Contemporary Engineering Sciences, Vol. 2, 2009, no. 3, 105 - 116

Developing a Hybrid Method for Identifying Monitoring Nodes in Intrusion Detection Systems of MANET

Marjan Kuchaki Rafsanjani

Ph.D Student, Science & Research Branch
Islamic Azad University (IAU), Tehran, Iran
kuchaki.m@srbiau.ac.ir

Ali Movaghar

Department of Computer Engineering
Sharif University of Technology, Tehran, Iran
movaghar@sharif.edu

Abstract

Nowadays with appearance of a wide range of wireless devices, security of Mobile Ad hoc Networks (MANET) became an important problem and Intrusion Detection System (IDS) can be deployed as a second line of defense in a MANET. In this paper, a monitoring nodes selection method with high battery power in these networks is presented. A three-phase detection scheme is proposed. In the first phase, unauthorized nodes and in the second phase, malicious nodes are detected. Finally in the third phase, nodes with the largest battery power as monitoring nodes are considered. So, with this scheme, some of nodes contribute in monitoring task and costs of network monitoring and intrusion detection system will be decreased.

Keywords: Authentication, Misbehaving nodes, Mobile Ad hoc Network (MANET), Security, Zero knowledge technique

1 Introduction

Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless media and form dynamic topologies. The basic characteristic of these networks is the lack of fixed infrastructure and therefore the absence of dedicated nodes that provide network management operations. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration since they dynamically change without using the management or infrastructure of the existing networks [1,2]. These characteristics and also node mobility pose many new challenges. The first major challenge was the routing problem which has been solved for the most part by protocols such as AODV. The second major challenge is security. Potential deployments of MANETs may be in un-trusted environments. Unfortunately existing security solutions for the Internet are inapplicable to MANETs due to mobility and the lack of a centralized network management point. Hence security is an important but hard problem for any realistic applications with MANETs [3].

Typical application areas of mobile ad hoc network include battlefields, emergency search, rescue missions, law enforcement and data acquisition in remote areas. A mobile ad-hoc network is also useful in classrooms and conventions where participants share information dynamically through their mobile computing devices. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms [3,4].

In this paper, a three-phase scheme for the detection of unauthorized and malicious nodes followed by the selection of monitoring nodes in MANETs is presented. The first and second phases is based on non-interactive zero knowledge technique which is based on proofs. The proposed scheme is able to detect the main network functions in network layer and link layer and can be used in intrusion detection systems in mobile ad hoc networks.

2 Background

In this section, we present an overview of significant concepts that are important for the understanding of the material to follow. We first briefly introduce intrusion detection systems in MANET. Then we describe the misbehaving nodes in MANET and how they create problems in these networks. Finally, we give a quick review of the authentication and key management problems. Our scheme could improve intrusion detection in the area of security.

2.1 Intrusion Detection Systems in MANET

Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System (IDS) [5,6].

Studies show that intrusion detection techniques just like encryption and authentication systems which are the first line of defense are not enough. As the system grows in complexity their weaknesses grow causing the network security problems to grow too. Intrusion detection can be considered as a second line of defense for network security. If an intrusion is detected then an answer for preventing intrusion or minimizing the effects can be generated. There are several assumptions for developing IDS. In the first assumption, user operations and the programs are visible and in the Second assumption, normal and intrusive activities in a system behave differently. So, IDS should analyze system activities and ensure whether or not an intrusion has occurred. Intrusion detection can be classified based on audit data which are host or network based. A network-based IDS, receives packets from the network and analysis it. On the other hand, host-based IDS, analyses the events taken place in application programs or the operating systems. IDS can be divided into three groups based on detection techniques; anomaly detection system, misuse detection systems and specification based detection [7,8].

In MANET, intrusion detection and response systems should be both distributed and cooperative in order to fulfill the needs of mobile ad hoc networks. For instance, in the architecture proposed in [9], every node in the mobile ad hoc network participates in intrusion detection and response. Since every node cannot trust its neighboring nodes, it is responsible for detecting signs of intrusion locally and independently. However, neighboring nodes can collaboratively exchange messages in case of a suspicious situation or confirmed intrusion detection [10].

