Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks

Peyman Kabiri and Mehran Aghaei
(Corresponding author: Peyman Kabiri)

Intelligent Automation Laboratory, School of Computer Engineering, Iran University of Science and Technology
University Road, Hengam Street, Resalat Square, Narmak, 16846-13114 Tehran, Iran
(Email: peyman.kabiri@iust.ac.ir, mehran_6280@yahoo.com)
(Received Sept. 2, 2009; revised and accepted Nov. 15, 2009)

Abstract

As Mobile Ad-hoc network (MANET) has become a very important technology, research concerning its security problem, especially, in intrusion detection has attracted many researchers. Feature selection methodology plays a central role in the data analysis process. The proposed features are tested in different network operating conditions. PCA is used to analyze the selected features. This is because, redundant and irrelevant features often reduce performance of the detection system. Performance reduction will occur both in speed and predictive accuracy. This paper aims to select and analyze the network features using principal component analysis. In this paper, performing various experiments, normal and attack states are simulated and the results for the selected features are analyzed.

Keywords: Feature selection, intrusion detection, MANET, PCA

1 Introduction

Mobile Ad-hoc Network (MANET) is an unstructured wireless network that can be established temporarily, e.g. applications for MANET may include deployment in battle field, small offices of universities. Each node is selfish and independent in the decision making. In MANET, nodes can add-in to the network or detach from it at any time. Thus, there is no central control on the network for the nodes to follow [20]. Intrusion detection models were introduced by Denning in 1987 and rather are a new technology [5, 20].

Intrusion detection systems can be categorized into two models: Signature-based intrusion detection [2] and anomaly-based intrusion detection. Signature-based intrusion detection uses signatures of the attacks to detect the intrusion. This type of detection monitors the network for finding a match between the network traffic and a known attack pattern. On the other hand, anomaly-based intrusion detection creates a profile based on the normal behavior of the network [23, 25]. In this approach, system monitors the network and detects the anomalous behaviors within it. In this method, detection is performed by learning the normal behavior of the network and comparing it versus the behavior of the monitored network. The advantage of the anomaly-based detection is its ability to detect new attacks without any prior knowledge about it [5].

This paper purposes a neighbor monitoring intrusion detection based on the traffic profile of the node, where feature selection is used to improve its performance. The proposed approach uses the anomaly-based intrusion detection method. In Ad-hoc networks, packets that are sent from each node can be used for network condition monitoring. Using the traffic data, behavior of the node's neighbor can be monitored. In the reported work, 16 features in the network traffic are monitored. This paper, intends to show the difference between the normal operating state of a network and the operating state of the network once it experiences a DoS attack. In the anomaly-based intrusion detection, the profile of the network in its normal state of operation is initially extracted. Later on, this profile is compared versus the current state of the network. Detecting any deviation from the normal state of operation in the network, system will produce an alarm message to show the anomalous behavior. Intention is to analyze these parameters in different working conditions in order to find the most stable features in the network for this purpose. To do so, various operating conditions for network traffic in both normal and attack states are simulated.

The reported work intends to reduce the dimensionality of the network features. This reduction may lead to increase in intrusion detection speed, since the IDS would have fewer features to analyze. Network features such as movement and number of the nodes are also considered in the reported work.

This paper is organized in the following way: Section 2 presents solutions for intrusion detection systems (IDS)

in mobile Ad-hoc networks. Section 3 describes the techniques and protocols used in this work. These techniques include PCA and profile-based IDS. Dynamic source routing (DSR) is the protocol used in the proposed scheme. Section 4 explains the simulation environment for the proposed scheme and the data collection methodology used in this work. Section 5 describes the analysis of the simulations results. Section 6 provides conclusions and Section 7 describes future works.

