World Applied Sciences Journal 4 (3): 444-449, 2008
ISSN 1818-4952

Identifying Monitoring Nodes with Selection of Authorized Nodes in Mobile Ad Hoc Networks

[1]*Marjan Kuchaki Rafsanjani and* [2]*Ali Movaghar*

[1]Department of Computer Engineering,
Science and Research Branch, Islamic Azad University (IAU), Tehran, Iran
[2]Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

Abstract: Mobile ad hoc networks have different characteristics from wired networks. There are new challenges related to security issues that need to be addressed. In this paper, a monitoring nodes selection method with high battery power in these networks is presented. We propose a two-phase detection scheme. In the first phase, authorized nodes are detected and in the second phase, nodes with the largest battery power as monitoring nodes are considered. So that the first phase of detection procedure uses non-interactive zero knowledge technique in order to determine the identity of nodes. In this technique, nodes do not need to exchange multiple messages to prove their identities. The proposed scheme is enabled with the main operations of ad hoc networking, which are found at the link and network layer. So, the proposed scheme could improve intrusion detection in the area of security.

Key words: Authentication · Intrusion Detection System (IDS) · Mobile Ad hoc Network (MANET) · Monitoring node · Security · Zero knowledge technique

INTRODUCTION

A Mobile Ad hoc network (MANET) is a collection of mobile nodes in which the nodes communicate with each other without the help of any fixed infrastructure. The connections of nodes with one another are made through wireless radio waves and they dynamically change without using the management or infrastructure of the existing networks. There are important problems in this network, problems such as routing and security. For these problems various solutions and algorithms in different situations are presented, still there are certain difficulties left. In contrast with other networks which use specific nodes for supporting packet forwarding, routing and managing the network, the MANETs operate with all the nodes of the network [1-3].

The MANETs have been used in military and non-military applications such as search and rescue missions, sensor networks and etc. The wireless nature and the mobile environment of these networks make them vulnerable to attacks from attackers. Attacking these networks is in the forms of either inactive eavesdropping or active interventions. In wired networks, the attacker must have physical access to the wires of the network or pass through defending lines of the firewalls and gateways; but in a wireless network, the attacker can attack from every direction and to all nodes. So, MANETs do not have a clear defending path and each node has to be prepared to confront the attacker. In MANETs, since all nodes are able to move independently, they can be conquered, compromised with, or stolen. So, nodes and infrastructure of the network must be prepared to operate in non-trust situations. In addition, the lack of a centralized authority provides a context for attackers to start new attacks [4]. Kim and *et al*. [5] proposed a monitoring node selection method in MANET, but in this method, selected node can be an unauthorized node.

In this paper, we have presented a two phase scheme for the detection of authorized nodes followed by the selection of monitoring nodes in MANETs. The scheme is able to detect the main network functions in network layer and link layer. The first phase is based on zero knowledge technique which does not rely on the algorithms of symmetric or asymmetric encryption, digital signatures, sequence numbers and time stamps to identify nodes. This technique is based on proofs. So, the proposed method can be used in MANET Intrusion Detection Systems (IDSs).

Corresponding Author: Dr. Marjan Kuchaki Rafsanjani, Department of Computer Engineering, Science and Research Branch, Islamic Azad University (IAU), Tehran, Iran

Authentication and key management problems: The methods of the initial authentication over users' mobile phones were reflected in the networks. 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 [6,7].

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 [8]. 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 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 and *et al*. [2] 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 Global System for Mobile (GSM) networks, Asadpour and *et al*. [9] presented a new anonymity scheme for anonymous authentication of users. Anonymity can be provided for the mobile users through encrypting the real identity or assigning some kind of alias (es). Either symmetric or asymmetric cryptography can be employed for encryption.

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.

The Detection Scheme: So far the methods presented in respect to authentication or detection in Ad hoc networks act in this way that they first detect current vulnerabilities and then for such threats either they have improved the existing protocols or have proposed a new one. Since these solutions are designed only for specific attack models, as a result, they work only for those specific attacks and would have difficulties in confrontation with new attacks [10,11].

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

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. Data link layer protocols provide the connections between neighbouring 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 [12-14].