2.2 Misbehaving nodes in MANET

Those nodes in the network which cause dysfunction in network and damage the other nodes are called Misbehaving or Critical nodes. MANETs like other wireless networks are liable to active and passive attacks. In the passive attacks, only eavesdropping of data happens; while in the active attacks, operations such as repetition, changing, or deletion of data are necessitated. Certain nodes in MANETS can produce attacks which cause congestion, distribution of incorrect routing information, services preventing proper operation, or disable them [11].

Those nodes in the network which perform active attacks to damage other nodes and cause disconnection in the network are called Malicious or Compromised nodes. Also, those nodes which do not send the received packets (used for storing battery life span to be used for their own communications) are called Selfish nodes [12,13]. A selfish node impacts the normal network operations by not participating in routing protocols or by not sending packets. A malicious node may use the routing protocols to announce that it has the shortest route to the destination node for sending the packets. In this situation, this node receives the packets and doesn’t send them. This operation is called Blackhole attack [14,15].

Malicious nodes stop the operation of a routing protocol by changing the routing information or by structuring false routing information; this operation is called Wormhole attack. As two malicious nodes create a wormhole tunnel and are connected to each other through a private link, it can be concluded that they have a detour route in the network. This allows a node to create an artificial route in the current network and shorten the normal currency of routing messages in a way that the massages will be controlled by two attackers [16,17].

Selfish nodes can intensively lower the efficiency of the network since they do not easily participate in the network operations. Malicious nodes can easily perform integrity attacks by changing the protocol fields in order to destroy the transportation of the packets, to deny access among legal nodes, and can perform attacks against the routing computations. Spoofing is a special case of integrity attacks with which a malicious node, due to lack of identity verification in the special routing protocols, forges the identity of a legal node. The result of such an attack by malicious nodes is the forgery of the network topology which creates network loops or partitioning of the network. The lack of integrity and authentication in the routing protocols creates forged or false messages [15,18,19,2].

If a node participated in routes finding but does not forward a packet, it is a misleading node and misleads other nodes. But if a node does not participate in routes finding, it is a selfish node [6].

2.3 Authentication and key management problems

The network needs the assurance that only the certified users have an access to its services and the users would have access to secure facilities in which lack of security in the network would be considered as a permanent threat for the user. The main goal is to create a session key for confidential communication, mutual authentication, and non-repudiation [20,21].

Most of the access control systems depend on public key management systems. The verification of a link between an identity and a key is established by a digital certificate. This certificate includes a public key, an identity, and other cryptography details signed by a trusted third party. In order to be used in applications, the certification of a public key is created by the Certificate Authority (CA). Security requirements are very important for CAs because they can encounter many attacks.

In conventional networks, the two main solutions of public key management are Pretty Good Privacy (PGP) and the X.509 public key infrastructure. The X.509 in comparison to PGP has a strong hierarchy. In PGP there are many central certificate repositories which are not often used. But in X.509 there is a hierarchy structure of CAs which is responsible for issuing certificates and their verifications. A node determines the verification of a certificate by using CA public key. The CA may revoke a certificate. So, it is necessary to propagate the Certificate Revocation List (CRL) periodically. Delay in propagating a CRL may cause acceptance of revoked certificates by some nodes in the network.

In Ad hoc networks, this method is difficult in practice in as much as access to a CA to get the latest CRL is not guaranteed all the time. The process of estimating the verification of a certificate in Ad hoc networks takes a lot of time and it is also difficult. It has been tried to eliminate the need for a centralized CA in key management methods for Ad hoc networks. In the first method, there is one

CA with distributing parts of the secret key on several nodes [5]. One proposed public key scheme for Ad hoc networks is using the threshold cryptography and the public key technique. In this scheme, the special nodes on which parts of the secret key are distributed are determined as servers. An attacker has to attack a certain number of servers in order to get access to the secret key service. To prevent the gradual compromising of the servers, refreshing is done constantly. To establish the service, this scheme needs pre communication and coordination of the nodes. In addition, some nodes will work more than other nodes. Also, if the number of nodes in Ad hoc network is high, knowing the public key for all nodes will not be possible. In another method, a self-organized public key infrastructure was used. Hubaux et al. [22] proposed a public key distribution based on trust building scheme for Ad hoc networks. In this scheme, there are no central certificate directories for the distribution of certificates.