2 Related Works

The first solution for IDS in MANET was proposed by Zhang et al. [26]. In their paper, they proposed two important solutions, i.e. anomaly-based and signature-based detection. The work detects attacks using anomaly-based intrusion detection. Implementing this kind of detection, moving speed of the nodes, their distance, rate for the rout change, hop counter parameters were used. In signature-based intrusion detection, a pre-prepared rule is used to detect an attack.

In a work reported by Hu et al., an approach based on digital signatures was used to detect rushing and wormhole attacks [11, 12].

In a work reported by Huang et al., a new anomaly-based intrusion detection system capable of detecting new attacks is introduced [13]. They introduced a new data mining method that performs "cross-feature analysis" to capture the inter-feature correlation patterns in normal traffic. This paper does not present a solution for detecting intrusions [13]. Huang et al.'s reported work can detect type and source of the attack [14]. This is achieved by exchanging monitored data between neighboring nodes.

In a reported work by Gilham et al., a rule-based intrusion detection system named IDES is introduced [19]. IDES learns users' behavior and uses misuse detection approach. Alerts are generated once a suspicious activity that deviates significantly from the established normal usage profiles is detected.

In a work reported by Kim et al., they have developed a real-time intrusion detection system which combines online feature extraction method with least squares support vector machine classifier [17]. They have used DARPA99 (KDD 99) dataset for the experiments and there is no simulation environment used in this work.

In a work reported by Farid et al., a new approach for intrusion detection based on adaptive Bayesian algorithm is proposed. This algorithm classifies different types of attacks included in KDD 99 benchmark intrusion detection dataset [7].

In a work reported by Wang et al., C4.5 decision tree classification method is used to build an effective decision tree for intrusion detection. Later on, the decision tree was converted into rules and was saved in a knowledge base of an intrusion detection system. These rules are used to judge whether the new network behavior is normal or not [7].

In a work reported by Ye et al., a distributed IDS in network layer is proposed for the MANET [25]. In a work reported by Denning et al., a new survey in IDS system is reported [5]. This paper categorizes IDS into three models: signature-based IDS, anomaly-based and feature-based IDS. The set of normal work specifies base model in the feature set and detects attacks monitoring deviation from this model. Thus this method can detect new attacks. In a work reported by Richeldi et al. [21], a genetic algorithm is proposed to select effective features. This method is very slow. Another feature selection is proposed by Chen et al., in which they utilize three feature selection algorithms. They use an SVM classifier [4] and two multi-labels [3].

In a work reported by Wang et al., Markov Blanket algorithm is applied on the feature selection part of an intrusion detection method [24]. In this approach, Markov Blanket algorithm can decrease the number of features.

This paper intends to find effective features in detecting intrusions in *MANET*. None of the above works present a method to measure effectiveness of the features and a way to find and select them.

3 The Proposed Techniques and Protocols

There are many techniques that can be used for monitoring the nodes and analyzing the results. In the proposed method of approach, a profile-based monitoring technique and the Principal Component Analysis (PCA) technique are implemented. Network performance is dependent on the selected routing protocol. For the same reason, the DSR protocol is used in this work.

3.1 Profile-based Neighbor Monitoring IDS

This paper proposes a profile-based intrusion detection system for wireless Ad-hoc networks [24]. In the proposed IDS, each node builds a profile for every one of its neighbors [18]. The profile includes all features listed in Table 1. The data packet size indicates the packet type. They are all traffic related features [10].

A node can use a profile by keeping it to monitor its neighbor node's behavior. This paper simulates this technique on a number of selected features in a simulation environment.

3.2 Principal Component Analysis

PCA is used to analyze results of the scenario-based Ad-hoc network simulations [10]. Simulation output is in comma-separated vector (CSV) format.

PCA is a classic technique in statistical data analysis, feature extraction and data compression. Goal is to find a smaller set of variables in a set of multivariate measurements with less redundancy.