The presented scheme includes two phases. In the first phase of the detection procedure, it is tried to detect the authorized nodes through a non-interactive zero knowledge technique. This phase of our scheme is based on first phase of Komninos and *et al*.'s framework [12]. Then in the second phase, from among authorized nodes, the ones which have higher battery power would be determined as monitoring nodes.

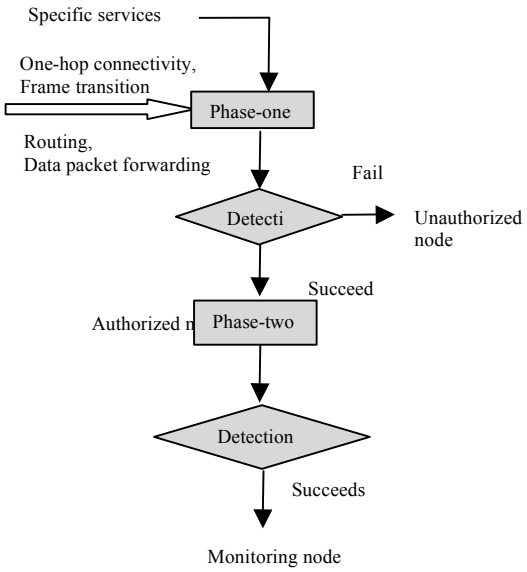

Fig. 1: Detection scheme of authorized nodes and identifying monitoring nodes in MANET

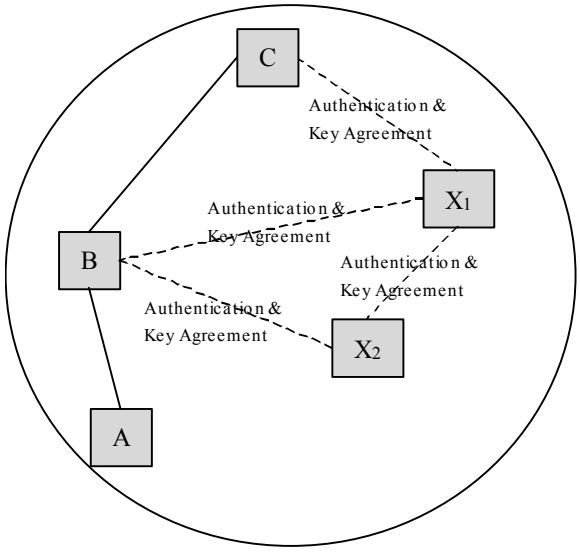

Fig. 2: Entering new nodes X_1 and X_2 to the MANET

Detecting authorized nodes phase: When one or a few nodes are linked to MANET, the procedure of detecting authorized 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.

Consider Fig. 2 in which A, B and C nodes are verified [12]. When node X_1 enters the MANET, its authentication action is done by neighbouring nodes B and C. As it is seen in the Fig. 2, new routes will be built between nodes. For example, as soon as node X1 arrives in MANET, Its authentication will be verified by its closest nodes that is nodes B and C. At this time node X_1 is an authorized node in the network. Then with the entrance of node X_2 into the MANET, nodes X_1 and B which are the closest to it would verify its identity. As soon as nodes X_1 and X_2 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. For example, the provably secure authentication scheme could be applied as a proper method in the first phase of detecting mechanism. Such a scheme is better than a computationally secure authentication scheme because its security depends on discrete interactive of a known computational problem (such as discrete logarithm problem) and does not necessarily need to use a symmetric or an asymmetric encryption algorithm. So, we do authentication by a zero knowledge protocol. In such protocols, nodes must exchange messages. In reference to these interactions the proofs are the probable proofs not the absolute proofs. 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, in Fig. 2, 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):

$$k_1.x_1 + k_2.x_2 = b(\text{mod } p) \quad (1)$$

k_1 and k_2 are integers and p is the prime number [12].

