A New Method based on Finite State Machine for Detecting Misbehaving Nodes in Ad hoc Networks

Dina Sadat Jalali, Alireza Shahrbanoonezhad
Islamic Azad University
Dehloran Branch
Dehloran, Iran
{jalali_ds, alireza_shahrbanoonezhad}@yahoo.com

ABSTRACT: *In this paper we express a new intrusion detection system based FSM (Finite State Machine) in ad hoc networks. Security is one of the most important issues in current networks. The most common cases of attacks in mobile Ad hoc networks can be drop of routing packages and changes in the incoming packet which aims at disrupting the network routing and overall network reduce performance. The presented approach based on FSM focuses at recognizing the malicious nodes within the network in a fast and accurate way, then it deals with rapid introduction of the malicious nodes to other nodes in the network to prevent sending multiple packets and drop and packet change. Finally, we will show the significant improvement of some factors in comparison with other last works and we simulated our methods by NS2 software.*

Keywords: Intrusion Detection, FSM, Ad hoc Network, Security, Malicious node

Received: 17 November 2011, Revised 31 December 2011, Accepted 5 January 2012

1. Introduction

An Ad hoc network is a wireless network without fixed infrastructure so it can be setup and used easily. Also all the computers in such network should be in the radio range of each other to make communication [1, 2]. These networks along with positive attributes, they also have disadvantages that include: Memory limitation, bandwidth limitation, lowlevel processing power and also limitation of nodes lifetime. All of this, along with features of media between nodes (radio frequency), has led the network to be vulnerable [2, 10].

Routing is the most important Problem in ad hoc network which is done by network nodes in a distributed way. An issue that may be difficult for the routing is the existence of a malicious node between nodes at the network. Due to nodes mobility, the network has a variable topology, so routing at these networks is more difficult than other networks routing and requires its own Routing algorithm.

On the other hand, the proposed routing algorithms for this network have low level of security and also no action has been performed to protect the network against attacks [4]. Hence, in recent years some solutions have been presented to provide the network security. Routing in these networks is very important and routing protocol for the ad hoc networks can be divide to three types described in [16,17]:

1.1 Proactive protocol

In this protocol, routing information to reach all the other nodes in a network is always save in the routing table at each node. When the network topology changes, many of routes will change and update the routing table at every node which causes

increasing the networks overhead. An example of proactive protocols is FSR (Fisheye State Routing) protocol [18].

1.2 Reactive protocol

In this protocol, discovering a route will be done just when a node wants to send data to another node in the network. When a route is discovered, it will be stored in the temporary cache at the source node until an event occurs in the network that imposes a need to new route discovering. Overhead of this protocol is less than proactive protocol. Examples of reactive protocols are DSR (Dynamic Source Routing) protocol [19] and AODV (Ad hoc On Demand Distance Vector) protocol [16].

1.3 Hybrid protocol

A proactive protocol for a large network needs a large routing table at every time, thus, it is not useful for a large network. On the other hand, due to route discovery, a reactive protocol for a large network has delay. Thus, using a protocol which combines both reactive and proactive protocol may be a better solution for Manet. An example of hybrid protocols is ZRP (Zone Routing Protocol)[20].

Each of the designed intrusion detection systems based on location and status of the network presents a special solution and has some advantages and disadvantages. The proposed method tries to considers the restrictions of the ad hoc network and number of common network attacks to present solutions in any location and position. The reminder of this paper is organized as follows: the first section presents the introduction. The second section presents the related works. Next we present the problems of previous intrusion detection systems in the third section. In fourthsection, we describe designing and mode of operations of our method. In fifth section, we show the simulation results of our method resulted from NS2 software. Finally, sixth section draws a conclusion.

2. Related Work

Intrusion detection systems in the Ad Hoc networks are generally divided into several categories from different viewpoints. The most important ones of the mentioned systems are as following: host based intrusion detection and network based intrusion detection. The rest of the paper expresses some of their features and functionality [5, 6].

2.1 Host based intrusion detection system (HIDS)

In these systems a technique is presented to detect intrusion. Also the intrusion detection technique is saved by each node and runs independently. Each decision about the suspicious network nodes will be made based on data collected only by the corresponding node and no cooperation between network nodes will exist for this matter [7, 8]. So no any kind of control and security information between network nodes will be sent. According to the structure of the intrusion detection systems and the method for identifying them, it'll be much better to use them in Flat networks than using them in Multi layer networks.