Table 1: Networks feature

Features	1. My address 2. Destination address 3. Route REQuest (RREQ) from node I 4. Route REPly (RREP) from node I 5. Route error from node I 6. Total packet received from node I 7. My received sent packet 8. ACK packet from node I 9. Traffic sent from node I 10. Total received RREQ, 11. Total RREP 12. Total received (Route Request ERror) RRER 13. Total Traffic received, 14. Total ACK received, 15. Timestamp 16. DSR header

The starting point for PCA is a random vector x with n elements. There are available samples $x(1)$ ... $x(T)$ from this random vector. No explicit assumptions on the probability density of the vectors are made in PCA, as long as the first and the second-order statistics are known or can be estimated from the sample [6]. No generative model is assumed for vector x. Typically the elements of x are measurements like pixel gray levels or values of a signal at different time instants [16].

In the PCA transform, the vector x is first centered by subtracting its mean [9, 16]:

$$x \longleftarrow x - E\{x\}.$$

In practice, the mean is estimated from the available sample $x(1) \ldots x(T)$.

The matrix X is a $n \times n$ covariance matrix of x.

$$C_x \longleftarrow E\{xx^T\}.$$

It is well known from basic linear algebra that the solution to the PCA problem is given in terms of the unit-length eigenvectors $e_1, e_2, \ldots, e_n$ of the matrix C_x. The ordering of the eigenvectors is such that the corresponding eigenvalues d_1, ..., d_n satisfy $d_1 \geq d_2 \geq \ldots \geq d_n$.

Thus the first principal component of x is

$$y_1 = e_1^T x.$$

3.3 DSR Protocol

DSR is an active routing protocol that is implemented based on source routing [15]. The header of the packet has a list of nodes addresses to pass it in source routing. At first, source route discovers the path to the source node. Using this method prevents the route to follow a cyclic path. Middle nodes of this routing do not need to collect latest nodes status such as sequence number unlike AODV. All nodes can listen to the packets in the DSR routing network. Nodes can update the routing information in cache table based-on available paths in packet header for further usages. This routing protocol does not need to use HELLO packets [22]. This paper intends to use this protocol because of the aspects such as Nodes ability to sniff packets in the network [8].

4 Implementation

This paper implements the networks to monitor the features and evaluate the selected feature and analyze networks. There are more than 80 scenarios that show normal and attack networks with parameters as described in Table 2. Since these 80 scenarios have similarities in their behavior, only a selected number of them are reported in this paper. For example, in a scenario with 20 nodes, voice over IP (VOIP-PCM) traffic, fast movement is simulated. An experimental network is implemented for experimenting with different scenarios. Networks test run was for 180 seconds. Radio signal radius is 250 meters for all nodes. The implementation area is 2000m * 2000m in size. The network topology is WLAN (infrastructure). All the scenarios were implemented in the simulation environment.

4.1 Data Collection

This paper intends to answer the following three questions. Question number one: why features listed in Table 1 are good candidates? Question number two: is this feature a proper one? Or how it can be evaluated? Question number three: which feature is appropriate?

This section will explain why the selected features are the right candidates. Selected features are described here.

1) My address:
It shows the source addresses. This feature is applied to specify the intruder or the misbehaved node.

2) Destination address:
Destination address is selected to specify nodes that are under attack.

3) RREQ from node I:
Some Denial of Service (DoS) attack methods attack other nodes by sending a lot of route request. Therefore, route request feature is selected to specify how many Route Requests is sent.

4) My sent packet:
This feature shows selfish behavior of the nodes. Assume a node that wants to send a packet to destination B, but there is no straight path from the node A to B. Therefore, it sends a Route Request to its neighbors. Let node X receives the packet and forwards it to other nodes. Since the node A is a neighbor of the node X, the forwarded packet is sent to node A as well. This feature specifies neighbor behavior. This

is needed because neighboring node may not forward the packet.

Other features are also selected to specify neighbor's behavior. Nodes monitor the whole received traffic. This traffic is received from neighboring nodes. Each node monitors these features from the network traffic.

