algorithm 1 (SHA1)*, Sep. 2001. IETF RFC 3174 (Informational).

[23] H. Yih-Chun and A. Perrig, "A survey of secure wireless ad hoc routing," *IEEE Security Privacy*, vol. 2, no. 3, pp. 28–39, May/Jun. 2004.

[24] H. Yih-Chun, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wirel. Netw.*, vol. 11, no. 1/2, pp. 21–38, Jan. 2005.

[25] H. Yih-Chun, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 175–192, Jul. 2003.

[26] M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A clusterbased security architecture for ad hoc networks," in *Proc. 23rd Annu. Joint Conf. IEEE Comput. Commun. Soc. INFOCOM*, Mar. 2004, pp. 2393–2403.

[27] M. Ramkumar and N. Memon, "An efficient key predistribution scheme for ad hoc network security," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 3, pp. 611–621, Mar. 2005.

[28] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 3, pp. 598–610, Mar. 2005.

[29] H. Deng, W. Li, and D. Agrawal, "Routing security in ad hoc networks," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 70–75, Oct. 2002.

[30] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in *Proc. 31st ICPP Workshops*, Aug. 2002, pp. 73–78.

[31] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks," in *Proc. 36th Annu. HICSS*, Jan. 2003, pp. 57–64.

[32] G. Vigna, S. Gwalani, K. Srinivasan, E. Belding-Royer, and R. Kemmerer, "An intrusion detection tool for AODV-based ad hoc wireless networks," in *Proc. 20th ACSAC*, Dec. 2004, pp. 16–27.

[33] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt, "A specification-based intrusion detection system for AODV," in *Proc. 1st ACM Workshop SASN*, Oct. 2003, pp. 125–134.

[34] Y. Huang, W. Fan, W. Lee, and P. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *Proc. 23rd ICDCS*, May 2003, pp. 478–487.

[35] Y. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in *Proc. 7th Int. Symp. RAID*, Sep. 2004, pp. 125–145.

[36] B. Sun, K. Wu, and U. Pooch, "Towards adaptive intrusion detection in mobile ad hoc networks," in *Proc. IEEE Global Telecommun. Conf. GLOBECOM*, Nov./Dec. 2004, pp. 3551–3555.

[37] R. Duda, P. Hart, and D. Stork, *Pattern Classification and Scene Analysis*. New York: Wiley, 1973.

[38] J. Tsumochi, K. Masayama, H. Uehara, and M. Yokoyama, "Impact of mobility metric on routing protocols for mobile ad hoc networks," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. PACRIM*, Aug. 2003, pp. 322–325.

[39] D. Maltz, J. Broch, J. Jetcheva, and D. Johnson, "The effects of on-demand behavior in routing protocols for multihop wireless ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 8, pp. 1439–1453, Aug. 1999.

[40] C. Perkins, E. Royer, S. Das, and M. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Pers. Commun.*, vol. 8, no. 1, pp. 16–28, Feb. 2001.

[41] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wirel. Commun. Mob. Comput.*, vol. 2, no. 5, pp. 483–502, Sep. 2002.

[42] G. Golub and C. V. Loan, "Matrix computations," in *Johns Hopkins Studies in Mathematical Sciences*, 3rd ed. Baltimore, MD: Johns Hopkins Univ. Press, 1996.

[43] I. Chakeres and C. Perkins, *Dynamic MANET on-demand (DYMO) routing*, Jul. 2007. IETF Internet Draft, draft-ietf-manet-dymo-10.txt.

[44] W. Yan, E. Hou, and N. Ansari, "Description logics for an autonomic ids event analysis system," *Comput. Commun.*, vol. 29, no. 15, pp. 2841–2852, Sep. 2006.

[45] W. Yan, E. Hou, and N. Ansari, "Extracting and querying network attack scenarios knowledge in IDS using PCTCG and alert semantic networks," in *Proc. IEEE ICC*, May 2005, pp. 1512–1517.


**Hidehisa Nakayama** (M'05) received the B.E., M.S., and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2000, 2002, and 2005, respectively.

He is currently a Senior Assistant Professor with Tohoku Institute of Technology, Sendai. He has been engaged in research on intelligent sensor technology, wireless mobile ad hoc networks, computer networking, character string analysis, pattern recognition, and image processing.

Dr. Nakayama is a member of the IEEE Communications Society, the Institute of Electronics, Information, and Communication Engineers (IEICE), and the Information Processing Society of Japan (IPSJ). He received the Paper Award for Young Researchers from the IPSJ Tohoku Chapter in 2000 and the Best Paper of Pattern Recognition Award at SCI 2003.