In the protocol, node X_1 first computes the y_3 and y_4 ($y_3= {}_3^{x3}$, $y_4= \alpha_4^{x4}$) then solves the equation (2) for integers x_3 and x_4:

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

Then the following messages are exchanged:

$$B, \leftarrow C\ X1: y_5 = \alpha_1^{x_3},\ y_6 = \alpha_2^{x_4} \quad (M1)$$

$$B,C \rightarrow X1: y_7 = H(\alpha_1, \alpha_2, y_1, y_2, k_1, k_2, b, y_5, y_6) \quad (M2)$$

$$B,C\ X1: y_8 = x_3 - y_7 . x_1 \pmod p,\ y_9 = x_4 - y_7 . x_2 \pmod p \quad (M3)$$

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 with the α_1 and α_2 bases 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 $y_{10} = \alpha_1^{y8}.y_1^{y7}$ and $y_{11} = \alpha_2^{y9}.y_2^{y7}$, then it is examined to see whether y_7 is an equivalent to y_{12}, when $y_{12}=H(\alpha_1,\alpha_2,y_1,y_2,k_1,k_2,b,y_{10},y_{11})$ and if the equation (3) is accurate:

$$k_1 . y_8 + k_2 . y_9 = -y_7 . b \pmod p \quad (3)$$

Firstly, it is seen that nodes B and C are always successful in making a reliable proof because $y_{10} = y_5$ and $y_{11} = y_6$.

$$y_{10} = \alpha_1^{y_8}.y_1^{y_7} \overset{y_8, y_1}{=} \alpha_1^{x_3 - y_7 . x_1}.\alpha_1^{x_1 . y_7} = \alpha_1^{x_3} = y_5,$$

$$y_{11} = \alpha_2^{y_9}.y_2^{y_7} \overset{y_9, y_2}{=} \alpha_2^{x_4 - y_7 . x_2}.\alpha_2^{x_2 . y_7} = \alpha_2^{x_4} = y_6.$$

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.

Secondly, suppose that the E attacker, which does not know x_1 and x_2, will be able to compute these proofs. Because reversing the y_7 one-way Hash function is difficult, we suppose that the y_{10} and y_{11} values before computing y_7 in M2 message were constant and also it seems to be necessary when the y_{10} and y_{11} values are constant, nodes B and C would be prepared for other possible messages. But this notion means that E also can compute different presentations of the y_{10} and y_{11} based on α_1, y_1 and α_2, y_2 which indicate the knowledge of x_1 and x_2, discrete logarithms of y_1, y_2 based on α_1, α_2. But this would contradict the hypothesis of E does not know x_1 and x_2.

Thirdly, nodes B and C, for verification, will replace the responses y_8 and y_9 in the equation (3):

$$k_1 y_8 + k_2 y_9 \overset{y_8, y_9}{=} k_1.(x_3 - y_7.x_1) + k_2.(x_1 - y_7.x_2)$$

$$= k_1 . x_3 - k_1 . y_7 . x_1 + k_2 . x_4 - k_2 . y_7 . x_2$$

$$= k_1 . x_3 - k_2 . x_4 - y_7 . (k_1 . x_1 + k_2 . x_2)$$

$$\overset{(1),(2)}{=} - y_7 . b \pmod p$$

And the identity of the node X_1 is known reliable. From successful authentication of node X_1 we conclude that the considered node is authorized to the specific applications in the MANET [12].

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 neighbouring 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 [15].

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 authorized nodes are determined in the first phase; in the second phase, from among them, the nodes which have higher battery power would be selected as the monitoring nodes. In this phase, the mobile nodes with the highest battery power among neighbouring nodes would be

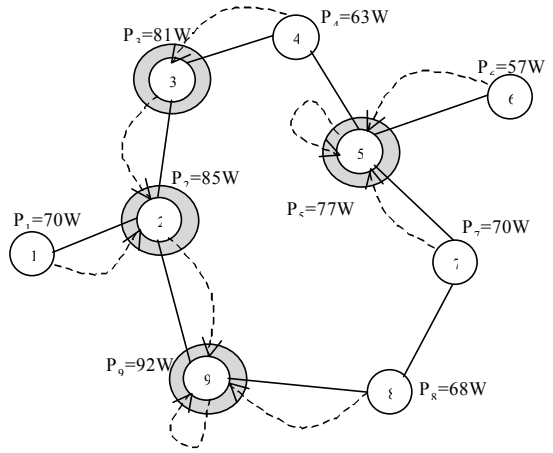

Fig. 3: Selecting monitoring nodes in network

selected as the monitoring nodes. Consider node i, its neighbouring nodes are the ones which are placed about one-hop from it. N^i is the set of the neighbouring 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 following equation:

$$i^* = \arg\max_{j \in N^i} P_j \quad (4)$$

In the Ad hoc networks, each node sends a periodically controlled packet including battery power value to its neighbouring nodes. So, all nodes always know their neighbouring nodes' battery power value. Then, to select the monitoring node, each node must vote. For example, in Fig. 3, a graph structured of nine nodes is seen [5].