Network traffic can be monitored by changing the DSR protocol. In the simulation environment a logger function was added to the DSR protocol, so that, it can log the feature values. A sampling rate of 1 second is selected in DSR protocol for the network. Later on, features are extracted and recorded for each network scenario. The collected dataset is stored in comma-separated text files, different files for different scenario. Next step is to analyze and evaluate dataset for the scenarios. PCA theory is used for the analysis, reduction dimension and evaluation of features. All the features are normalized (zero mean and unit variance). Then covariance matrix is calculated. Covariance matrix is a n*n matrix. Features dependency is shown in this matrix. PCA (as described in Section 3.2) is applied on the covariance matrix.

4.2 Scenarios

In this section, three scenarios are presented. This work uses a profile-based feature selection.

4.2.1 Scenario 1

A normal state of operation for a network is a state that presents the normal daily operation of the network once it is not under any kind of attacks. Different types of network traffics are generated in network. Node movements in some networks are made to be fast or slow. Nodes are made static or dynamic. In this network, distances between nodes are variable.

Network parameters used in this work are presented in Table 2. Networks are simulated in the simulation environment and feature values are recorded for different combinations of the network parameters (Table 2).

A sample network may include 20 nodes with VOIP (GSM) traffic. The nodes in this network are pervaded in 2000*2000 square meter area and these nodes can move as fast as 200 meters per second. Distant nodes are very few, and nodes are within the transmission radius of several nodes. Other networks are implemented using same parameters as in Table 2.

Network operation is tested and simulated in various operating conditions and its operating profile was stored in different profile files.

DoS attack is described in the following section and then some attack scenarios are explained.

4.2.2 DoS Attack

DoS attack is divided into two categories. In the first category, one intruder attacks other nodes in the Ad-hoc network services and does not let them to provide their services. In the second category, this attack is a distributed attack and more than one intruder performs attack on the other nodes [1].

Table 2: Network parameters

Number of Nodes	20-50
Traffic type	Voip (gsm)-Voip (pcm)-video conference high quality-video conference (low quality)
Nodes movement	Random way point (fast-static-low)
Nodes distances (density)	Far-close

This is called Distributed DoS (DDoS) attack. Because of the inherent limitations of MANET's routing protocols various types of DoS and DDoS are possible. The attack initiates or forwards fake Route Requests (RREQs) that lead to forcefully allocating network resources and forcing denial of service to genuine nodes. As mentioned earlier, the default value of RREQ rate is limited to 10 RREQs/sec. This means that each node is expected to observe some self-control on the number of RREQs that it sends in one second. A compromised node may choose to set the value of parameter RREQ_RATELIMIT to a high number or even disable this limiting feature. Thus compromised nodes allow their system to send large number of RREQ packets per second. The proposed scheme transfers the responsibility of monitoring this parameter to the node's neighbor. This problem is caused due to the flooding of RREQs from a compromised node.

4.2.3 Scenario 2

Denial of Service (DoS) is simulated in this scenario. In DSR protocol, a malicious node overrides the restriction by increasing or disabling RREQ_RATELIMIT (limit for initiating/forwarding RREQ per second). A node can change this parameter. This is possible since it has authority over this parameter. A compromised node chooses the value of RREQ_RATELIMIT parameter to a high number. This allows DoS to flood the network with fake RREQ rate and will lead to a kind of DoS attack. In this type of DoS attack, a non-malicious node cannot fairly serve the other nodes due to the network-load imposed by the fake RREQ rate. This leads to the following problems:

- Network bandwidth reduction.
- Node's processing time is wasted (more overhead).
- The network resources like memory (routing table entries) are wasted.
- The node's battery power is rapidly consumed.

Most of the network resources are wasted trying to generate routes to the unknown destinations or routes that are not going to be used for any communication. This implies that the existing version of DSR is vulnerable to such type of malicious behavior from an internal node (which is named a compromised node).

Intruder nodes are deployed in different areas, with different traffic and different node movement to find better results. This scenario is simulated and results are recorded in various profiles.

