INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS
Int. J. Commun. Syst. 2007; **20**:695–721
Published online 18 September 2006 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/dac.853

Integration of mobility and intrusion detection for wireless *ad hoc* networks

Bo Sun[1],*,†, Kui Wu[2],‡, Yang Xiao[3],§ and Ruhai Wang[4],¶

[1] *Department of Computer Science, Lamar University, Beaumont, TX 77710, U.S.A.*
[2] *Department of Computer Science, University of Victoria, BC, Canada V8W 3P6*
[3] *Department of Computer Science, University of Alabama, 101 Houser Hall, Box 870290 Tuscaloosa, AL 35487, U.S.A.*
[4] *Department of Electrical Engineering, Lamar University, Beaumont, TX 77710, U.S.A.*

SUMMARY

One of the main challenges in building intrusion detection systems (IDSs) for mobile *ad hoc* networks (MANETs) is to integrate mobility impacts and to adjust the behaviour of IDSs correspondingly. In this paper, we first introduce two different approaches, a Markov chain-based approach and a Hotelling's T^2 test based approach, to construct local IDSs for MANETs. We then demonstrate that nodes' moving speed, a commonly used parameter in tuning IDS performances, is not an effective metric to tune IDS performances under different mobility models. To solve this problem, we further propose an *adaptive* scheme, in which suitable normal profiles and corresponding proper thresholds can be selected *adaptively* by each local IDS through periodically measuring its local *link change rate*, a proposed unified performance metric. We study the proposed adaptive mechanism at different mobility levels, using different mobility models such as random waypoint model, random drunken model, and obstacle mobility model. Simulation results show that our proposed adaptive scheme is less dependent on the underlying mobility models and can further reduce false positive ratio. Copyright © 2006 John Wiley & Sons, Ltd.

Received 1 June 2005; Revised 1 June 2006; Accepted 1 July 2006

KEY WORDS: intrusion detection; mobile *ad hoc* networks; mobility model

1. INTRODUCTION

Global trustiness has become one of the fundamental assumptions in building mobile *ad hoc* networks (MANETs). Nevertheless, this assumption is not always true in reality. MANETs are

*Correspondence to: Bo Sun, Department of Computer Science, Lamar University, Beaumont, TX 77710, U.S.A.
† E-mail: bsun@cs.lamar.edu
‡ E-mail: wkui@cs.uvic.ca
§ E-mail: yangxiao@ieee.org
¶ E-mail: wang@ee.lamar.edu

Contract/grant sponsor: Texas Advanced Research Program; contract/grant number: 003581-0006-2006

very vulnerable to malicious attacks compared to traditional wired networks, because of the nature of MANETs such as open medium, low degree of physical security of mobile nodes, dynamic topology, limited power supply, and absence of central management point [1]. As a result, each node in MANETs should be prepared to work in a distributed environment with less trust to peers.

Intrusion prevention measures, such as encryption and authentication, can be used in MANETs to reduce intrusions, but cannot totally eliminate them. For example, a physically captured node that carries the private keys may allow the defeat of the authentication safeguards. A smart and determined attacker might find some security holes to break into a system no matter how many intrusion prevention measures are deployed. Hence, intrusion detection systems (IDSs), serving as a second line of defense, are necessary for constructing highly survivable networks.

One of the main difficulties in building MANET IDSs is how to consider mobility impacts when we design detection engines. This is especially important because most dynamics in MANETs are caused by mobility. MANET IDSs without properly considering mobility are prone to a high false positive ratio, rendering the IDSs less effective. Most previous work on MANET IDSs adopts mobile speed or node pause time to capture the influence of mobility on detection algorithms. However, we have observed that mobile speed alone is not an accurate measurement metric. The extraction of a common feature among different mobility models is necessary for tuning system parameters in detection engines.

In this paper, utilizing the feature values extracted from MANET routing activities, we first apply two different approaches, the Markov chain-based approach [2] and the Hotelling's T^2 test based approach [3], to construct local IDSs for MANETs. Using Markov chain models at different orders to construct the normal profiles for MANET routing activities at different mobility levels, we can examine the effectiveness of the *ordering* property of MANET routing activities. A *m-order* Markov chain model assumes that the next event depends on the last *m* events in the past. Using the Hotelling's T^2 test to construct MANET routing normal profiles that can detect both the mean shift, i.e. the deviation from the mean of extracted feature values, and the counter-relationships, i.e. the deviation from the correlation of multivariate feature values, we can examine the effectiveness of the frequency-distribution, i.e. the occurrences of multiple feature values in combination, of MANET routing activities.

One of the main challenges in building IDSs for MANETs is to integrate mobility impacts and to adjust behaviours of IDSs correspondingly. Utilizing different mobility models, the random waypoint model [4], the random drunken model and the obstacle mobility model [5], we first demonstrate that nodes' moving speed, a commonly used parameter in MANETs, is not effective in measuring the performance of MANET IDSs for different applications. Nodes' moving speed cannot reflect MANET dynamics accurately under different mobility models. Therefore, IDS measurements in terms of speed depend heavily on the underlying mobility models. We then propose an effective and unified measurement metric, *link change rate*, to capture the common feature of different mobility scenarios. We further propose an *adaptive* scheme, in which suitable normal profiles and proper thresholds can be selected *adaptively* by each local IDS agent through periodically measuring its local link change rate. By properly selecting the trained detection engine at different mobility scenarios, IDS performances can be further improved. Utilizing the Markov chain-based anomaly detection model as an exemplary MANET IDS, we demonstrate that our proposed adaptive mechanisms are less dependent on the underlying mobility models and can further reduce the false positive ratio, which is one of

DOI: 10.1002/dac

the main concerns when we deploy an anomaly-based IDS. Another contribution is that this paper provides a comprehensive performance evaluation and analysis of MANET IDSs under different mobility models.

The rest of the paper is organized as follows. In Section 2, a brief introduction of wired IDSs and wireless IDSs is presented. Section 3 presents the assumptions for this work. In Section 4, we introduce a threat model and the previous work on building an anomaly-based IDS for MANETs. In Section 5, we present the details of applying Hotelling's T^2 test to MANET IDSs. In Section 6, we propose a better and unified metric, Link Change Rate, and present adaptive mechanisms that can be integrated into local IDS agents. Section 7 presents detailed simulation results in terms of nodes' moving speed and the link change rate. Furthermore, we compare the performance of adaptive and non-adaptive MANET IDSs. Finally we conclude the paper in Section 8.

2. INTRUSION DETECTION SYSTEMS

Intrusions are defined as any set of actions that compromise confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges [6]. The system can be a host computer, a network equipment, a firewall, a router, a corporate network, or any information system being monitored by an IDS.

An IDS dynamically monitors a system and users' actions in the system in order to detect intrusions. Because an information system can suffer from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system which is not susceptible to attacks. Experience teaches us never to rely on a single defensive technique. IDSs, by analysing the system and user operations in search of activity undesirable and suspicious, can effectively monitor and protect against threats.

Research on IDSs began with a report by Anderson [7] followed by Denning's seminal paper [8], which lays the foundation for most of the current intrusion detection techniques. Since then, many research efforts have been devoted to wired IDSs. Numerous detection techniques and architecture for host machines and wired networks have been proposed. Readers can find a good taxonomy of wired IDSs in Reference [6].

With the rapid proliferation of wireless networks and mobile computing applications, new vulnerabilities that do not exist in wired networks have appeared. Security poses serious challenges in deploying wireless networks in reality. However, differences between wired and wireless networks make traditional intrusion detection techniques inapplicable. IDSs for wireless networks, emerging as a new research topic, aim to develop new architecture and mechanisms to protect wireless networks. Next, we briefly introduce the existing IDSs for wired networks (Wired IDSs) and IDS for wireless networks (Wireless IDSs).

2.1. Wired intrusion detection systems

Extensive research efforts have been devoted to wired IDSs, focusing mainly on network traffic data and computer audit data. There are two general approaches to detecting intrusions: misuse-based intrusion detection (also referred to as knowledge-based detection, or detection by

DOI: 10.1002/dac

appearance) and anomaly-based intrusion detection (also referred to as behaviour-based detection, or detection by behaviour). They are complementary to each other for intrusion detections.

2.1.1. Misuse-based intrusion detection systems. Misuse-based IDSs operate based on a database of known attack signatures and system vulnerabilities. When an IDS analyser identifies an activity matching a signature that is stored in the database, an alarm is triggered. Advantages of misuse-based IDSs include low false alarm ratio, being efficient and accurate in detecting known intrusions. Furthermore, triggered alarms are meaningful because attack signatures contain diagnostic information about the causes of the alarms. Disadvantages include that attack signature databases and system vulnerabilities need to be kept up-to-date. This is a tedious task because new attacks and system vulnerabilities are detected on a daily basis. Careful analysis of vulnerabilities is also time-consuming. Misuse-based IDSs also face the generalization issues because most of knowledge of attacks is focused on different versions of operating systems and applications.

There are several techniques in constructing misuse-based IDSs, differing in both representation and matching algorithms employed to detect intrusions, e.g. Expert Systems, Pattern Recognition, Colored Petri Nets, and State Transition Analysis, etc.