2.2 Network based intrusion detection system (NIDS)

In this system, detecting attacks and malicious actions are done by a group of neighboring nodes by their cooperation between each other. Usually clustering techniques are used to implement existing models in this category such that a node will be selected as the inter cluster supervisor. The supervisor monitors the performance of existing nodes in the cluster and detects the malicious nodes of the cluster by using received information from the nodes existing in its area. Thus, suspected nodes within other cluster nodes will be found. In addition, the supervisor node is in charge of sending attack warning message to other clusters by communicating with other supervisor nodes of adjacent clusters [9, 10].

A combination of the HIDS and NIDS can be used to discover attacks at the ad hoc network. This combination is a powerful and distributed intrusion detection system. In this system, the exchanged packets in the network and also data collected from the network nodes are considered as a basis for intrusion detection. Each of intrusion detection systems use the following techniques to detect attacks at Ad hoc network [11, 15].

2.2.1 Anomaly detection Technique

In this technique, using all the normal activities of the network, a model of normal network behavior is obtained such that any deviation from this normal network behavior model is diagnosed as a Network attack if it is more than a certain threshold. In this technique, the normal network behavior model should be updated in the specified time intervals. Using of this technique for Ad hoc networks is more cost effective.

2.2.2 Signature detection or Misuse detection Technique

This technique detects the attack by comparing current system behavior with the model of an attack. These models are called

signature and are predetermined and saved in the system database. The advantage of this technique is reporting the kind of attack if it detects an attack. One of the disadvantages of this technique is the ability of detecting just one of the known intrusions and cannot identify new attacks over the network. In this situation, the Network Manager should add the model of new attacks to the intrusion detection system.

Architecture used for intrusion detection systems in Ad hoc networks are introducing at the rest of the paper.

2.2.2.1 Stand-alone IDS

In this architecture an intrusion detection system is to be installed on each node. Then the mentioned system discovers the occurred attack to the node according to data collected from that node. In this intrusion detection architecture the nodes do not participate and cooperate with each another to detect attacks. Clearly this kind of intrusion detection architecture is not suitable for Ad hoc networks because the information of each node is not sufficient to detect intrusion [12, 13].

2.2.2.2 Distributed and Cooperative IDS

In the Ad hoc network, IDS systems must be Distributed and Cooperative to work together well and satisfy the need of Ad hoc network. In this architecture, each node in the network has its own IDS and collects all the local information of its neighbor nodes. Also, if IDS observes dissonance in the received information then it'll cooperate with other nodes to attack detection process [14].

2.2.2.3 Hierarchical IDS

This architecture often is used in multi layer networks. Also it is used in the networks that use clustering techniques. In This architecture IDS is installed on all the nodes and will be paying to check the performance of its nodes and neighboring nodes. Then, collected data and name of suspicious nodes will be sent to the cluster head and the cluster head performs the attack detection operation according to information obtained from the nodes [10].

3. Problem

Rather than benefits of Ad hoc networks, these networks have some limitations and weaknesses. That are more about security issues these networks. Because of the specific characteristics and nature of network communication media, the variety and number of attacks is very high in such networks. Tiny drop route request packets with the aim of disrupting the routing, Tiny drop data packets to interfere with submitting information to the destination And creating delays in it, Changing the content of routing packages to change the optimized rout. And other types of network attacks that aim to lower the overall performance and network resource consumption. Alongside these wide attacks, the various intrusion detection methods are designed that they have sometimes some bugs. Including the ability of discovering just one or two attacks. Or to detect malicious nodes from control packets and exchange them into large networks. This makes overhead for network. Some other methods require heavy computation with complex algorithms to detect malicious nodes. Due to the limitations of Ad hoc networks in processing, the mentioned methods don't have very high performance will [2, 3, 10]. In this paper a method is discussed to detect three types of attacks at the same time. By considering the limitations of the Ad hoc network, the detect operation can be done. In addition, the amount of received packets at the destination increases.

4. Proposed Method

In this paper we present a new intrusion detection method based on FSM and cache memory. Eavesdropping the sent data by neighbor nodes is the basic idea of this method. This method which is placed Between Data link layer and physical layer can detect three types of attacks simultaneous: strike drop data packets, routing packets drop and changes in the incoming packet. This method operates as follows.