4.2.4 Scenario 3

Another kind of DoS attack is simulated in this scenario. It changes intruder's path manager parameters to send a large number of RREDs. This is implemented for two reasons. First reason is that the invisible cache is destroyed quickly. Thus, this node sends one RREQ for each data packet. Second reason is because the intruder tries to establish a random short time connection with other Ad-hoc nodes. This method of attack is tested in previous scenarios.

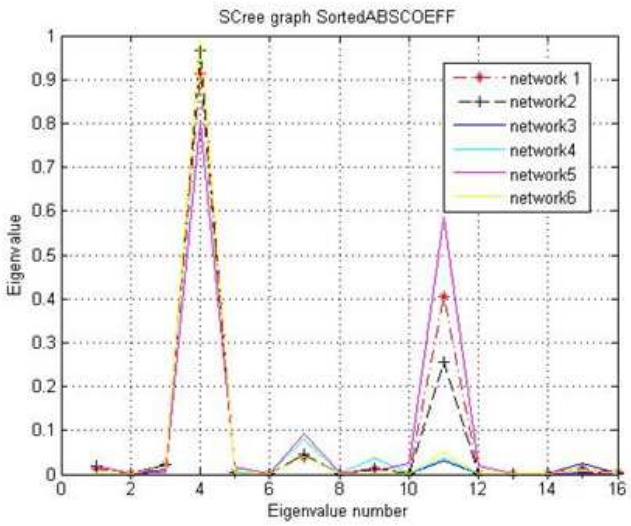

Figure 1: Network's six normal states of operation are presented with different colors

5 Analysis

Analysis for PCA outputs is presented in this section. The scenarios in Section 4.2 are simulated in various conditions (relevant to Table 2). Important features for various normal and abnormal states in Ad-hoc networks are described in the following sections. It is also shown that some features in normal state of operation are universal features and their values only experience small changes once the state of the operation for the network changes.

5.1 Experiment 1

There are 20 networks tested in this experiment. Since all the 20 networks have shown similar behaviors during the simulations, only 6 selected experiments are reported in this paper (Table 3).

These experiments implement the scenario one as it was explained earlier in this paper. In Figure 1, features are presented on the horizontal axis. Results from different network operation scenarios are presented by different colors in Figure 1.

Figure 1 shows that the 4th and the 11th feature, where the latter one is the most important one and has the maximum variance. This feature holds maximum information value among all other features in the network. Features are tested in 20 network scenarios. Networks are implemented using parameters in Table 2. Features 4, 11, 7 have 99.6%, 60% and 15% information value respectively. This means that, these features are static with respect to the network traffic type, density and other network parameters that have changing values. In the other words, normal states can be derived using these features. Using these features, normal states will have similar operating conditions regardless of the network traffic type. Thus definition of a universal normal state profile would be possible. In this figure, Features 4 and 11 represent received RREP from each node and total RREP received from all nodes.

When network operates in a normal state, nodes send RREQ to the other nodes with a fixed rate. But in different operating conditions it shows a low variation in its value. 14 first features show less variation than Feature 15. As for example, RREP sent from all adjacent nodes, have higher variations with respect to the timestamp (time).

Next step in this paper is about a DoS attack experiment implementing scenarios two and three.

5.2 Experiment 2

The kind of DoS that is tested in this section was described in Section 4.2.3. This attack is tested with various network traffics. Attacks are simulated and results are logged using parameters in Table 3. Network attacks are simulated using 30 parameters. Results for Networks 1, 2, 3, 4 and 6 are depicted in Figure 2.

As it is presented in this figure, DoS attack on different network traffics have a similar graph in this simulation. The 15^{th} feature is the most important one in these networks. Other features have lower variation than the 15^{th} feature. Feature 15 is the timestamp. Timestamp value is one second. It means that, other features have smaller variation in one second. This state show that the network traffic is in stall. At this state (state of attack), RREP and RREQ have smaller variations than in normal operating state. This shows that during a DoS attack, network features will have different behavior than when the network was operating in its normal state of operation.