2.1.2. Anomaly-based intrusion detection systems. Anomaly-based IDSs assume that an intrusion can be detected by observing a deviation from normal or expected behaviours of the system or users. Normalcy is defined by the previously observed subject behaviour, which is usually created during a training phase. The normal profile is later compared with the current activity. If a deviation is observed, IDSs flag the unusual activity and generate an alarm. The advantages of anomaly-based IDSs include that they might be able to detect all attacks, i.e. they can detect attempts that try to exploit new and unforeseen vulnerabilities. They are also less system dependent. Disadvantages include that they may have a very high false alarm ratio and are more difficult to configure because a comprehensive knowledge of the expected system behaviour is required. They usually require a periodic online learning process in order to build the up-to-date normal behaviour profile. Anomaly-based detection approach is more difficult to implement than misuse-based detection approach, and it has only recently gained strong commercial support.

Several anomaly-based detection techniques exist and differ in the representation of a normal profile and the inference of a deviation from the normal profile. The main techniques used in anomaly-based IDSs include Statistics, Neural networks, Immunology, Expert Systems, etc.

Besides misuse-based detection and anomaly-based detection, there is a new class of detection algorithm: specification-based detection techniques [9]. It combines the advantages of misuse-based detection and anomaly-based detection techniques by detecting attacks as deviations from a normal profile. Their approaches are based on manually developed specifications, thus avoiding a high rate of false alarms. However, the development of detailed specifications can be time-consuming.

2.2. *Wireless intrusion detection systems*

Relatively few research efforts have been devoted to wireless IDSs. In Reference [10], Kachirski *et al.* proposed a distributed IDS for *ad hoc* wireless networks based on mobile agent

DOI: 10.1002/dac

technology. In Reference [11], Samfat *et al.* proposed an intrusion detection architecture for mobile networks (IDAMN). Its main functionality is to track and detect mobile intruders in real time. IDAMN includes two algorithms that model behaviours of users in terms of both telephony activities and migration patterns. In Reference [12], a routing misbehaviour in mobile *ad hoc* networks is identified: a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious, or broken. The authors proposed to install extra facilities, watchdog and pathrater, to identify routing misbehaviour in MANETs.

Zhang *et al.* proposed a general intrusion detection and intrusion response architecture for MANETs in Reference [1]. An agent is attached to each mobile node, and each node in the network participates in the intrusion detection and response. A majority-based distributed intrusion detection approach is proposed to facilitate the cooperation of neighbouring nodes, in that the intrusions will be detected with strong evidence unless the majority of the nodes are compromised. In Reference [13], a data mining method that performs the cross-feature analysis to capture the interfeature correlation patterns of MANET normal traffic is introduced to construct the normal profile. They focused on techniques for automatically constructing anomaly-based detection methods that are capable of detecting new attacks. In Reference [14], Huang *et al.* investigated how to improve the anomaly-based detection approach to provide more details on attack types and sources. In Reference [2], Sun *et al.* proposed a Markov chain-based anomaly detection algorithm for MANETs. However, most of the previous work uses the nodes' moving speed or pause time to tune IDS performances and consider only one specific mobility model.

3. FUNDAMENTAL ASSUMPTIONS

In the context of intrusion detection, we assume that normal and abnormal behaviours have distinct manifestations. This is the essential assumption that all anomaly-based detection systems are based on Reference [8]. Without such an assumption, anomaly-based intrusion detection will be impossible. It has been demonstrated via simulation in previous work [1, 13] that routing tables do exhibit different behaviours under attacks.

We assume that the local IDS agents are secure. Security of IDS agents presents another challenge for MANETs and is beyond the scope of this paper. Most of research in IDSs [1, 11, 13, 14] has to rely on this assumption to separate problem domains, and the assumption permits us to focus on one specific problem at a time. The same strategy has been used broadly in location-based routing protocols for *ad hoc* networks, where the availability of localization and location management are usually taken as granted, even if the localization and location management actually pose a much more challenging task for *ad hoc* networks [15].

4. BACKGROUND

4.1. Threat model

Since routing protocols provide one of the core functionalities for MANETs, this research will focus on detection of attacks targeted at MANET routing protocols, more specifically, on detecting one kind of the most important active attacks: routing disruption attacks described in

DOI: 10.1002/dac

the next subsection. Routing disruption attacks are particularly harmful to the whole network. It is deemed as one kind of the most vicious attacks and has been studied broadly by other researchers. In this section, we use the dynamic source routing (DSR) protocol [16] as the exemplary routing protocol to demonstrate behaviours of the routing disruption attacks. Our technique can be easily applied to other places.

4.1.1. Basic operations of DSR. DSR uses the source routing approach to forward packets, i.e. every data packet carries the whole path information in its header. Before a source node sends data packets, it must know the total path to the destination. Otherwise, it will initiate a route discovery procedure by flooding a route request (RREQ) message. The RREQ message carries a sequence of hops which it passes through in the message header. Nodes that have received the RREQ message broadcast it, but not again for the same message. Once an RREQ message reaches the destination node, the destination node replies with a route reply (RREP) packet to the source. The RREP packet carries the path information obtained from the RREQ packet. When the RREP packet traverses backward to the source, the source and all traversed nodes know the route to the destination. Each node uses a route cache to record complete routes to desired destinations. Route failure is detected by the failure of message transmissions. Such a failure initiates a route error message to the source. When the source and the intermediate nodes receive the error message, they erase all the paths that use the broken link from their route cache.

4.1.2. Routing disruption attack. Figure 1 illustrates one example of the routing disruption attack. In Figure 1, node 1 is compromised by an attacker. In order to effectively disrupt the routing logic, it actively sends falsified routing reply (RREP) packets into the network. Because of the source routing nature of DSR, the randomly constructed RREP needs to contain a valid path $1 \rightarrow 5 \rightarrow 3$ to guarantee the delivery of the RREP. There are many ways for the attacker to get this path. For example, node 1 could initiate a *route discovery* first, and wait for the path contained in the reply message. The attacker could then add a randomly constructed path, for example $\{2, 7, 9\}$, and form a RREP $\{2, 7, 9, 1, 5, 3\}$. Because of the wireless broadcast nature, there may exist many victims during the unicast of this faked RREP. In this example, the victims include node $\{2, 4, 7, 8\}$.

One significant characteristic of the *routing disruption* attack in MANETs is the 'partial victim' phenomenon. Because of arbitrary movements of nodes, link breakage is quite often.

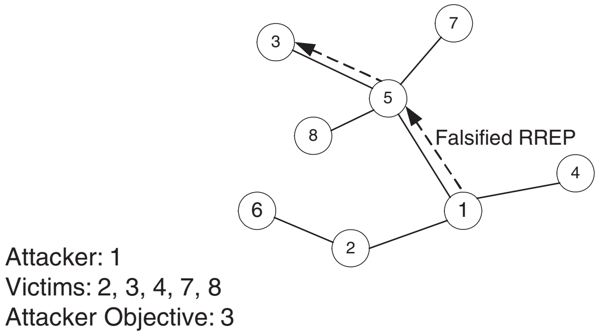
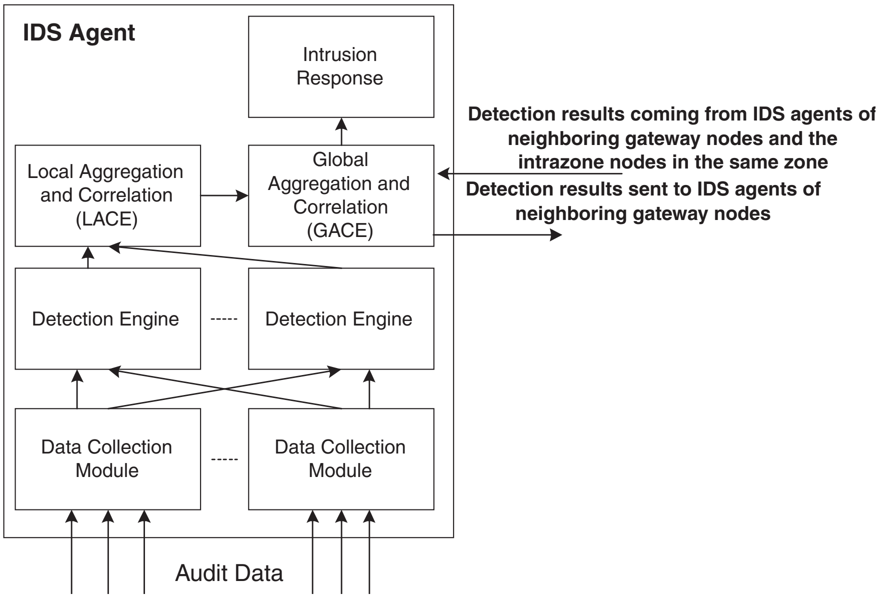


Figure 1. An example of the routing disruption attack.

DOI: 10.1002/dac


IDS Agent
Intrusion Response
Detection results coming from IDS agents of neighboring gateway nodes and the intrazone nodes in the same zone
Local Aggregation and Correlation (LACE)
Global Aggregation and Correlation (GACE)
Detection results sent to IDS agents of neighboring gateway nodes
Detection Engine

Detection Engine
Data Collection Module

Data Collection Module
Audit Data

Figure 2. Diagram of an IDS agent.