First, the network nodes are clustered by a certain clustering method and a cluster head node is determined for the cluster, periodically and dynamically. The task of cluster head is final diagnosis of malicious nodes within the cluster and informing the adjacent cluster heads. Then each node in the cluster produces a FSM for each neighbor by sending a path request packet to each one of them and also produces a FSM for each output data packet. Then based on the type of packet sent from the node which can be data packet or routing packet, one of the following two scenarios will be estimated:

Scenario 1: Evaluating the neighbor nodes during the route request packet receiving: A node when receives a route request packet will have two different modes (whether the node is destination or not), that show in figure1:

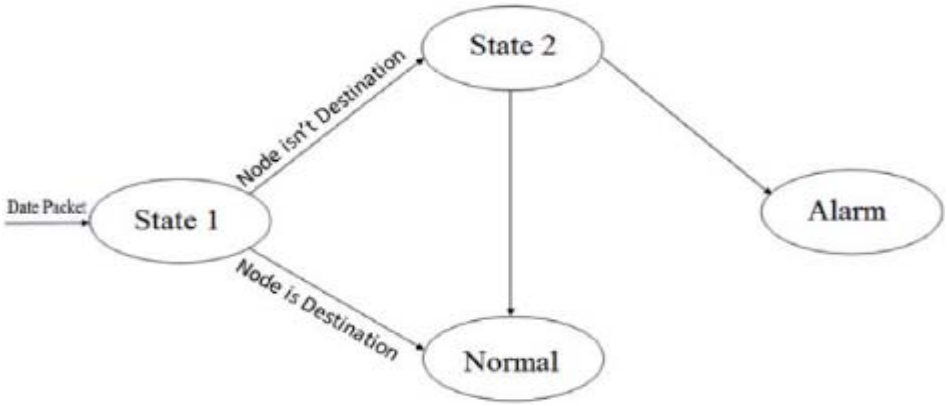

Figure 1. FSM to route request packet

State2- Receiving node is the destination node, In this case, if the node sends a Reply then the FSM of the node switches to normal mode, otherwise it switches to the Alarm mode.

State3-Receiving node isn't the destination node, In this case, if the node sends Reply (there is a route to destination) or a Broadcast (there isn't any route to destination) then the FSM of the node switches to normal mode, otherwise it switches to the Alarm mode.

Scenario 2: Evaluating the neighboring nodes performance during receiving data package: When a node receives a data packet it'll have two different modes (whether the node is destination or not), that show in figure 2:

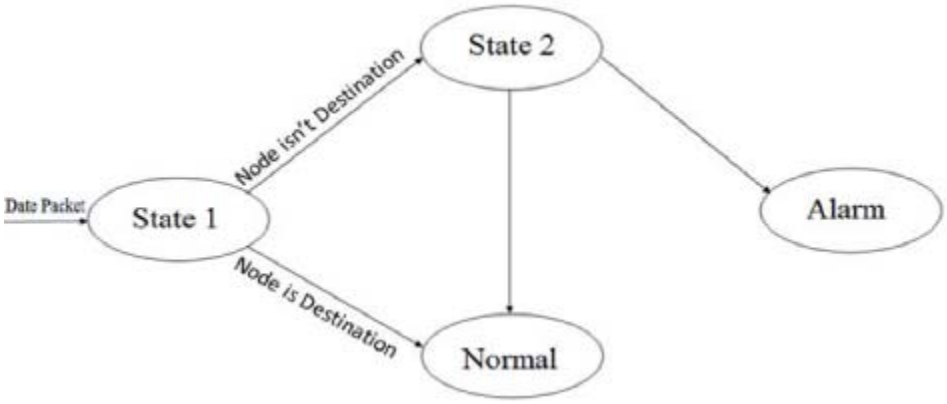

Figure 2. FSM to Data Packet

Normal State: in this case the node who receives data packet also is the destination node. In this situation the FSM of the node will go to normal mode.

State2: when the node which receives data packet isn't the destination node. In this case if the node sends the data package to the next node then the FSM of the node switches to normal mode, otherwise it will go to Alarm mode.

In addition, to detect changes in the incoming packets, the source node stores the packet1 with a FSM in its memory and sends the packet to the intermediate node then it compares the packet outputting from the intermediate node with the sent packet (Packet1 and Packet2) and based on the responses of this comparison, the necessary changes to the FSM will be satisfied. The figure 3 shows detecting the changes of incoming packet.