Table 3: Networks status parameters

Traffic Type	Density	No. of Nodes	Nodes Movement	Network No.
Video conference heavy/light-voip (gsm/pcm)	high	20	slow	**1**
Voip(pcm-low quality)	high	20	slow	**2**
Video conference heavy/light-voip (gsm/pcm)	high	20	fast	**3**
low	high	20	fast	**4**
low	low	20	slow	**5**
low	high	50	fast	**6**

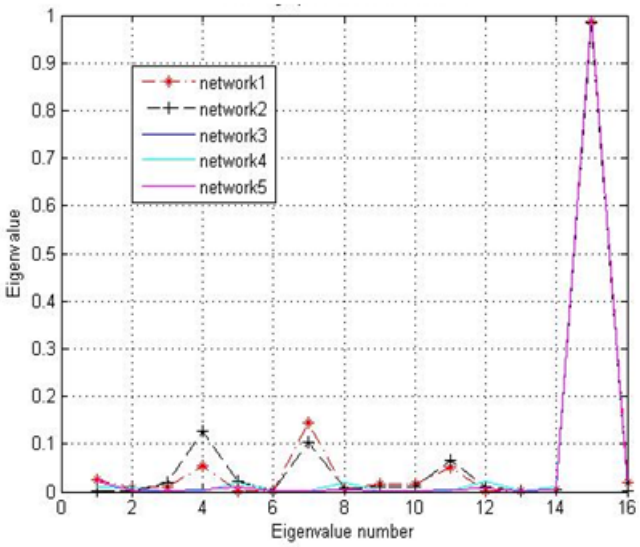

Figure 2: DoS attack Type 2. This type of DoS attack has a higher number of dynamic features than Type 1.

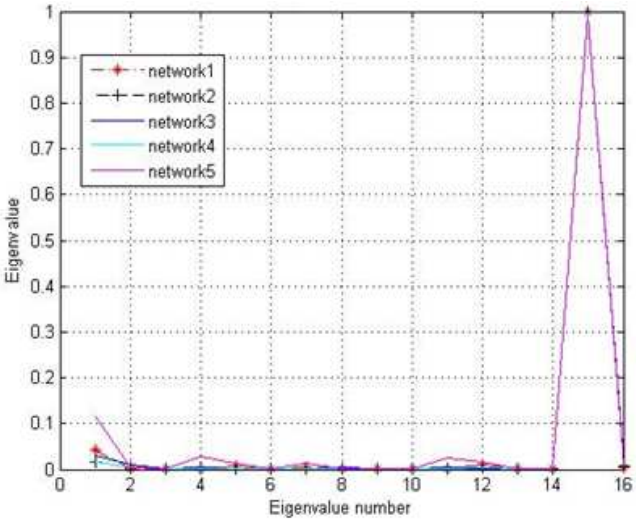

Figure 3: DoS attack Type 1. Feature 15 shows the highest variation in its value.

5.3 Experiment 3

Another DoS attack is simulated in this experiment. Similar to the previous experiments, parameters in Table 3 are selected for the profiling. A total number of 30 attack attempts are simulated. Results are depicted in Figure 3. As depicted in Figure 3, these types of attacks are similar to the previous attacks where Feature 15 was the most important feature. In comparison with Experiment 2, in Experiment 3, other network features become more active and hold a higher information value[1] (Figure 3). Feature 15 has the highest information value.

5.4 Experiment 4

In this experiment, Network 1 presents normal state, Network 2 presents DoS attack-type one and Network 3 shows a DoS attack-type two, all simulation results are depicted in Figure 4. This figure shows the following cases:

- Two types of DoS attack (as described in Experiments 3 and 4) are simulated in various networks. They display similar behaviors in all the networks and depicted graphs are similar.
- The normal state and the attack state show different parameters with completely different values. This difference shows that this feature can separate these two operating states.