Therefore, it is difficult to target a node all the times. For example, movements of nodes lead to the breakage of link 5 → 3. This enables node 3 free of the impact of falsified routing packets. This phenomenon becomes more intense with the increase of the mobility.

4.2. Markov chain-based anomaly detection in MANETs

In this section, we briefly introduce a Markov chain-based anomaly detection system for MANETs. For the details, please refer to our previous work in Reference [2]. In the system, each node includes a local IDS agent. The internal structure of the IDS agent is shown in Figure 2.

The data collection module is mainly responsible for collecting security related data from various audit sources and preprocesses them to the input format required by detection engines. The detection engine then uses the data to perform intrusion detection tasks locally. We construct a Markov chain-based anomaly detection algorithm as the local detection model [2]. The local aggregation and correlation engine (LACE) locally aggregates and correlates detection results from different detection engines in the IDS agent. The functionality of global aggregation and correlation engine (GACE) is to aggregate and correlate the alert information from a wider area in order to make a better decision. The functionality of the intrusion response module is to handle the generated alarms.

We have implemented a Markov chain-based anomaly detection approach for MANET IDSs. Specifically, we construct a Markov chain from the discretized routing table changes. Using the immediate previous w consecutive events (the routing table changes), also called the *from_state*, we can predict the transition probability of the next state, *to_state*. This transition probability is then used to calculate the distance and classify the observed activities.

DOI: 10.1002/dac

The work in Reference [2] also shows that the classifier constructed using PCH (percentage of the change in number of hops) performs better than the classifier constructed using PCR (percentage of the change in route entries). Therefore, in Section 6, we use the classifier constructed using PCH as the local detection engine and compare its performance under different mobility models.

5. HOTELLING'S T^2 TEST BASED INTRUSION DETECTION

Markov chain-based approach examines the *ordering* property of the routing activities. Intrusion detection research in wired networks has demonstrated that the frequency distribution of audit events may also have impacts on the IDS performance [17]. Therefore, in this section, we apply the Hotelling's T^2 test to MANET IDSs and examine the effectiveness of frequency distribution of PCH and PCR.

Hotelling's T^2 test [3] is one of the most important multivariate process-monitoring and control procedures to detect anomalies in a process. In the following, we present the basic principle of the Hotelling's T^2 test and its application to MANET IDSs. For the purpose of presentation, bold variables are used to denote vectors or matrixes.

5.1. Hotelling's T^2 test

We treat the MANET routing table changes of each node as a process. Means and covariances are two important parameters that can be used to characterize the properties of a process. We denote the expectation of a random variable x by $E(x)$. Suppose that we use p random variables, $x_1, x_2, \ldots, x_p$, to represent the measurements on p characteristics of the MANET routing process. Suppose that the expectations of these p variables are $E(x_1), E(x_2), \ldots, E(x_p)$, respectively. We then define the mean of this process as $\boldsymbol{\mu} = E(\mathbf{x}) = [E(x_1), E(x_2), \ldots, E(x_p)]' = [\mu_1, \mu_2, \ldots, \mu_p]'$. The covariance matrix $\sum$ of this process is then defined as

$$\begin{bmatrix} (x_1-\mu_1)^2 & (x_1-\mu_1)(x_2-\mu_2) & \ldots & (x_1-\mu_1)(x_p-\mu_p) \\ (x_2-\mu_2)(x_1-\mu_1) & (x_2-\mu_2)^2 & \ldots & (x_2-\mu_2)(x_p-\mu_p) \\ \vdots & \vdots & \vdots & \vdots \\ (x_p-\mu_p)(x_1-\mu_1) & (x_p-\mu_p)(x_2-\mu_2) & \ldots & (x_p-\mu_p)^2 \end{bmatrix} \tag{1}$$

Let $\mathbf{x} = [x_1, x_2, \ldots, x_p]'$, a p-component vector, denote an observation of p variables from the MANET routing process at time t. Then given this observation $\mathbf{x}$, the Hotelling's T^2 statistic is computed as

$$T^2 = (\mathbf{x}-\boldsymbol{\mu})' \sum^{-1} (\mathbf{x}-\boldsymbol{\mu}) \tag{2}$$

The value T^2 indicates the deviation of the observation $\mathbf{x}$ from the in-controlled population. The larger the value T^2, the larger the deviation of the observation $\mathbf{x}$ from the in-controlled population is. From Equation (2), we can see that statistic T^2 can be used to detect both the

DOI: 10.1002/dac

mean shift through $(\mathbf{x} - \boldsymbol{\mu})$ and the counter-relationships of multivariate variables through the covariance matrix $\sum$.

In practice, however, it is difficult to obtain $\boldsymbol{\mu}$ and $\sum$. Therefore, we use the sample mean $\overline{\mathbf{x}}$ and sample covariance matrix $\mathbf{S}$ to estimate $\boldsymbol{\mu}$ and $\sum$, respectively.

Given a data sample of n observations $\mathbf{x_1}, \mathbf{x_1}, \ldots, \mathbf{x_n}$, where $\mathbf{x_i} = [x_{i1}, x_{i2}, \ldots, x_{ip}]'$, $1 \leqslant i \leqslant n$. The sample mean can be computed as $\overline{\mathbf{x}} = [\overline{x_1}, \overline{x_2}, \ldots, \overline{x_p}]'$, where $\overline{x_i} = \frac{1}{n}\sum_{j=1}^{n} x_{ji}$, $1 \leqslant i \leqslant p$ [3].

The sample covariance matrix $\mathbf{S}$ of these p variables can be computed as

$$\mathbf{S} = \frac{1}{n-1}\sum_{i=1}^{n}(\mathbf{x_i} - \overline{\mathbf{x}})(\mathbf{x_i} - \overline{\mathbf{x}})'$$

Replacing $\boldsymbol{\mu}$ with $\overline{\mathbf{x}}$ and $\sum$ with $\mathbf{S}$ in Equation (2), we can use Equation (3) to compute the sample $\overline{T^2}$ as

$$\overline{T^2} = (\mathbf{x} - \overline{\mathbf{x}})'\mathbf{S}^{-1}(\mathbf{x} - \overline{\mathbf{x}}) \tag{3}$$

5.2. *Applying Hotelling's T^2 test to MANET IDSs*

Hotelling's T^2 test provides a complete data model of the multivariate data $\mathbf{x}$ and it can indicate the deviation of the subject activities. The value T^2 depends on the frequency-distribution of the vectors (observations). When we have a new observation $\mathbf{x}$, we use Equation (3) to compute its T^2 value. If the distance between the computed T^2 and $\overline{T^2}$, $d = |T^2 - \overline{T^2}|$, is larger than a threshold δ, a *signal* is raised on $\mathbf{x}$. Otherwise, $\mathbf{x}$ is regarded as normal.

We have used the Markov chain-based approach to identify that both PCR and PCH are effective features that can be used to characterize the routing activities of MANETs [2]. Therefore, we use PCR and PCH to form a two-dimensional vector to represent each observation, i.e. $\mathbf{x} = [\mathrm{PCR}, \mathrm{PCH}]$. Utilizing T^2, we test whether a new observation $\mathbf{x} = [\mathrm{PCR}, \mathrm{PCH}]$ follows the trained normal profile. Because the random waypoint model [4] is the most commonly used mobility model, we adopt it as our mobility model to carry out simulations.

Specifically, using the same simulation setting as in [2], we collect the training data and test data at different mobility levels. For the training data at one mobility level, we use the training data to compute the sample mean $\overline{\mathbf{x}}$, the sample covariance matrix $\mathbf{S}$, and sample $\overline{T^2}$. We further compute the standard deviation of $\overline{T^2}$, denoted as σ.

Under the same simulation setting, we further collect a set of test data (including normal data and attack data) to test the performance. Simulation results and discussions are presented in the following section.

5.3. *Simulation results and discussions*

5.3.1. Data sets. We use a simulation model based on GloMoSim [18] to evaluate the performance of our MANET IDSs using different metrics. The channel capacity of mobile hosts is set to 2 Mbps. We use the distributed co-ordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. In the simulation of all three mobility models, 30 mobile nodes move in a rectangular region of $1000 \times 500\ \mathrm{m}^2$. Eight source-destination pairs are selected randomly to generate constant bit rate (CBR) traffic. The interval time for data transmission is 0.25 s. The size of all data packets is set to 512 bytes. When we simulate a routing disruption attack, the attacker is chosen from the 30 nodes randomly.

DOI: 10.1002/dac

We adopt the random waypoint model and set the pause time to 0S. We use different (*minimum speed*, *maximum speed*) pairs to represent different mobility scenarios. *Speed* is then defined as the average of the *minimum speed* and *maximum speed*. At each mobility level, we run the simulation 100 min in order to get the normal data, and collect the normal data from all nodes to generate a normal data trace. For each data trace, we collect (PCR and PCH) feature values every 3 s after a warm-up period of 300 s. We use a different random seed to further generate a collection of test data.

Based on GloMoSim, we simulate the routing disruption attack scenarios, as described in Section 4.1.2. To obtain data of intrusive behaviours, under the same mobility scenario, we run the simulation 10 min. For each run, we let the attack script start at 400 s, and each attack lasts 60 s.