In most methods of authentication and key management, there are many attacks which can target the identity of a mobile node or the encryption key that is stored or exchanged with the protocols of cryptography [2,15,23].

3 The detection scheme

The detection scheme that we proposed is shown in figure 1 and it is based on the main operations of Ad hoc networks in link and network layers of Open Systems Interconnection (OSI) Reference Model.

In link layer the cases of one-hop connectivity and frame transition, and in network layer, the cases of routing and data packet forwarding are considered [5,12,15]. Data link layer protocols provide the connections between neighboring nodes and will also provide the accuracy of the transmitted frames. As routing protocols exchange routing data between nodes, as a result, they would maintain routing states in each node. Based on routing states, data packets are transmitted by mediated nodes along an established route to the destination.

The presented scheme includes three phases. In the first phase of the detection procedure, it is tried to detect the unauthorized nodes and the second phase from among authorized nodes, will specify malicious nodes. These two phases of our scheme is based on Komninos and et al.'s framework and use a non-interactive zero knowledge technique [15]. Then in the third phase, from among authorized and valid nodes, the ones which have higher battery power will be determined as monitoring nodes.

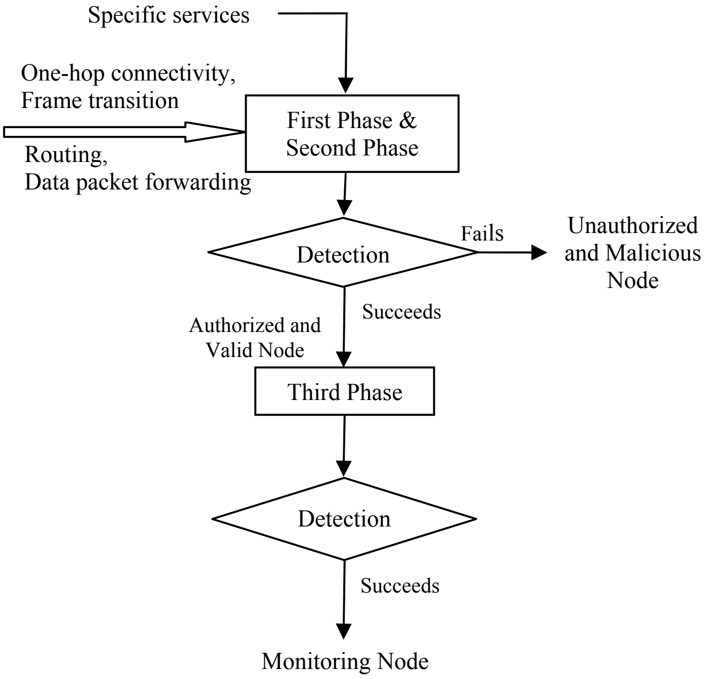

Fig. 1 Detection scheme of identifying monitoring nodes in MANET

3.1 Detecting unauthorized nodes phase

When one or a few nodes are linked to MANET, the procedure of detecting unauthorized nodes begins working. In this phase, there is a need for authentication and so the nodes with verifiable authentication are determined and they can have access to specific applications or services in a MANET. This function can be performed by a suitable authentication protocol for MANET.

Suppose B and C nodes are verified. When node X_1 enters the MANET, its authentication action is done by neighboring nodes B and C. New routes will be built between nodes. As soon as nodes X_1 are verified as authorized nodes in the network, routing and transmitting packets would be done through them.

There are several suitable protocols for authentication in the MANET which can be used. Of course, it is necessary to use protocols with low complexity and non-interactive which would not produce excessive computational overhead in the network. The interactive zero protocols are not suitable for the wireless environments because they exchange many messages and as a result the efficiency of the network decreases. The non-interactive zero knowledge protocols are proper for the MANET networks in such a way that the nodes do not need to exchange messages to verify their identities. For example, the node X_1 can prove its identity to the nodes B and C and guarantees that discrete logarithms of $y_1=\alpha_1^{x1}$ and $y_2 = \alpha_2^{x2}$ are computed with α_1 and α_2 bases and are displaced in equation (1):

$$k_1.x_1 + k_2.x_2 = b(\mathrm{mod}\, p) \qquad (1)$$

k_1 and k_2 are integers and p is the prime number [15].