[1]Higher variation

6 Conclusions

In this paper, a profile-based neighbor monitoring intrusion detection approach in MANET was presented. This approach is based on feature selection method and it applies PCA theory to determine network operating conditions. Best network parameters (features) to identify normal state of network operation are presented. 16 features are selected for test in these networks. PCA shows that it is not necessary to monitor all the features to identify the operating condition of the networks. Some features have more variation in their values than others, which makes them more valuable for network condition monitoring. Thus, this approach can reduce the overhead of monitoring the networks. A normal state of operation is

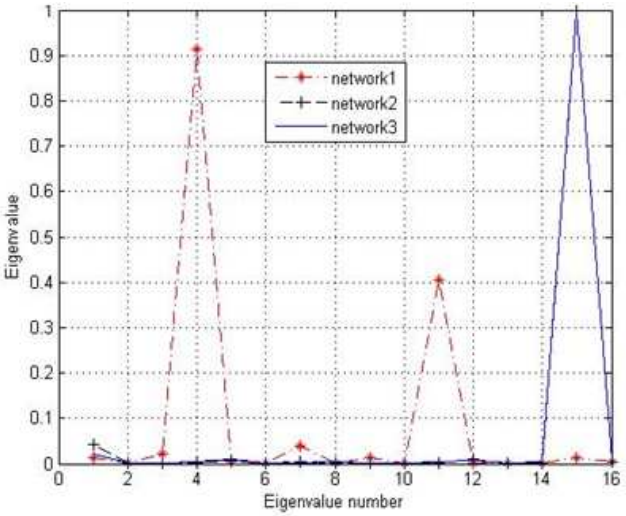

Figure 4: Normal state versus DoS attack. Show the different status

separated from the attack state by detecting deviation of certain feature values and selected parameters.

7 Future Works

In this paper, DSR protocol is selected as the route protocol. Ad-hoc On Demand Vector (AODV) can be also selected for the routing. This new protocol can be tested in the simulation environment. Another extension is feature selection on all network features that include both static features and traffic related features for intrusion detections.

References

[1] A. Agah, and S. K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145-153, 2007.

[2] F. Anjum, D. Subhadrabandhu, and S. Sarkar. "Signature-based intrusion detection for wireless Ad-hoc networks," *Proceedings of Vehicular Technology Conference*, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[3] W. Chen, J. Yan, B. Zhang, Z. Chen, and Q. Yang, "Document transformation for multi-label feature selection in text categorization," *Proceedings of Seventh IEEE International Conference on Data Mining*, pp. 451-456, USA, 2007.

[4] H. Deng, Q. A. Zeng, and D. P. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," *Proceedings of the IEEE Vehicular Technology Conference*, pp. 2147-2151, USA, 2003.

[5] D. E. Denning, "An Intrusion Detection Model," *IEEE Transactions in Software Engineering*, vol. 13, no. 2, pp. 222-232, USA, 1987.

[6] H. A. Edelstein, *Introduction to Data Mining and Knowledge Discovery*, Crows Corporation, Third Edition, 1999.

[7] D. M. Farid, and M. Z. Rahman, "Learning intrusion detection based on adaptive Bayesian algorithm," *11th International Conference on Computer and Information Technology (ICCIT2008)*, pp. 652-656, 2008.

[8] Y. K. Hassan, M. Hashim, A. El-Aziz, A. Safwat, A. El-Radi, "Performance Evaluation of Mobility Speed over MANET Routing Protocols," *International Journal of Network Security*, vol. 11, no. 3, pp. 101-111, 2010.

[9] H. Hotelling, "Analysis of a complex of statistical variables into principal components," *Journal of Educational Psychology*, vol. 24, no. 7, pp. 498-520, 1933.