5.3.2. Simulation results. We first present the concept *signal rate* before we discuss the simulation results.

Definition: Signal rate is measured over a set of observations. Suppose that there are j measured observations, and i of them raise *signal*s, *signal rate* is defined as i/j.

We measure the signal rate over both the normal data and attack data. The threshold δ should be tuned to consider the trade-off between the signal rate of both normal data and attack data. A too small δ leads to a high signal rate from the normal data. A too large δ, on the other hand, leads to a small signal rate from the attack data. We set δ to σ, 2σ, and 3σ, respectively, and measure the corresponding signal rates. Based on our simulation, we find that a large δ tends to lead to a small detection rate. This is because the attack session may be intermitted with the normal activities. If we use a large δ, this will significantly lower the signal rate of the attack data and makes it hard to distinguish normal sessions from attack sessions. Therefore, we set $\delta = \sigma$.

Figure 3 illustrates the average computed T^2 over the collected attack and test data at different mobility levels. We observe that the computed T^2 values of normal data are, on the average, smaller than that of the attack data. Note that the smaller the T^2, the closer the observation is to the normal profile. We also observe that with the increase of the mobility, i.e. the increase of the moving speed, the difference between normal data's T^2 and attack data's T^2 becomes smaller. Actually, when the mobility level is high enough, e.g. with an speed of

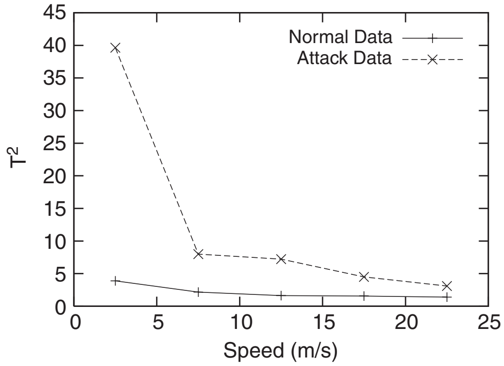


Figure 3. T^2 of test data.

DOI: 10.1002/dac

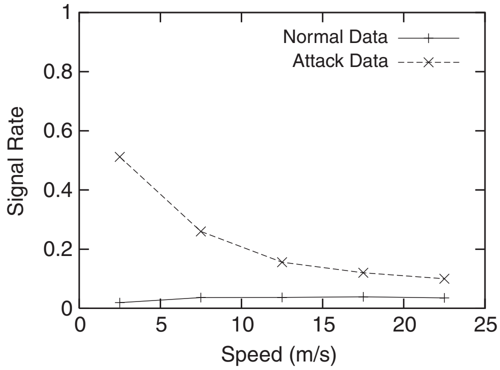


Figure 4. Average signal rate.

22.5 m/s, there is little difference between normal data's T^2 and attack data's T^2. This is because when the mobility is high, there are more dynamics in the normal routing activities. This makes much normal yet unexpected activities appear abnormal in the normal data. Therefore, it is difficult to distinguish normal data from attack data when the mobility level is high.

Figure 4 illustrates the average signal rate over normal data and attack data at different mobility levels. For one attack session, we should not expect a 100% signal rate. This is because attack activities often involve some normal behaviours. This is especially true in MANETs because of mobility-induced errors. However, when the mobility is low, the overall behaviour of attack activities is statistically different from those of the normal activities, as we observe from Figure 4. Therefore, when the mobility level is low, we can use the signal rate to distinguish the normal data from the attack data. Again, this distinction is not effective with a high mobility level, when the signal rate difference between the normal data and attack data is small.

Note that we cannot directly use the T^2 value to distinguish normal data from attack data. Otherwise, this leads to a very low alarm detection rate, as we can see from Figure 4.

Based on Figure 4, we can use a proper *detection rate d* to distinguish normal sessions from attack sessions. In other words, if the actual signal rate is smaller than d, then the activities are normal. Otherwise, the activities belong to attack sessions. At a given mobility level, suppose that the average signal rate of the normal data and attack data are s_n and s_a, respectively, then a suitable d can be set to $(s_n + s_a)/2$.

5.4. Discussion

Markov chain-based approach examines the effectiveness of the ordering property. The discretized feature values give a time-series representation of MANET routing activities. Normal profiles based on Markov chains can examine the probability of the next feature value based on previous several values. Hotelling's T^2 test examines the effectiveness of the frequency property of MANET routing activities. Based on the occurrence frequency of the extracted feature values, Hotelling's T^2 test can monitor both the mean vector of the routing activities and the correlations among the observed variables.

DOI: 10.1002/dac

It can be demonstrated that both the ordering property and the frequency distribution of routing activities are useful in distinguishing normal activities from malicious activities. Also, a single observation at a given time is not enough to make a correct decision.

However, both approaches are not effective when the mobility is high. So, cooperative IDSs are necessary in order to provide more practical MANET IDS schemes. This can effectively suppress more false positives, as we have demonstrated in Reference [19].

In the following sections, we further consider the performance of IDSs under different mobility models. Specifically, we use the Markov chain-based IDS as the local IDS to propose a general mobility-independent MANET IDS scheme.

6. ADAPTIVE IDSs

6.1. Different mobility models

Three mobility models, the random waypoint (RW) model [4], the random drunken (RD) model, and the obstacle mobility (OM) model [5], are adopted in this paper.

RW model is adopted because it is one of the most widely used mobility models. There exist many research efforts whose simulations are based on the RW model. In the RW model, each node randomly selects a destination in the simulated area and a speed from a uniform distribution of specified speeds. The node then travels to its selected destination at the selected speed. Once arriving at the destination, it is stationary for a given pause time. After that, the node resumes its movement to a newly selected destination with a newly selected speed.

The reason that we adopt the RD model is because it contrasts sharply with the RW model. The comparison of IDS performances based on these two models can clearly demonstrate that speed alone is not a good metric in IDS tuning. In the RD model, each node moves independently with the same average speed. Each node moves continuously within the region without pausing at any location. It changes direction after every unit of distance. Although the RD model is not likely valid in a realistic application, it can provide us with the knowledge of IDS performances in an environment where nodes change directions very quickly but links stay relatively stable [20].

Besides the RW and RD model, we further adopt the OM model because it is a more realistic movement model through the incorporation of realistic obstacles and movement paths. Most of the existing mobility models, such as the RW model and the RD model, do not take into consideration obstacles, so that their movement patterns are not necessarily comparable to real world movement. The OM model is constructed to model the movement of mobile nodes in terrains that resemble real world topographies. It is a more realistic movement model since the objects model buildings and other structures that provide a barrier to both movements of mobile nodes, as well as wireless transmission of these nodes. Arbitrarily complex polygonal shapes are used to specify the obstacles (buildings). Each polygonal shape is specified as an ordered sequence of its vertices (corners), where each vertex is defined by its co-ordinates. Voronoi Diagram [21] of the obstacle corners are used as the movement graph. In the OM model, nodes move along paths that are defined by the edges of the Voronoi diagram between the set of objects. Transmission behaviour in the OM model is influenced by the presence of objects. Objects are assumed substantial enough to prevent the passage of transmissions through their walls.

DOI: 10.1002/dac

6.2. *A better metric*

6.2.1. Speed is not an accurate metric. Nodes' moving speed is one of the most commonly used metrics in measuring the performance of MANETs. It is very obvious that speed could be used to reflect MANET dynamics. The larger the moving speed, the more dynamic MANETs are. However, nodes' moving speed does not take into consideration the relative movement of nodes. Consider a group of nodes moving at the same speed along the same direction. Even if they move at a very high speed, there are few incurred network dynamics because this leads to little relative movements among this group of nodes. Because of this, there are few triggered routing table changes. Therefore, IDSs based on the speed alone could demonstrate different behaviours at the same mobility level under different mobility models. This is further illustrated in Section 7.3.

6.2.2. Link change rate. Our research motivation is to find a unified metric which is less dependent on mobility models and can be used to adjust the MANET IDS performance. Because routing table changes are more directly impacted by link changes, we measure the link change rate of different mobility models and use it as a unified metric.

Two nodes are called neighbours if they can communicate with each other directly. For a given node a, at time t_1, its neighbour set (all those neighbours of node a) is denoted as N_1; at time t_2 ($t_2 > t_1$), its neighbour set is denoted as N_2. Because of mobility, N_1 and N_2 can be two different sets. Furthermore, the greater the mobility, the greater the difference between N_1 and N_2 can be.

We define the *link change rate* (lcr) as

$$\mathrm{lcr} = (|N_2 - N_1| + |N_1 - N_2|)/|t_2 - t_1|$$

$|N_2 - N_1|$ means the number of new neighbours during the interval $(t_2 - t_1)$, and $|N_1 - N_2|$ means the number of neighbours that move away during the interval $(t_2 - t_1)$. $|N_2 - N_1|$ and $|N_1 - N_2|$ represent the number of changed neighbours during the time interval $(t_2 - t_1)$.

Let's use one example to illustrate the concept of the *link change rate*. Suppose that for node 22, its neighbour set at time $t_1 = 12$ s is $\{1, 2, 10, 15, 18\}$, its neighbour set at time $t_2 = (t_1 + 3)$ s is $\{1, 2, 10, 16, 20, 28\}$. Then $|N_2 - N_1| = 3$ because of the newly increased neighbours $\{16, 20, 28\}$, and $|N_1 - N_2| = 2$ because of the newly decreased neighbours $\{15, 18\}$. lcr is $(3 + 2)/3 = 1.667$. Also, we can see that link change rate can be *locally* collected by each node.