In the protocol, node X_1 first computes the y_3 and y_4 ($y_3= \alpha_3^{x3}$, $y_4= \alpha_4^{x4}$) then solves the equation (2):

$$k_1.x_3 + k_2.x_4 = 0(\text{mod } p) \qquad (2)$$

Then the following messages are exchanged:

$$\text{B,C} \leftarrow \text{X}_1 : y_5 = \alpha_1^{x_3} \text{ , } y_6 = \alpha_2^{x_4} \qquad \text{(M1)}$$

$$\text{B,C} \rightarrow \text{X}_1 \ : y_7 = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_5, y_6) \qquad \text{(M2)}$$

$$\text{B,C} \leftarrow \text{X}_1 : y_8 = x_3 - y_7 .x_1 (\text{mod } p), \quad y_9 = x_4 - y_7 .x_2 (\text{mod } p) \qquad \text{(M3)}$$

Node X$_1$ sends y$_5$ and y$_6$ to the B and C nodes. As soon as these nodes receive the M1 message, compute the y$_7$ with a one-way hash function and send M2 message to the node X$_1$. Node X$_1$ by examining M1 validity builds the M3 message and sends y$_8$ and y$_9$ to the B and C nodes.

Node X$_1$ convinces nodes B and C that it knows the discrete logarithms of y$_1$ and y$_2$ with the α$_1$ and α$_2$ basis and also knows that these logarithms build a linear equation. This can be done through verifying the resulted proof of y$_7$, y$_8$, and y$_9$. It is easily seen that nodes B and C will be always successful in making an accurate proof by reconstructing y$_{10}$= α$_1^{y8}$.y$_1^{y7}$ and y$_{11}$= α$_2^{y9}$.y$_2^{y7}$, then it is examined to see whether y$_7$ is an equivalent to y$_{12}$, when y$_{12}$=*H*(α$_1$,α$_2$,y$_1$,y$_2$, k$_1$,k$_2$,*b*,y$_{10}$,y$_{11}$), and if the equation (3) is accurate:

$$k_1.y_8 + k_2.y_9 = -y_7.b(\text{mod } p) \qquad (3)$$

It is seen that nodes B and C are always successful in making a reliable proof because y$_{10}$= y$_5$ and y$_{11}$= y$_6$.

$$y_{10} = \alpha_1^{y_8}.y_1^{y_7} \overset{y_8, y_1}{=} \alpha_1^{x_3 - y_7.x_1}.\alpha_1^{x_1.y_7} = \alpha_1^{x_3} = y_5 , \qquad y_{11} = \alpha_2^{y_9}.y_2^{y_7} \overset{y_9, y_2}{=} \alpha_2^{x_4 - y_7.x_2}.\alpha_2^{x_2.y_7} = \alpha_2^{x_4} = y_6 .$$

So,

$$y_{12} = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_{10}, y_{11}) = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_5, y_6) = y_7$$

In this way, nodes B and C compute y$_{12}$ and compare it with y$_7$ in M2 message. Nodes B and C, for verification, will replace the responses Y$_8$ and Y$_9$ in the equation (3):

$$\begin{aligned} k_1 y_8 + k_2 y_9 &\overset{y_8, y_9}{=} k_1.(x_3 - y_7.x_1) + k_2.(x_1 - y_7.x_2) \\ &= k_1 . x_3 - k_1 .y_7. x_1 + k_2 . x_4 - k_2 . y_7. x_2 \\ &= k_1 . x_3 - k_2 . x_4 - y_7 .(k_1 . x_1 + k_2 . x_2) \\ &\overset{(1),(2)}{=} - y_7 . b(\text{mod } p) \end{aligned}$$

Then the identity of node X$_1$ is known authorized [15,23].

3.2 Detecting malicious nodes phase

When routing information or data packets are ready to be delivered, the second step of detection mechanism begins to identify the malicious nodes on the starting nodes with one step in the route continuing from the source to the destination. Due to the mobility of the node in the ad hoc network, the route from the source to the destination is changeable. The detection procedure is independent of the mobility of the nodes and the routing protocol of is responsible for delivering the data to nodes.