[10] A. Hyv̈arinen, J. Karhunen, and E. Oja, *Independent Component Analysis*, John Wiley & Sons Inc., USA, 2001.

[11] Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad-hoc network routing protocols," *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 30-40, USA, 2003.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370-380, IEEE, 2006.

[13] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," *Proceedings of The 23rd International Conference on Distributed Computing Systems (ICDCS)*, pp. 478-487, USA, 2003.

[14] Y. A. Huang, and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN' 03)*, pp. 135-147, USA, 2003.

[15] D. B. Johnson, and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, pp. 153-181, Kluwer Academic Publishers, 1996.

[16] J. Karhunen, and J. Joutsensalo, "Generalizations of principal component analysis, optimization problems, and neural networks," *Neural Networks*, vol. 8, no. 4, pp. 549-562, 1995.

[17] B. J. Kim, and I. K. Kim, "Kernel based intrusion detection system," *Fourth Annual International Conference on Computer and Information Science (ACIS)*, pp. 13-18, USA, 2005.

[18] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on aodv-based mobile ad-hoc networks by dynamic learning," *International Journal of Network Security*, vol. 5, no. 3, pp. 338-346, 2007.

[19] T. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. Neumann, H. Javitz, A. Valdes, and T. Garvey, *A Real-time Intrusion Detection Expert System*

(IDES), Technical Report, Computer Science Laboratory, SRI International, 1992.

[20] P. Mohapatra, and S. V. Krishnamurthy, *Ad-hoc Network Technologies and Protocols*, Springer-Verlag, Business Media Inc., USA, 2005.

[21] M. Richeldi, and P. L. Lanzit, "A tool for performing effective feature selection," *Proceedings eighth IEEE international conference on tools with Artificial Intelligence*, pp. 102-105, 1996.

[22] E. Royer, "A review of current routing protocols for ad-hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, pp. 46-55, 1999.

[23] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwary, H. Yang, and S. Zhou, "Specification-based anomaly detection: A new approach for detecting network intrusions," *Proceedings of the 9th ACM Conference on Computer and Communication Security*, pp. 265-274, USA, 2002.

[24] X. Wang, T. L. Lin, and J. Wong, *Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network*, Technical Report, Computer Science, Iowa State University, USA, 2005.

[25] N. Ye, S. M. Emran, X. Li, and Q. Chen, "Statistical process for computer intrusion detection," *Proceeding in DARPA Information Survivability Conference and Explosion (DISCEX'01)*, vol. 1, pp. 3-14, USA, 2001.

[26] Y. Zhang, and W. Lee, "Intrusion detection on wireless ad hoc networks," *Proceedings 6th Annual International Conference on Mobile Computing and Networking (MobiCom' 00)*, pp. 275-283, USA, 2000.

Peyman Kabiri received his PhD in Computing and MSc in Real time Systems from the Nottingham Trent University, Nottingham-UK in years 2000 and 1996 respectively. He received his B.Eng. in Computer Hardware Engineering from Iran's University of Science and Technology, Tehran-Iran in 1992. He was with the Faculty of Computer Science/ University of New Brunswick as project coordinator from early September 2004 until the end of September 2005. His previous academic positions were as follows: Assistant professor in Department of Computer Engineering Iran's University of Science and Technology (where he is currently an assistant professor) and Assistant Professor in Azad University - central branch - Faculty of Engineering both in Tehran-Iran. His research interests include Machine Learning, Remote Sensing, Robotics and Network Intrusion Detection.

Mehran Aghaei is a M.SC student at Iran's University of Science and Technology. He received his B.S. in computer software engineering from Azad University, Sari 2006. His research interests include intrusion detection in wireless Ad-hoc networks. His M.Sc. thesis was about intrusion detection on Ad-hoc networks. In his work, he simulates networks to observe their features and to classify their operating conditions. He is currently working at the Hadaf and Payamnoor University as a lecturer. He teaches algorithm processing and internet engineering. He has other industrial engagements as well.