**Satoshi Kurosawa** received the B.E. degree from Miyagi University of Education, Sendai, Japan, in 2004 and the M.S. degree from Tohoku University, Sendai, in 2006.

He is currently with the Information Technology R&D Center, Mitsubishi Electric Corporation, Kamakura, Japan. His recent work has focused on ad hoc routing protocols and sensor network security. His research interests lie in the field of wireless networking, particularly ad hoc network security.

Mr. Kurosawa received the Dean of the Graduate School of Information Sciences Award in 2005.

**Abbas Jamalipour** (S'90–M'96–SM'00–F'07) received the Ph.D. degree from Nagoya University, Nagoya, Japan.

He is currently with the School of Electrical Information Engineering, University of Sydney, Sydney, Australia. He is the author of the first book on wireless IP, as well as two other books, and has coauthored five books and over 180 technical papers, all in the field of mobile communications networks. He is also the author of several invited papers. His areas of research are wireless data communication networks, wireless IP networks, next-generation mobile networks, traffic control, network security and management, and satellite systems. He was one of the first researchers to disseminate the fundamental concepts of next-generation mobile networks and broadband convergence networks, as well as the integration of wireless local area networks and cellular networks, some of which are being gradually deployed by industry and included in the ITU-T standards.

Dr. Jamalipour is a Fellow of the Institute of Engineers Australia, an IEEE Distinguished Lecturer, the Editor-in-Chief of IEEE WIRELESS COMMUNICATIONS, and a Technical Editor of several scholarly journals, including IEEE COMMUNICATIONS, the *Wiley International Journal of Communication Systems*, *Journal of Communication Networks*, etc. He has been a keynote speaker at many prestigious conferences. He served as the Chair of the Satellite and Space Communications Technical Committee (TC) from 2004 to 2006 and is currently the Vice Chair of Communications Switching and Routing TC and the Chair of Chapters Coordinating Committee, Asia-Pacific Board, all with the IEEE Communications Society. He is a voting member of the IEEE GITC and IEEE WCNC Steering Committees. He was the Vice Chair of the IEEE WCNC from 2003 to 2006, the Program Chair of SPECTS2004, the Chair of symposiums at IEEE GLOBECOM 2005 to 2007 and IEEE ICC 2005 to 2008, as well as many other conferences. He has received several prestigious awards, such as the 2005 Telstra Award for Excellence in Teaching, the 2006 IEEE Communications Society Best Tutorial Paper Award, and the 2006 IEEE Distinguished Contribution to Satellite Communications Award.

**Yoshiaki Nemoto** (S'72–M'73–SM'05) received the B.E., M.E., and Ph.D. degrees from Tohoku University, Sendai, Japan, in 1968, 1970, and 1973, respectively.

He is a Full Professor with the Graduate School of Information Sciences, Tohoku University, where he has also been an Executive Vice President since 2008. He has been engaged in research on microwave networks, communication systems, computer network systems, image processing, and handwritten character recognition.

Dr. Nemoto is a Fellow of the Institute of Electrical, Information, and Communication Engineers (IEICE) and the Information Processing Society of Japan (IPSJ). He is a corecipient of the 1982 Microwave Prize from the IEEE Microwave Theory and Techniques Society, the 2005 Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, and the FUNAI information Science Award.

**Nei Kato** (M'03–A'04–SM'05) received the M.S. and Ph.D. degrees from Tohoku University, Sendai, Japan, in 1988 and 1991, respectively.

Since 1991, he has been with Tohoku University, where he is currently a Full Professor with the Graduate School of Information Sciences. He has published more than 120 papers in journals and peer-reviewed conference proceedings. He has been engaged in research on computer networking, wireless mobile communications, image processing, and neural networks.

Dr. Kato is a member of the Institute of Electronics, Information, and Communication Engineers (IEICE). He has served as a Symposium Cochair at GLOBECOM'07 and ChinaCom'08 and as a Technical Program Committee member on a large number of IEEE international conferences, including ICC, GLOBECOM, WCNC, and HPSR. He was a Co-Guest Editor for the *Journal of Communications and Networks* (JCN) Special Issue on Broadband Convergence Networks (BcNs) in 2005. Since 2006, he has been the Technical Editor of IEEE WIRELESS COMMUNICATIONS. Since 2008, he has been the Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He is the corecipient of the 2005 Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee, the corecipient of the FUNAI Information Science Award in 2007, and the corecipient of the 2008 TELCOM System Technology Award from the Foundation for Electrical Communications Diffusion. He is serving as an expert member of the Telecommunications Council, Ministry of Internal Affairs and Communications, Japan.