5. Simulation Results

We simulated our method by NS2 software. Our simulation conditions are as follows: In our simulation, ad hoc routing protocol is AODV. In these simulations of 64 hosts used randomly within an 1000 × 1000 m2 area. Each node has a radio propagation range

of 250 m and the channel capacity was 2 Mbps. The minimum and maximum speed is set to 2 and 10 m/s, respectively. Intrusion detection engine for 12 malicious nodes. The malicious behavior is carried between 50 and 300 sec. malicious nodes drop all data packet they receives. 12 traffic generators were developed to send constant bit rate datagram to 12 destination nodes. The mean size of the data payload was 512 bytes.

As usual to examine performance of intrusion detection algorithms, four parameters are examined that including:

* True Positives: (number of malicious nodes that have been correctly diagnosed).

*False Positive: (number of malicious nodes that have been incorrectly diagnosed).

*Detection Ratio: (detection ratio that is percent of nodes which have been correctly diagnosed to the total malicious nodes).

Figure 3. Detecting the Changes of Incoming Packet

* False Alarm Ratio: (Rate of false alarm that is percent of Nodes which incorrectly have been diagnosed as malicious than the total Nodes which have been diagnosed).

We use a threshold to detect a malicious Node and If the Node has drop or changes in the package further away from the threshold, As a malicious Node is reported. It is very important to determine Threshold for diagnoses drop packets in the network, because its high levels cause to be detected less malicious nodes and therefore Detection Ratio comes down. And if the threshold value is low, the Healthy nodes will be incorrectly diagnosed as malicious node that therefore False Alarm Ratio increases. In addition to threshold, number of Nodes that introduce a Node as a malicious Node is also important.

Therefore, if the number of suspicious behaviors of Node was higher than threshold and more than two to three Nodes also had been reported a kind of suspicious behavior in a node, Node is introduced as the malicious Node.

Threshold for alarm drop package, twice the average of number of suspicious behaviors which are reported, is considered for each Node and from there that normal nodes do not attempt to change the packages, Minimum number of reporters will be enough for alarm changing in packages. Revealing the threshold, to review the results of the simulation explains.

5.1 Results to detect change in data packets in an assumed network

Regardless of what model be changed or be done with what purpose, Each node can make sure that changes in data packets have been done or not by making notes IP header and Getting a HASH of its content, After listening again of output of packet from neighboring node and its Comparison. Because the healthy nodes do not cause some changes in data packets, the node that would change hands is definitely malicious node. If we assume that malicious nodes do not attempt to introduce the healthy nodes as malicious nodes, there will be no false diagnoses. figure 4 shows that the proposed method has very good Ability to detection and also Figure 5 shows that the detection ratio per number of malicious nodes is almost 100 percent.

5.2 Results to detect changes in the routing packets in an assumed network

Unlike the selfish nodes, Malicious nodes will try to conduct network traffic into their position by Changing in routing packets, And they listen Information, that in this case, from there healthy nodes do not attempt to change the packets, These nodes will be easily identifiable. Figure 6 shows that the Number of nodes which have been correctly diagnosed and also Figure 7 shows detection ratio per number of malicious nodes. So the simulation results to detect of changes in routing packets are very good.

5.3 Results to detect data drop packets in an assumed network

We do simulation for the case that the malicious nodes participate in routing and drop total data packets. Because drop ratio of nodes is high in Ad hoc networks for various reasons and healthy Node also may have drop, it is very difficult to detect the malicious nodes in this case and detection ratio is low. Figure 8 shows Average False Alarm. That we can obtain a higher detection ratio with consider a lower threshold, But at the same time the amount of False Alarm increases.

5.4 Results for the routing drop packets in an assumed network

There are several major problems to examine Route request packets (RREQ) in AODV protocol, first the packets are broadcast

and in this case, the MAC layer protocol does not guarantee the packet to be correctly received by all neighbors. Second, Each Node will broadcast the packet just once in case of received Route request packet and will drop the other Incoming packets. And Thus through the examination of sending of neighbor nodes, we will not be able to distinguish malicious Node that drops route request packets. Of course if the Node drops only part of the RREQ packets, then there will be probability that the RREP packets to create and if it tried to drop RREP packets in this case, malicious Node will be detectable. We can say that the detection accuracy of drop RREP packets is almost that of data drop packets.