The IDS performance in terms of the link change rate over different mobility models is illustrated in Section 7.4.

6.3. *Adaptive mechanisms*

The fact that the link change rate can be used to reflect MANET dynamics and it is less dependent on mobility models motivates us to investigate *adaptive* mechanisms that utilize the link change rate as a security feature and integrate it into our IDS model. For an effective anomaly-based IDS, an important requirement is that the constructed profiles are better to be adaptive. Adaptive profiles can account for normal network changes to reduce raising false alarms. This is especially important in MANETs given their dynamic environments, where different mobility levels will need different normal profiles.

We introduce adaptive mechanisms into our systems by adjusting the probability transition matrix characterized by the Markov chain and the detection threshold through learning its

DOI: 10.1002/dac

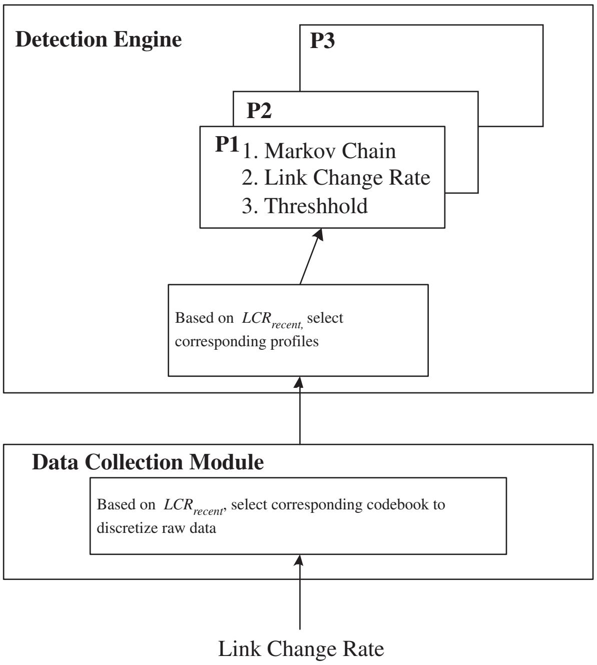

Detection Engine
P3
P2
P1
1. Markov Chain
2. Link Change Rate
3. Threshhold
Based on $LCR_{recent,}$ select corresponding profiles
Data Collection Module
Based on LCR_{recent}, select corresponding codebook to discretize raw data
Link Change Rate

Figure 5. Adaptive mechanism.

environments *locally*. In our adaptive mechanism, each node measures its link change rate periodically. Based on the measured link change rate in the recent history, each local IDS can adjust the parameter settings of the Markov chain and the detection threshold. MANET IDSs at different mobility scenarios need different profiles and different thresholds. The link change rate can provide a unified metric and it is less dependent on different mobility models. In this respect, it can be used to adjust the behaviour of IDSs.

We take the following procedures to construct our adaptive MANET IDS, as illustrated in Figure 5:

- *Offline training*: Using different mobility models, we first identify different mobility levels and compute their corresponding average link change rate. At each specific link change rate, we collect the routing activities in terms of PCH. Following the existing offline training approach to construct the classifier [2], we compute the codebooks (the output of the LBG algorithm [22] used to discretize the raw continuous data), Markov Chains, detection thresholds, etc., as the normal profile at different mobility levels.
- *Online selection*: The data collection module of each IDS agent periodically collects its local link change information and computes its link change rate over the recent history, denoted as $\text{LCR}_{\text{recent}}$. It is normal that a node could change its mobility level over time. $\text{LCR}_{\text{recent}}$ reflects the recent local dynamics for this specific node. PCH is also periodically measured over the recent history, as specified in Reference [2]. Based on $\text{LCR}_{\text{recent}}$, the data preprocess module selects the corresponding codebook whose link change rate has the smallest Euclidean distance to $\text{LCR}_{\text{recent}}$. Using this codebook, raw data (i.e. PCH) are

discretized using the LBG algorithm. $\mathrm{LCR}_{\mathrm{recent}}$ is then reported to detection engines, which can select the normal profile whose link change rate has the smallest Euclidean distance to $\mathrm{LCR}_{\mathrm{recent}}$. After the normal profile is selected, the intrusion detection process can start. For a summary of the detailed process, please refer to Reference [23].

Because of the existence of obstacles and fixed paths in the OM model, links may have abrupt changes compared to those in the RW model and the RD model. For example, when a node turns around a corner, old links may be blocked and a lot of new links may be found. In this way, the link change rate could change abruptly. Therefore, a mechanism is needed to accommodate this abrupt change. Thus, for the OM model, we add a training data preprocess to offline generate its classifier.

The main functionality of the training data preprocess is to split the original training data set into a new set of training data, with each set corresponding to one calculated link change rate. Given the originally collected training data sets, we first compute its average link change rate at each mobility level, denoted as $\mathrm{lcr}_{\mathrm{avg}\_i}$, where i is the corresponding mobility level. For each specific training data set at mobility level i, we break it based on the Euclidean distance of its recent link change rate to $\mathrm{lcr}_{\mathrm{avg}\_i}$. That is, we add the block of *raw* training data set (the link change rate of this block of training data set has the smallest Euclidean distance to the selected $\mathrm{lcr}_{\mathrm{avg}\_i}$) to the newly formed training data set corresponding to mobility level $\mathrm{lcr}_{\mathrm{avg}\_i}$ in sequence. For a detailed training data preprocess for the OM model, please refer to Reference [23].

Existing research work could be used to help measuring the link change rate. For example, in Reference [24], a link expiration scheme is proposed to help improving the performance of various routing protocols.

7. PERFORMANCE EVALUATION

7.1. Simulation platform and parameter settings

Our simulation is still based on GloMoSim [18]. Except the mobility models, we use the same simulation setting as in Section 5.3.1. Here we just list the details about how to set up the mobility models.

In the RW model and OM model, the *pause time* was set to 0 s. In each movement epoch, the speed was uniformly chosen between the *minimum speed* and the *maximum speed*. The *minimum speed* and *maximum speed* are set to different values in order to measure the impact of the speed on IDS performances. In the RD model, the movement granularity was set to 1 m.

In the OM model, the obstacles are utilized to calculate pathways and obstruct transmissions [5]. In our simulation, the obstacles are in the locations illustrated in Figure 6. The Voronoi paths are then generated based on this model.

7.2. Performance metrics

We use the following metrics throughout the simulation.

- *False positive ratio*: It is defined as the percentage of decisions in which normal data are flagged as anomalous.

DOI: 10.1002/dac

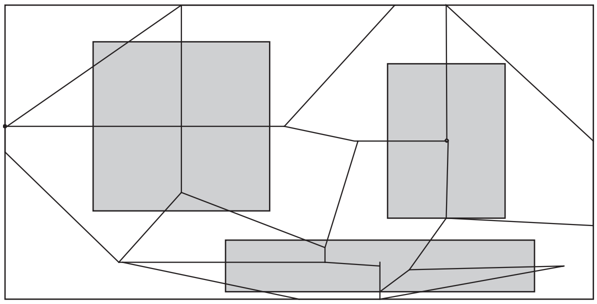


Figure 6. Simulated terrain under the OM model.

- *Detection ratio*: It is reported for traces of intrusive behaviour and is computed from dividing the total number of correct detections by the total number of victims in the anomalous data.
- *Mean time to the first alarm* (*MTFA*): It is defined over anomalous traces and measures how fast the classifier detects the attack. Given an anomalous trace ξ, if we suppose that the attack start location is L_a and our IDS generates its first alarm after scanning the L_dth symbol, then the MTFA corresponding to ξ normalized by the length (denoted as L) of the locality frame is given by $\text{MTFA}(\xi) = (L_d - L_a)/L$.

For each scenario, ten runs with different random seeds were conducted and the results were averaged. When the confidence intervals were calculated, the confidence levels were set to 95%.

7.3. IDS behaviour using speed as a metric

In order to investigate the impact of different mobility models on the performance of local MANET IDSs, we use the same parameters (the same number of discretized output of *Vector Quantization* algorithm, 'rare symbol' conversion threshold, window size, length of short-term subject activity, penalized value, etc.) to tune *alert threshold* of IDSs under different mobility models [2]. Given a mobility model, the same amount of training data, test data, and abnormal data at different mobility levels are collected using the same procedure in order to build the classifier. A different set of data is collected to evaluate the performance of the classifier.

7.3.1. False positive ratio. We use relatively larger speed (small mobility interval time) in the RD model because we observe that when the speed is small in the RD model, the link changes are very small, the routing tables are quite stable, and thus the false positive ratio is almost zero.

In Figure 7, we can see that for the RW model and the RD model, with the increase of speed, the false positive ratio increases. This change is dramatic for the RW model. With the increase of moving speed, no matter what mobility models we use, the node routing tables have more changes. Therefore, the trace demonstrates lower regularity, which results in the higher false positive ratio.