This process requires the authentication of the valid and compromised identity situation of the interacting nodes. So, the identity of nodes is verified with zero-knowledge technique; and the situation of a malicious node is determined by an agent which collects and analyses the audit data. The agents that are on nodes, distinguish the standard profile of the user, the deviation of records from this source, and also the known attacking signatures. Anyhow, the operations of the agent are in accordance with IDS type. The agent has a passive local role in gathering and analyzing audit data plus authorizing a confidence interval for the neighboring node for the next step. The agent can collect and analyze data in an organized time interval or it can provide a continued service for an open environment. Data processing determines the method of node detection and it also determines the situation of the malicious node.

Suppose node X_1 enters MANET and its identity is verified by zero-knowledge technique; then, when the routing information is ready for delivery, node X_1 should prove its identity and maliciousness again to nodes B and C and it should guarantee that the discrete logarithms $y_1 = \alpha_1^{x_1 + f(z_1 + z_2)}$ and $y_2 = \alpha_2^{x_2 + f(z_1 + z_2)}$ with bases α_1 and α_1 are computed and displaced in equation (4).

$$k_1.x_1 + k_2.x_2 = f(z_1, z_2) + b(\mathrm{mod}\, p) \tag{4}$$

k_1, k_2 and b are integers and p is the prime number [15].

Equation (4) has a multi-variable function of $f(z_1,z_2)$ which determines the maliciousness of a node. This function is defined in equation (5).

$$f(z_1, z_2) = \begin{cases} k_1.z_1 + k_2 .\, z_2 = C \ \mathrm{mod}\, P, & for \quad x_1 \le z_1,\, z_2 \le x_2 \\ 0 \quad , & otherwise \end{cases} \tag{5}$$

k_1 and k_2 are integers and p is the prime number.

The value of $f(z_1,z_2)$ is determined by a local agent. Based on the analysis of data, the agent defines a confidence interval. With the help of this confidence interval, the agent can identify a malicious node. The confidence interval can follow a normal distribution, shown in figure 2, in a way that the values x_1 and x_2 are discrete and the interval is continuous [15].

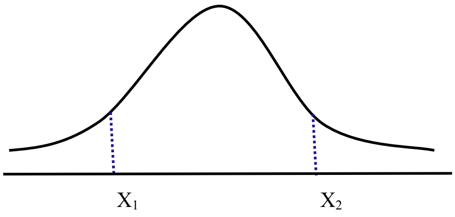

Fig. 2 Confidence interval for malicious nodes

If values z_1 and z_2, determined by agent, are found in interval x_1 and x_2 then $f(z_1,z_2)$ equals $k_1.z_1 + k_2 .\, z_2 = C \ \mathrm{mod}\, P$, then node X_1 proves its true identity to nodes B and C and the routing information is exchanged. Conversely, if values z_1 and z_2 are outside the distance from x_1 to x_2, in this case $f(z_1,z_2)=0$. Therefore, equation (1) and (4) are the same. In this situation, node X_1 is considered to be Malicious because it verifies its identity to nodes B and C in the first step. Therefore, the routing information will be unreliable and it will be deleted by nodes B and C [15,2].

3.3 Selecting monitoring nodes phase

Since in the intrusion detection systems in MANET, the node, which has been selected to monitor, must collect and analyze all packets in the communication area. So, it uses the extra resources and energy. When the monitoring node identifies the attacker intrusion, it propagates warning messages to the neighboring nodes. Since the bandwidth and the battery power in the MANETs are limited, there is a need for an effective method of utilizing these resources to build detecting intrusion systems. The lifetime of the network is the time that the first failure or decrease (de-charge) of the battery, which is one of the important efficiency criteria, happens to the point that the failure of one node would be able to link the network to some disconnected sub-networks and the next communication services among separated networks would stop [24].