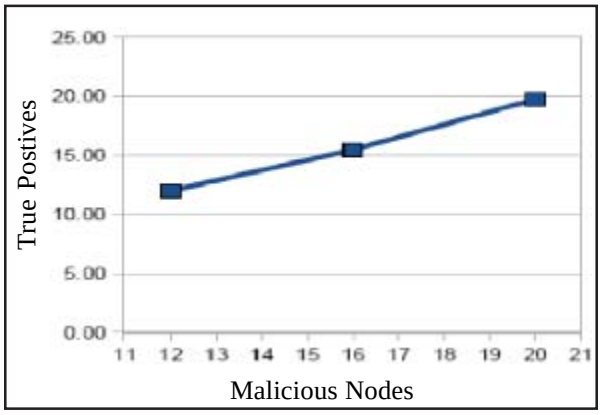

Figure 4. Number of nodes which have been correctly diagnosed

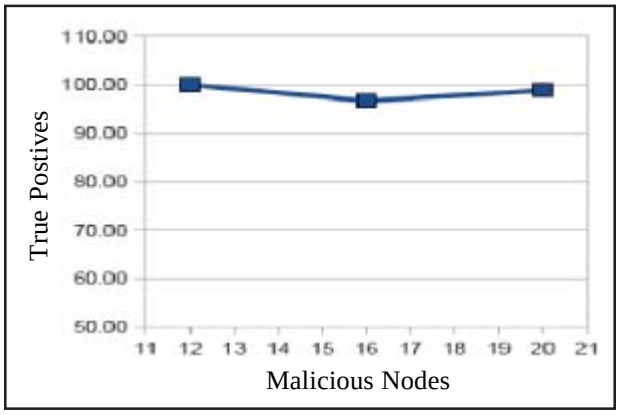

Figure 5. Detection ratio per number of malicious node

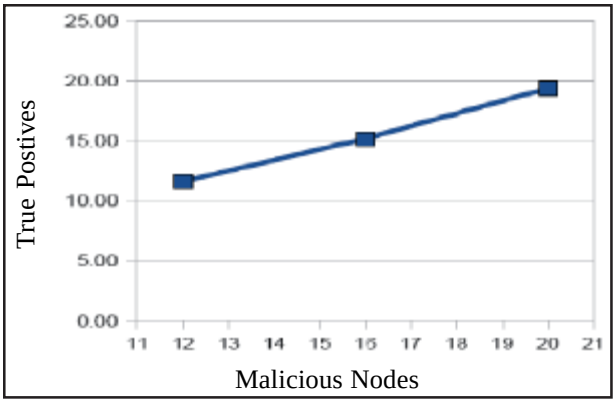

Figure 6. The Number of nodes which have been correctly diagnosed

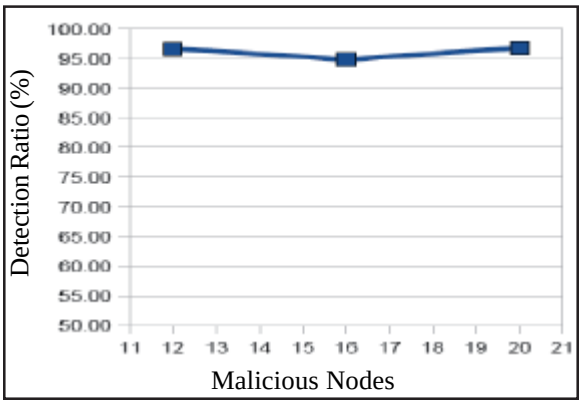

Figure 7. Detection ratio per number of malicious nodes

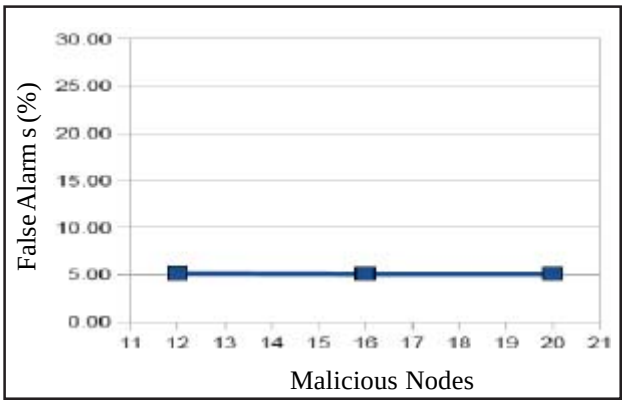

Figure 8. False alarms ratio per Number of malicious Nodes

In this section, our simulation conditions are as follows: Ad hoc routing protocol is AODV.In these simulations network of 50 hosts placed randomly within an 1000 × 1500 m2 area. Each node has a radio propagation range of 250 m and the channel capacity was 2 Mbps. The nodes in the simulation move according to the 'random way point' model. The speed is 1 m/s, respectively. Intrusion detection engine for 10, 20 and 30 malicious nodes. The malicious behavior is carried between 50 and 300 sec. malicious nodes drop all data packet they receives. The nodes perform normally between 0 and 50 sec. 3 traffic generators were developed to send constant bit rate datagram to ten destination nodes. The mean size of the data payload was 128 bytes.

In figure 9 and 10, the comparison of the selfish node detection rates and also the false alarm rates between the presented method and the results of existing methods in [21] is shown. As can be seen, while the proposed method in this project is much easier than the mentioned compared method but their results are very close and almost same. It should be noted that calculating strategy for false alarm rate and detection rate of the compared article are local and achieved only for monitor nodes and then the average is obtained while in this project, both the criterions are calculated for whole the network, generally.

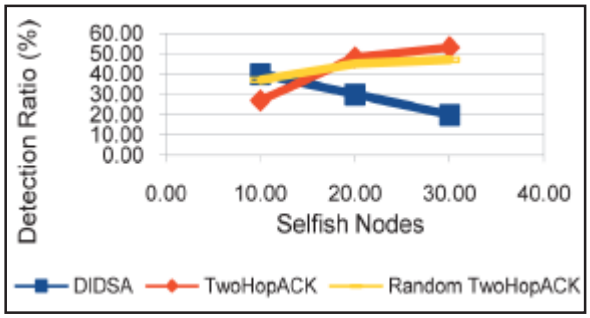

Figure 9. Detection ratio per number of malicious nodes

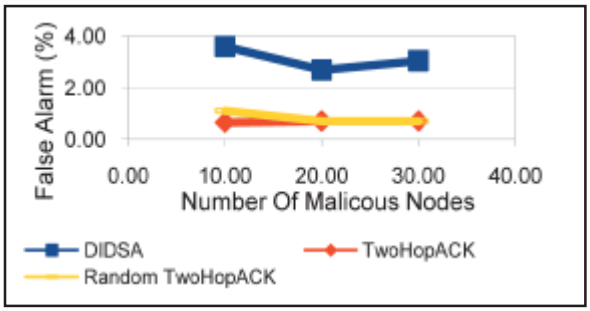

Figure 10. false alarms ratio per Number of malicious Nodes

6. Conclusion and Future Works