We can see that although the moving speed of the RD model is larger than that of the RW model and the OM model, its false positive ratio is much smaller. This is because given the same moving speed, the RD model does not generate as many link breakages as the RW model does [20], and also because routing table changes are impacted directly by link changes instead of

DOI: 10.1002/dac

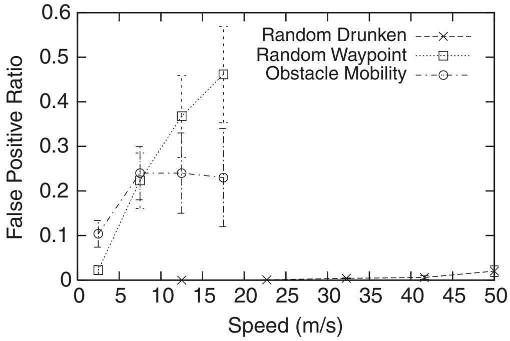


Figure 7. False positive ratio when using nodes' moving speed as a parameter.

nodes' moving speed. If a group of nodes move in the same direction, it is possible that although they move at a very high speed, their routing tables experience small changes. This demonstrates that speed is not a good metric in measuring false positive ratio when we consider different mobility models.

We can also see in Figure 7 that the false positive ratio of the OM model increases with the increase of speed at a relatively lower speed. However, when the speed is increased further, we do not observe this phenomenon. This is because the moving paths in the OM model are fixed. The fixed paths can greatly reduce the randomness although the speed is high. Therefore, it is easier to characterize normal routing behaviour more accurately. This will contribute to the lower false positive ratio compared to the RW model at a high speed.

From Figure 7, we can also see that there are some abrupt changes for the false positive ratio of IDS over the OM model. This illustrates the impact of the OM model on the IDS performance. In the OM model, mobile nodes move along the constructed pre-defined paths, as illustrated by the solid lines in Figure 6. Based on the design of the OM model [5], the radio transmission is completely blocked by the obstacle. Therefore, it is possible that all of the routing entries in a mobile node can become invalid all of a sudden, which will lead to a dramatic change on the routing activities. This will incur irregularities on both the training data and the test data. The incurred irregularity to the normal data will make it more difficult to construct the routing normal profile, while the incurred irregularity to the test data will lead to some unexpectedness of the false positive ratio.

When the nodes' moving speed is relatively low, the false positive ratio of the RD model is zero in our simulation. This seemingly impossible result does not mean any errors in the simulation. Instead, it indicates that links are quite stable in the RD model and with our simulation settings we did not observe any false positive ratio. Nevertheless, as we introduced before, the RD model is unlikely to happen in realistic applications. The purpose of introducing the RD model is purely for comparison. Similar usage of the RD model has also been introduced by other researchers in the context of MANETs before [25].

7.3.2. Detection ratio. From Figure 8, we can see that in all three mobility models, detection ratio decreases with the increase of the speed. When mobility is low, routing table changes are less dramatic and have less unexpected changes. Therefore, abnormal behaviours tend to have a larger distance from normal profiles, and it is easier for the classifier to identify the abnormal

DOI: 10.1002/dac

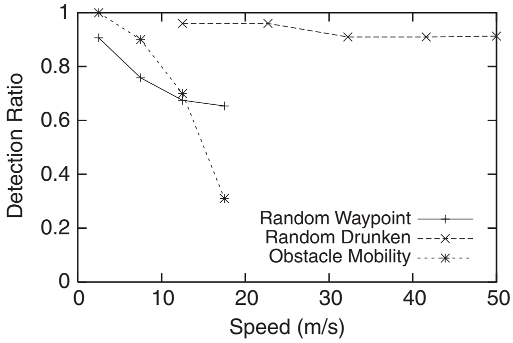


Figure 8. Detection ratio when using nodes' moving speed as a parameter.

behaviour. Also, the phenomenon of 'partial victims' is more obvious at high mobility. 'Partial victims' will contribute to the decrease of the detection ratio.

We observe that the overall detection ratio of the RD model is higher than that of the RW model and the OM model, even if the nodes' moving speed is much higher in the RD model. The reason is similar: network topology is much more stable in the RD model than in other models at the same moving speed. This demonstrates that speed is not an accurate metric in measuring detection ratio.

We can see that the detection ratio of the OM model drops more quickly than that of the RW model. This demonstrates the impact of obstacles and the transmission behaviour in the OM model. The existence of obstacles may block fake routing packets, and thus a targeted victim may only receive very few fake routing packets. Based on this, the detection engine is not able to effectively detect the attack. This type of 'partial' victims leads to the decrease of the detection ratio in the OM model. Nevertheless, low detection ratio does not necessarily mean the inefficiency of the detection engine. In this special case, the attacker cannot cause serious damage, because the few fake routing entries are erased from the victim's routing cache by the timeout.

7.3.3. MTFA. As illustrated in Figure 9, for the RW model and the OM model, its MTFA increases with the increase of nodes' moving speed. This is because larger moving speed leads to a larger *alert threshold*, and therefore leads to larger MTFA. We can also see that although the nodes' moving speed is larger in the RD model, its MTFA is smaller than those of the RW model and the OM model. This again demonstrates that speed is not a good metric in measuring the performance of IDS.

7.4. IDS behaviour using link change rate as a metric

For a given mobility model and a given mobility level represented by {*minimum speed*, *maximum speed*} pair, we compute the average link change rate. Using the computed link change rate, we measure the MANET IDS performance over different mobility models to see if its performance is mainly determined by link change rate. The IDS performance over different mobility models is illustrated in Figures 10–12.

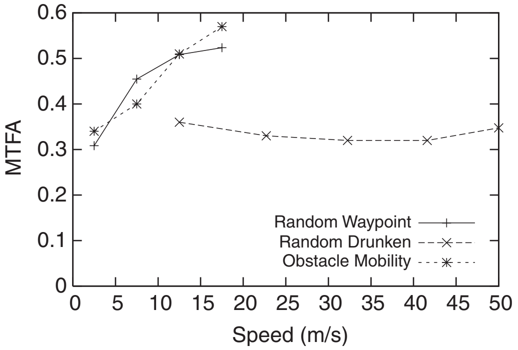


Figure 9. MTFA when using nodes' moving speed as a parameter.

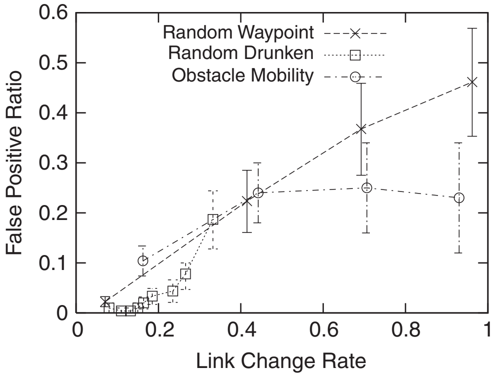


Figure 10. False positive ratio when using link change rate as a parameter.

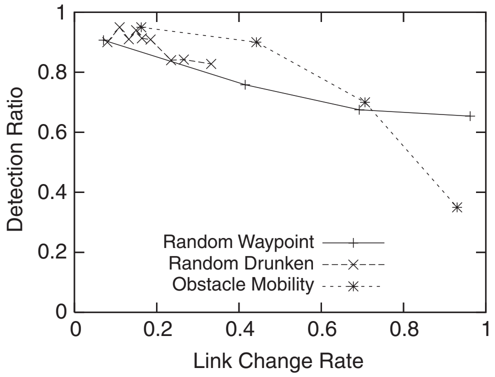


Figure 11. Detection ratio when using link change rate as a parameter.

DOI: 10.1002/dac

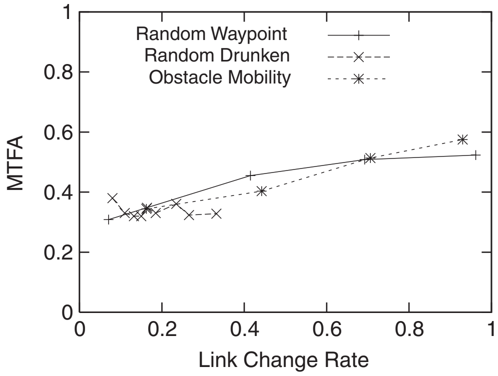


Figure 12. MTFA when using link change rate as a parameter.

7.4.1. False positive ratio. As shown in Figure 10, with the increase of the link change rate, the false positive ratio increases. Compared to Figure 7, Figure 10 demonstrates that if parameter settings of IDS are based on the link change rate, the performance of IDS will be less dependent on mobility models. Compared with nodes' moving speed, link change rates can be used more accurately to measure routing table changes. A larger link change rate implies a more dynamic environment, which makes it more difficult to differentiate normal and abnormal behaviours.

Compared to the RW model and the RD model, the use of obstacles and pathways in the OM model has impacts on the performance of IDS. In the OM model, nodes move along paths that are defined by the edges of the Voronoi diagram between the set of objects. This greatly reduces the randomness of path selection in the OM model, which makes it relatively easy for the detection engine to characterize the normal routing behaviour accurately. Therefore, the false positive ratio in the OM model does not increase dramatically with the increase of the link change rate, compared to the other two mobility models.

7.4.2. Detection ratio. The overall trend for the detection ratio is that with the increase of the link change rate, the detection ratio for all three models drops. From Figure 11, we can see that for the same link change rate, the differences of detection ratio among different models do not have big gap. In contrast, for the same moving speed, the results of detection ratio for different mobility models are basically incomparable as shown in Figure 8.