So, in order to improve the lifetime of the network, an effective method in selecting a monitoring node is needed so that a required level of detection intrusion in MANETs would be provided. So, in the proposed method, after the unauthorized and malicious nodes are determined in the first ad second phases; in the third phase, from among authorized and valid nodes, the nodes which have higher battery power would be selected as the monitoring nodes. Consider node i, its neighboring nodes are the ones which are placed about one-hop from it. N^i is the set of the neighboring nodes which include the node i too, and the P_i is the remaining battery power of node i. The node i^* is the monitoring node which is searched, for each node, according to the equation (6):

$$i^* = \arg\ \max_{j \in N^i} P_j \tag{6}$$

Each node sends a periodically controlled packet including battery power value to its neighboring nodes. So, all nodes always know their neighboring nodes' battery power value. Then, to select the monitoring node, each node must vote. The node which would receive at least one vote becomes a monitoring node and the monitoring sensors of the network is loaded and executed. Whenever the condition of the connectivity changes or whenever the remaining battery power of a monitoring node becomes lower than the lowest battery power among the neighboring nodes, the process of selecting the monitoring node must be performed again (equation 7):

$$P_{i^*} < \min_{j \in N^{i^*}} P_j \tag{7}$$

In the equation (7), N^{i^*} is the set of neighboring nodes of monitoring node i* [25,23,2].

4 Analysis the proposed scheme

The selected nodes for hosting the monitoring sensors in network, collect all the packets in their communication area and analyze them in order to discover undesired attack patterns. The used energy by a monitoring node during an interval of Δt is computed by equation (8):

$$E = (m^t s^t + b^t) + (m^r s^r + b^r) + (m^o s^o + b^o) + (m^m s^m + b^m) \tag{8}$$

In this equation, s^t, s^r, s^o, and s^m, respectively show the sizes of the packets in bytes in the operations of transmission, receiving, eavesdropping, and monitoring. The *m* and *b* factors are respectively the varied and constant energy costs for each operation, and are derived experimentally [26]. In this method, monitoring nodes change constantly. Kim and et al. [25] presented a monitoring node selection scheme for intrusion detection in mobile ad hoc network, as selected node as the monitoring node can be an unauthorized or malicious node. The advantage of our scheme is that monitoring nodes are chosen among authorized and valid nodes.

On the other hand, in the most of the existing intrusion detection systems for MANETs, a detection system sits on every node, which runs all of the time. This intrusion detection system could be monitoring traffic in its neighborhood, or changes in its routing table and etc. [15,27,28,29,30]. Since, a node in a MANET has limited battery power, so, selecting all of nodes to contribute in monitoring turn out to be a costly overhead.

5 Conclusions

Power resources and rare computational of mobile nodes in mobile ad hoc networks impose heavy limitations on functionality of an effective intrusion detection system. Our work in this paper is to select the monitoring nodes with largest energy power. We propose detection scheme based on the non-interactive zero knowledge technique to exchange information for their authentication; so, the unauthorized and malicious nodes are identified. Our scheme will improve the lifetime of the network among nodes by evenly distributing of the usage of the resources. Meanwhile the nodes that will be selected as monitoring nodes in the network will be authorized and valid nodes. We have also analyzed the performance of the proposed scheme theoretically. In the future, we will simulate aspects of intrusive behavior of unauthorized and malicious nodes by *ns2* network simulator.

References

[1] L. Stamouli, P.G. Argyroudis and H. Tewari, Real-time intrusion detection for ad hoc networks, The 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2005, 374-380.

[2] M. K. Rafsanjani and A. Movaghar, Identifying monitoring nodes in MANET by detecting unauthorized and malicious nodes, International Symposium on Information Technology, 2008, 2798-2804.

[3] B. Sun, H. Chen and L. Li, An intrusion detection system for AODV, The 10th IEEE International Conference on Engineering of Complex Computer Systems, 2005, 358-365.

[4] H. Xie, Z. Hui, An intrusion detection architecture for ad hoc network based on artificial immune system, The 7th International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006, 1-4.

[5] L. Zhou and Z. J. Haas, Securing ad hoc networks, IEEE Network Magazine Special Issue on Network Security, 13(1999), 24-30.

[6] Y. Xiao, X. Shen and D.Z. Du, Wireless/Mobile Network Security, Springer, 2006.

[7] P. Brutch and C. Ko, Challenges in intrusion detection for wireless ad-hoc networks, The Symposium on Applications and the Internet Workshop, 2003, 368-373.