The presented approach based on FSM focuses at recognizing the malicious nodes within the network in a fast and accurate way, then it deals with rapid introduction of the malicious nodes to other nodes in the network to prevent sending multiple packets, that Our method is able to identify three type of the attacks (Data packet Drop, Drop of route request packets and changes in the incoming packet) at the same time in the network. Our method doesn't need heavy computation and also its speed and accuracy in detecting suspicious nodes are great. According to the results presented in the simulation Section, it is characterized that the proposed method in this paper could have very good results for the control changes in data or routing packets. Any small changes would be detected because for the each packet is separately created a state machine. From the other side, the results for control of drop packets are not satisfactory. Because the nature of the network does not allow the exact control for this purpose and should have used another method for control drop. For the future work, this method can be combined with other methods which will have good results to drop packets and totally gives a better protocol. On the other hand, it should be noted that the quality of the proposed method about drop and changes in the routing protocol is quietly related with used routing algorithms and the other results may obtain for the other routing algorithms. Our proposed method to deal with malicious nodes that try to go intrusion with complex way and make disturbance in working of network, Is a good method. Also for future works, it seems that with using double opportunity mechanism, our method reduces false alarm in the network and can increase accuracy and probably increase the amount of data received at the destination.

References

[1] Claudio Basile, Zbigniew Kalbarczyk, Iyer, Ravi, K. (2005). Neutralization of errors and attacks in wireless ad hoc networks, IEEE Computer Society.

[2] Hadi Otrok, Noman Mohammed, Lingyu Wang, Mourad Debbabi, Prabir Bhattacharya, (2008). A game-theoretic intrusion detection model for mobile ad hoc networks, *Computer Communications*, 31(4) 708–721.