We observe that the detection ratio in the OM model decreases quickly with the increase of the link change rate. Because of obstacles, it is very likely that victims will not receive the randomly constructed fake RREP packets. Therefore, many victims only experience a very short intrusion time. It is very hard for this type of 'partial' victims to detect intrusions, resulting in low detection ratio. As stated before, the low detection ratio does not necessarily mean inefficiency of detection engines in this special case.

7.4.3. MTFA. From Figure 12, we can see that the MTFA increases with the increase of the link change rate. In terms of MTFA, the three models exhibit trivial differences. In comparison with the results in Figure 9, link change rates are more accurate than mobile speed in capturing the dynamics of networks.

DOI: 10.1002/dac

7.5. Simulation study of adaptive and non-adaptive IDSs

We mix the training data of the RW model and the RD model at different mobility levels together to construct an adaptive IDS. We use this adaptive IDS to measure traces of the RW model and RD model. Because the OM model demonstrates different behaviour, we treat it separately. The results of adaptive IDSs for the RW model and the RD model are illustrated in Figures 13–15. The results of adaptive IDSs for the OM model are illustrated in Figures 16–18.

7.5.1. Adaptive IDSs under the RW model and the RD model. The performance of the RW model is very similar to that of the RD model when the link change rate is used as the metric. Therefore, we only display the performance of the RW model.

From Figure 13, we can see that at the same link change rate, the false positive ratio of adaptive IDS is lower than that of IDS not using adaptive mechanism. This phenomenon is especially true at large link change rate. Adaptive mechanisms take into consideration mobility-caused dynamics and can change normal profiles correspondingly, enabling the IDS to suit the

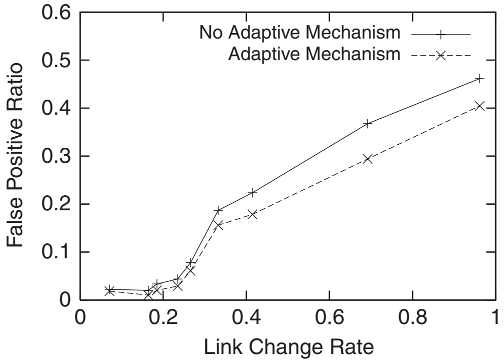


Figure 13. False positive ratio.

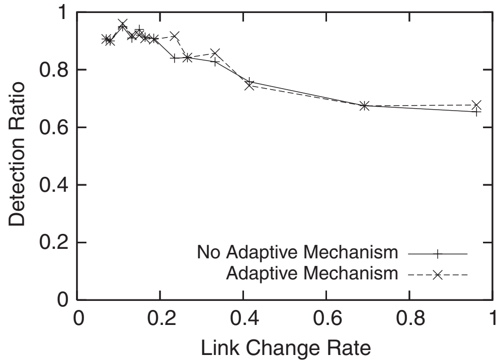


Figure 14. Detection ratio.

DOI: 10.1002/dac

environment better. False positives, which are the main concern when deploying IDSs in reality, can be reduced correspondingly.

We can see that detection ratios with and without adaptive mechanisms do not show much difference, as illustrated in Figure 14. Although in theory, if the IDS can model the normal

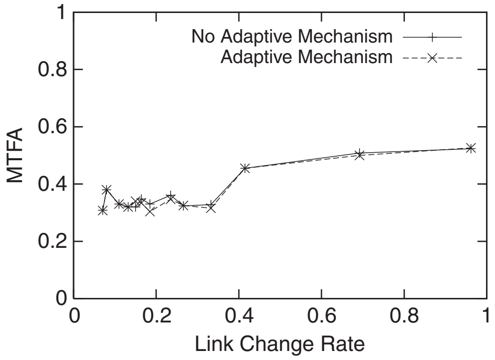


Figure 15. MTFA.

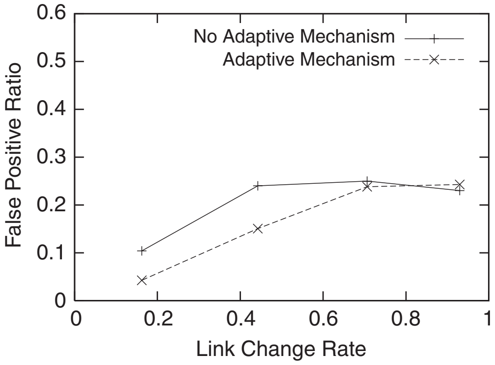


Figure 16. False positive ratio.

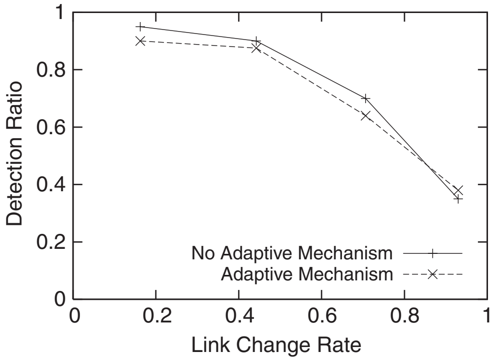


Figure 17. Detection ratio.

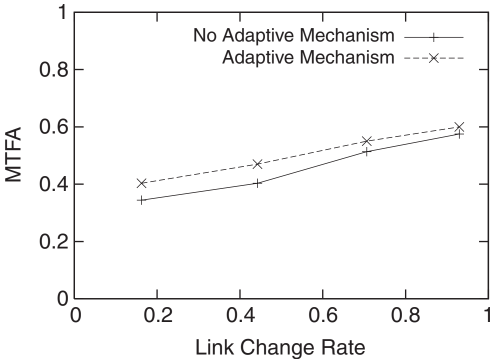


Figure 18. MTFA.

behaviour accurately by using adaptive mechanisms, it should be able to detect more intrusions. Unfortunately, we find this is not really true for our detection engine. When attacks happen in the network, abnormal routing table changes do not expect to follow any normal profiles. The *adaptive* mechanism does not enable the abnormal changes caused by the attack to be found in any normal profiles. This is the main reason that adaptive mechanisms are not helpful in improving detection ratio for our detection engine. Because of the similar reason, MTFA with and without adaptive mechanisms does not show much difference, as illustrated in Figure 15.

To summarize, the main benefit of the adaptive mechanisms to our detection engine is to lower the false positive ratio, while keeping roughly the same performance in terms of detection ratio and MTFA.

7.5.2. Adaptive IDS under the obstacle mobility model. As shown in Figures 16–18, the OM model behaves differently at high link change rates. From the following performance results, however, the same conclusion that adaptive mechanisms can reduce false positive ratio still holds.

We can see from Figure 16 that for the OM model, the false positive ratio of adaptive mechanisms is lower than that of non-adaptive mechanism. The reason is similar: adaptive mechanisms integrate mobility-caused dynamics and can adjust the normal profiles correspondingly, resulting in lower false positive ratio.

We can also see from Figures 17 and 18 that for the OM model, the detection ratio and MTFA of the adaptive mechanisms and the non-adaptive mechanism do not show much difference. The reason is similar as in the previous section. This again illustrates that the main advantage of the adaptive mechanisms is to decrease the false positive ratio, while keeping roughly the same detection ratio and MTFA.

8. CONCLUSIONS AND FUTURE WORK

Conclusions and future work are summarized as follows.

DOI: 10.1002/dac

8.1. Conclusions

Constructing effective MANET IDSs is a challenging task. The dynamics incurred by mobility make it hard to build the normal profiles for MANETs. Capturing the impact of mobility on IDS performances is a critical step in building effective IDSs for MANETs. This paper presents our initial effort in this direction. Specifically, we first introduce two different approaches, the Markov chain-based approach and the Hotelling's T^2 test based approach, to construct local IDSs for MANETs. They utilize the ordering property and frequency distribution, respectively, to build the normal profiles of MANET routing activities. Both approaches are effective when the mobility is low. Based on the Markov chain-based approach, we then investigate the impact of mobility models on the performance of MANET IDSs. Utilizing different mobility models, we first demonstrate that nodes' moving speed is not a good metric in measuring the performance of MANET IDSs. False positive ratio, detection ratio, and MTFA of MANET IDSs have different characteristics under different mobility models when speed is used as the metric. We then propose a unified measurement metric, link change rate, to capture the impact of mobility on IDS engines. Simulation results demonstrate that the performance of MANET IDSs in terms of the false positive ratio, detection ratio, and MTFA is less dependent on mobility models if the link change rate is used as the metric.

Based on the link change rate, we further propose how to integrate adaptive mechanisms to construct local MANET IDSs. By selecting the properly trained normal profiles at different mobility levels, our proposed adaptive MANET IDSs are more suitable for the MANET dynamics. Using the routing disruption attack as the threat model, we demonstrate that our proposed adaptive mechanisms can further decrease the false positive ratio, while keeping roughly the same detection ratio and MTFA.