[8] M. K. Rafsanjani, A. Movaghar and F. Koroupi, Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes, The Proceedings of World Academy of Science, Engineering and Technology, 2008, 351-355.

[9] Y. Zhang, W. Lee and Y. Huang, Intrusion detection techniques for mobile wireless network, Wireless Networks Journal, 9(2003), 545-556.

[10] N. Nasser and Y. chen, Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks, The IEEE International Conference on Communications, 2007, 1154-1159.

[11] A. Karygiannis, E. Antonakakis and A. Apostolopoulos, Detecting critical nodes for MANET intrusion detection systems, The 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006, 9-17.

[12] J. Kong, Adaptive Security for Multi-layer Ad Hoc Networks, Special Issue of Wireless Communications and Mobile Computing, John Wiley InterScience Press, 2002.

[13] L. Blazevic, L. Buttyan, S. Capkun, S. Giordano, J. Hubaux and J. Le Boudec, Self-organization in mobile ad-hoc networks: The approach of terminodes, IEEE Communications Magazine, 39(2001), 166–174.

[14] Y. Zhang and W. Lee, Intrusion detection in wireless ad-hoc networks, The 6th Annual International Conference on Mobile Computing and Networking, 2000, 275–283.

[15] N. Komninos, D. Vergados and C. Douligeris , Detecting unauthorized and compromised nodes in mobile ad hoc networks, Elsevier Ad hoc network, 5(2007), 289-298.

[16] P. Kyasanur and N. Vaidya, Detection and handling of MAC layer misbehavior in wireless networks, International Conference on Dependable Systems and Networks, 2003, 173–182.

[17] Y. Hu, A. Perrig and D. B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, The 22th Annual Joint Conference of the IEEE Computer and Communications Societies, 2003, 1976-1986.

[18] P. Papadimitratos, Z. J. Haas and E.G. Sirer, Path set selection in mobile ad hoc networks,The 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2002 , 1–11.

[19] B. Sun, W. Kui and U. W. Pooch, Towards adaptive intrusion detection in mobile ad hoc networks, The IEEE Global Telecommunications Conference, 2004, 3551–3555.

[20] L. Venkatraman and D. P. Agrawal, A novel authentication scheme for ad hoc networks, The 2nd IEEE Wireless Communications and Networking Conference, 2000, 1268-1273.

[21] E. C. H. Ngai, M. R. Lyu and R. T. Chin, An authentication service against dishonest users in mobile ad hoc networks, The IEEE Aerospace Conference, 2004, 1275–1285.

[22] J. Hubaux, L. Buttyan and S. Capkun , The quest for security in mobile ad hoc networks, The 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2001, 146-155.

[23] M. K. Rafsanjani and A. Movaghar, Identifying monitoring nodes with selection of Authorized nodes in mobile ad hoc networks, World Applied Science Journal, 4(2008), 444-449.

[24] J. H. Chang and L. Tassiulas, Energy conserving routing in wireless ad-hoc networks, The 19th Annual Joint Conference of the IEEE Computer and Communication Societies, 2000, 22–31.

[25] H. Kim, D. Kim and S. Kim, “Life-time enhancing selection of monitoring nodes for intrusion detection in mobile ad hoc networks, International Journal of Electronics and Communications, 60(2006), 248-250.

[26] L.M. Feeney and M. Nilsson, Investigating the energy consumption of a wireless network interface in an ad hoc networking environment, The IEEE Conference on Computer Communications, 2001, 1548–1557.

[27] A. Partwardhan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, Secure routing and intrusion detection in ad-hoc networks, The 3rd IEEE International Conference on Pervasive Computing and Communications, 2005, 191-199.

[28] K. Nadkarni and A. Mishra, Intrusion detection in MANETs - the second wall of defense, The 29th IEEE Industrial Electronics Society Conference, 2003, 1235–1239.

[29] S. Marti, T. J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in a mobile ad-hoc environment. The 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000, 255–265.

[30] C. Manikopoulos and L. Ling, Architecture of the Mobile Ad-hoc Network Security (MANS) system. The IEEE International Conference on Systems, Man and Cybernetics, 2003, 3122–3127.

Received: November, 2008