[3] Yabandeh, Meysam., Mohammadi, Hossein., Yazdani, Naser (2007). Multipath Routing in Mobile Ad hoc Networks: Design Issues, 12th International CSI Conference Computer (CSICC07) Shahid Beheshti University, Tehran, Iran.

[4] Razak, Shukor Abd ., Samian, Normalia., Ma'arof, Mohd. Aizaini., Furnell, S. M., Clarke3, N. L., Brooke, P. J. (2009). A Friend Mechanism for Mobile Ad Hoc Networks, *Journal of Information Assurance and Security*, p. 440-448.

[5] Ramachandran, Chandrasekar ., Misra, Sudip., Obaidat, Mohamed, (2008). Fork: A Novel two-Pronged strategy for an agent-based intrusion detection scheme in ad hoc network, *Computer Communications*, 31(16) 3855-3869.

[6] Ibrahim, Mohamad M., Sedak, Nayera., EL-Banna, Mohamed (2009). Prevention of Dropping Routing Traffic Attack in wireless Ad hoc AODV Based Network using Real-time Host intrusion detection, *In:* 26th national Radio science conference, IEEE.

[7] Lauf, Adrian P., Peters, Richard A., Robinson, William H.(2010). A Distributed Intrusion Detection System for resource-constrained Ad hoc Networks, *Ad Hoc Networks*, 8(3) 253–266.

[8] Sun, Bo., Wu, Kui ., Pooch, Udo W.(2004). Towards Adaptive Intrusion Detection in Mobile Ad Hoc Networks, IEEE Communications Society, p. 3551-3555.

[9] Kim, Hyunwoo., Kim, Dongwoo., Kim, Sehun (2006). Lifetime-enhancing selection of monitoring nodes for intrusion detection in mobile Ad hoc networks, *International Journal of Electronics and Communications*, 60 (3) 248-250.

[10] Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C., Balupari, R., Tseng, C-Y., Bowen, T., Levitt2, K., Rowe, J. (2005). A General Cooperative Intrusion Detection Architecture for MANETs, *In:* Proceedings of the 3th IEEE international workshop on information Assurance.

[11] Subhadrabandhu, Dhanant., Sarkar,Saswati ., Anjum, Farooq (2004). Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols, IEEE VTC.

[12] Srinivasan, T., Vijaykumar, V., Chandrasekar, R. (2006). An auction based task allocation scheme for power-aware intrusion detection in wireless Ad hoc networks, *In*: Third international conference on wireless and optical network, IEEE wocn.

[13] Huang, Yi-An., Lee, Wenke., Zhang, Yongguang (2003). Intrusion detection techniques for mobile wireless network, accepted *ACM MANET Journal*.

[14] Yi, Ping., Jiang, Yichuan., Zhong, Yiping., Zhang, Shiyong (2005). Distributed Intrusion Detection for Mobile Ad Hoc Networks, *In:* Proceedings of the Symposium on Applications and the Internet Workshops, IEEE.

[15] Zhang, Y., Lee, W., Huang, Y. (2003). Intrusion detection techniques for mobile wireless networks, ACM Wireless Networks, ACM, p. 545–556.

[16] Perkins, C., Royer, EM. (1999). Ad hoc On Demand Distance Vector (AODV) Routing, *In:* Proceedings of the Second Workshop on Mobile Computing Systems and Applications, IEEE, p. 90-100

[17] Corson, MS., Ephremides, A. (1995). A Distributed Routing Algorithm for Mobile Wireless Networks, ACM Baltzer Wireless *Networks Journal*, p. 61-81.

[18] Iwata, A., Chiang, CC., Pei, G., Gerla, M., Chen, TW. (1999). Scalable Routing Strategies for Ad hoc Wireless Networks, *Journal on Selected Areas in Communications*, Special Issue on Wireless Ad hoc Networks,IEEE, p. 1369-1379.

[19] Johnson, DB., Maltz, DA. (1996). Dynamic Source Routing in Ad-Hoc Wireless Networking, Mobile Computing, Kluwer Academic Publishing, New York.

[20] Peralman, MR., Haas, ZJ. (1999). Determining the Optimal Configuration for the Zone Routing Protocol, *IEEE Journal on Selected Areas in Communications*, Special Issue on Wireless Ad hoc Networks, p. 1395-1414.

[21] Djenouri, Djamel., Badache, Nadjib (2009). On eliminating packet droppers in MANET: A modular solution., *Ad hoc Networks*, 7, 1243–1258.