8.2. Future work

First, the performance of MANET IDSs at high mobility levels is still not as good as expected. For example, under the RW and OM mobility models, MANET IDSs at high mobility levels still suffer from a high false positive ratio. It is a challenging task to reduce the false positive ratio because the mobility-induced errors at high mobility levels make it hard to distinguish between normal activities and malicious activities. More effective features and alert aggregation/correlation mechanisms may provide solutions to this problem. Second, because of the various existing mobility models, it is very challenging to construct mobility-independent MANET IDSs. More interesting mobility models can be simulated and experimented in the future to watch their impacts on the performance of MANET IDSs. In this way, we can extract better mobility-independent features. Third, how to test IDS performance comprehensively is still our ongoing research work. Currently, there still lack a comprehensive and scientifically rigorous methodology to test the effectiveness of existing IDS systems [26]. This situation is worse in the context of MANETs, which is still a relatively new communication paradigm compared to traditional wired networks. In this paper, we only adopt the most commonly used metrics and measure the performance of our schemes based on simulation. Future work needs to systematically test the performance of MANET IDSs based on real experiment. Fourth, in the OM model, we clearly see the impact of the obstacles on the IDS performance. In this paper, we only use one particular obstacle setting. More work is needed to measure the various deployments of obstacles and their impacts on IDS performance.

DOI: 10.1002/dac

ACKNOWLEDGEMENTS

This research was supported in part by the Texas Advanced Research Program under grant 003581-0006-2006.

REFERENCES

1. Zhang Y, Lee W. Intrusion detection in wireless ad hoc networks. *The 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, August 2000; 275–283.
2. Sun B, Wu K, Pooch U. Routing anomaly detection in mobile ad hoc networks. *12th International Conference on Computer Communications and Networks* (*ICCCN'03*), Dallas, TX, October 2003; 25–31.
3. Montgomery DC. *Introduction to Statistical Quality Control*. Wiley: New York, 2005. ISBN: 0-471-65631-3.
4. Broch J, Maltz DA, Johnson DB, Yih-Chun Hu, Jetcheva J. A performance comparison of multi-hop wireless ad hoc network routing protocols. *Proceedings of ACM International Conference on Mobile Computing and Networks* (*MOBICOM'98*), Dallas, TX, U.S.A., October 1998; 85–97.
5. Jardosh A, BeldingRoyer EM, Almeroth KC, Suri S. Towards realistic mobility models for mobile ad hoc networks. *The 9th Annual International Conference on Mobile Computing and Networking*, San Diego, CA, 2003; 217–229.
6. Debar H, Dacier M, Wespi A. A revised taxonomy for intrusion-detection systems. *Annales des Telecommunication* 2000; **55**:361–378.
7. Anderson JP. Computer security threat monitoring and surveillance. *Technical Report*, James P. Anderson Co., Fort Washington, PA, April 1980.
8. Denning DE. An intrusion-detection model. *IEEE Transactions on Software Engineering* 1987; **13**(7):222–232.
9. Ko C, Fink G, Levitt K. Execution monitoring of security-critical programs in distributed systems: a specification-based approach. *Proceedings of 1997 IEEE Symposium on Security and Privacy*, Oakland, CA, May 1997; 134–144.
10. Kachirski O, Guha R. Intrusion detection using mobile agents in wireless ad hoc networks. *Proceedings of IEEE Workshop on Knowledge Media Networking* 2002; 153–158.
11. Samfat D, Molva R. IDAMN: an intrusion detection architecture for mobile networks. *IEEE Journal on Selected Areas in Communications* 1997; **15**(7):1373–1380.
12. Marti S, Giuli T, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. *The 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, August 2000; 255–265.
13. Huang Y, Fan W, Lee W, Yu PS. Cross-feature analysis for detecting ad-hoc routing anomalies. *Proceedings of the 23rd International Conference on Distributed Computing Systems*, Providence, RI, May 2003; 478–487.
14. Huang Y, Lee W. A cooperative intrusion detection system for ad hoc networks. *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks* (*SASN'03*), Fairfax, VA, October 2003; 135–147.
15. Stojmenovic I. Position based routing in ad hoc networks. *IEEE Communications Magazine* 2002; **40**(7):128–134.
16. Broch J, Johnson D, Maltz D. The dynamic source routing protocol for mobile ad hoc networks. February 2002, IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt
17. Ye N, Li X, Chen Q, Emran SM, Xu M. Probabilistic techniques for intrusion detection based on computer audit data. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 2001; **31**(4):266–274.
18. Zeng X, Bagrodia R, Gerla M. GloMoSim: a library for parallel simulation of large-scale wireless networks. *Proceedings of the 12th Workshop on Parallel and Distributed Simulations* (*PADS '98*), Banff, Canada, 26–29 May 1998; 154–161.
19. Sun B, Wu K, Pooch U. Alert aggregation in mobile ad-hoc networks. *ACM Wireless Security* (*WiSe'03*) *in Conjunction with ACM Mobicom'03*, San Deigo, CA, 2003; 69–78.
20. Wu K, Harms J. Performance study of proactive flow handoff for mobile ad hoc networks. *ACM/Kluwer Wireless Networks Journal* (*ACM WINET*) 2006; **12**(1):119–135.
21. de Berg M, van Kreveld M, Overmars M, Schwarzkopf O. *Computational Geometry: Algorithms and Applications*. Springer: New York, 2000. ISBN: 3-540-61270-X.
22. Linde Y, Buzo A, Gray RM. An algorithm for vector quantizer design. *IEEE Transactions on Communications* 1980; **28**(1):84–95.
23. Sun B, Wu K, Pooch U. Towards adaptive intrusion detection for mobile ad hoc networks. *IEEE Globecom 2004*, Dallas, TX, October 2004.
24. Su W, Lee SJ, Gerla M. Mobility prediction and routing in ad hoc wireless networks. *International Journal of Network Management* 2001; **11**(1):3–30.
25. Yih-Chun Hu, Johnson DB. Caching strategies in on-demand routing protocols for wireless ad hoc networks. *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking* (*MobiCom 2000*), ACM, Boston, MA, August 2000.
26. Mell P, Hu V, Lippmann R, Haines J, Zissman M. An overview of issues in testing intrusion detection systems. *NIST IR 7007*, National Institute of Standards and Technology, June 2003.

DOI: 10.1002/dac

AUTHORS' BIOGRAPHIES

Bo Sun received his PhD degree in Computer Science from Texas A&M University, College Station, U.S.A., in 2004. He is now an assistant professor in the Department of Computer Science at Lamar University, U.S.A. His research interests include the security issues (intrusion detection in particular) of Wireless *Ad Hoc* Networks, Wireless Sensor Networks, Cellular Mobile Networks, and other communications systems.

Kui Wu received the PhD degree in computing science from the University of Alberta, Canada, in 2002. He then joined the Department of Computer Science, University of Victoria, Canada, where he is currently an Assistant Professor. His research interests include mobile and wireless networks, sensor networks, network performance evaluation, and network security.

Yang Xiao worked at Micro Linear as a medium access control (MAC) architect involving the IEEE 802.11 standard enhancement work before he joined the Department of Computer Science at The University of Memphis in 2002. He joined Department of Computer Science at The University of Alabama since 2006. He was a voting member of IEEE 802.11 Working Group from 2001 to 2004. He is an IEEE Senior Member. He currently serves as Editor-in-Chief for *International Journal of Security and Networks* (*IJSN*) and for *International Journal of Sensor Networks* (*IJSNet*). He serves as an associate editor or on editorial boards for the following refereed journals: *International Journal of Communication Systems* (*Wiley*), *Wireless Communications and Mobile Computing* (*WCMC*), *EURASIP Journal on Wireless Communications and Networking* (*WCN*), and *International Journal of Wireless and Mobile Computing* (*IJWMC*). He serves as a guest editor for *IEEE Wireless Communications*, special issue on Radio Resource Management and Protocol Engineering in Future Broadband and Wireless Networks in 2006, a (lead) journal guest editor for the IJSN special issue on security issues in sensor networks in 2005, a (lead) journal guest editor for the EURASIP WCN special issue on wireless network security in 2005, a (sole) journal guest editor for *Computer Communications journal* (*Elsevier*) special issue on energy efficient scheduling and MAC for sensor networks, WPANs, WLANs, and WMANs in 2005, a (lead) journal guest editor for the WCMC (Wiley) special issue on mobility, paging, and quality of service management for future wireless networks in 2004, and as a (lead) journal guest editor for the IJWMC special issue on medium access control for WLANs, WPANs, *ad hoc* networks, and sensor networks in 2004. He serves as a referee/reviewer for many funding agencies, as well as a panelist for NSF and a member of Canada Foundation for Innovation (CFI)'s Telecommunications expert committee. He serves as TPC for more than 70 conferences such as INFOCOM, ICDCS, ICC, GLOBECOM, WCNC, etc. His research areas are wireless networks, mobile computing, and network security. He has published more than 140 papers in major journals and refereed conference proceedings related to these research areas.

DOI: 10.1002/dac

Ruhai Wang received a PhD degree in Electrical Engineering from New Mexico State University, U.S.A., in 2001. He currently serves as an assistant professor in Department of Electrical Engineering at Lamar University, Texas. His research interests include computer networks and communication systems with emphases on wireless communications, wireless and space Internet, network protocols and security, and performance analysis. He has published numerous papers in international journals and conferences proceedings. He is serving as an editorial board member of Wireless Communications and Mobile Computing (WCMC) Journal. He has also served as a TPC co-chair and member for major international conferences and workshops.

DOI: 10.1002/dac