Consider node 2, the neighbouring nodes are 1, 3 and 9; Also all of them are authorized nodes. When node 9 has the highest battery power, node 2 sends a vote packet to node 9 and this process is done for each node. The node which would receive at least one vote becomes a monitoring node and the monitoring sensors of the network is loaded and executed. The selected nodes for hosting the monitoring sensors are shown in deep colours. We see that 4 of the 9 nodes of all nodes of the network function as the monitors of the network. 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 neighbouring nodes, the process of selecting the monitoring node must be performed again (equation (5)).

$$P_{i^*} < \min_{j \in N^{i^*}} P_j \quad (5)$$

In the equation (5), N^{i^*} is the set of neighbouring nodes of monitoring node i^* [5].

Performance measurement: This method will improve the lifetime of the network among nodes by evenly distributing of the usage of the resources. To measure the performance, the selected nodes for hosting the monitoring sensors in the 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 (6):

$$E = (m^t s^t + b^t) + (m^r s^r + b^r) + (m^o s^o + b^o) + (m^m s^m + b^m) \quad (6)$$

In equation (6), 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 [16]. Since in this scheme, the monitoring nodes are selected according to the connectivity and the battery power, therefore, monitoring nodes change constantly. Kim and *et al*. [5] presented a monitoring node selection scheme for intrusion detection in mobile ad hoc network, so that selected node as the monitoring node can be an unauthorized node. The advantage of our method is that the monitoring nodes are chosen among authorized 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 neighbourhood, or changes in its routing table and etc. [10,17-20]. 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.

CONCLUSIONS

Security of mobile ad hoc networks (MANET) is a more sophisticated problem than security in other networks, because of open nature, lack of infrastructure, lack of central management, nodes mobility and change of dynamic topology. So, the issue of security is very important and in order to detect intrusion in these networks, it is necessary to identify the authentication of the participating nodes in the network. In this paper, we have presented a scheme in which, at first, the nodes apply the non-interactive zero knowledge technique to

exchange information for their authentication; therefore, the unauthorized nodes are identified. Then in the next phase, from among the authorized nodes, the ones which have high energy power are considered as the monitoring nodes. Due to their having several tasks, the monitoring nodes consume more energy in the MANET in intrusion detection.

REFERENCES

1. Chlamtac, C.M. and J.N. Liu, 2003. Mobile Ad Hoc Networking: Imperatives and Challenges. Ad Hoc Networks, 1(1): 13-64.
2. Hubaux, J.P., L. Buttyan and S. Capkun, 2001. The Quest for Security in Mobile Ad Hoc Networks. In Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Long Beach, CA, USA, pp: 146-155.
3. Haghpanah, M., M. Akhoondi, M. Kargar and A. Movaghar, 2007. Trusted Secure Routing for Ad Hoc Networks. In Proceedings of the 5th ACM International Workshop on Mobility Management and Wireless Access (MOBIWAC), Chania, Greece, pp: 176-179.
4. Otrok, H., M. Debbabi, C. Assi and P. Bhattacharya, 2007. A Cooperative Approach for Analyzing Intrusions in Mobile Ad Hoc Networks. In the Proceedings of the 27th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'07), pp: 86-86.
5. Kim, H., D. Kim and S. Kim, 2006. Life-time Enhancing Selection of Monitoring Nodes for Intrusion Detection in Mobile Ad Hoc Networks. Intl. J. Elect. Comm., 60(3): 248-250.
6. Venkatraman, L. and D.P. Agrawal, 2000. A Novel Authentication Scheme for Ad Hoc Networks. In Proceedings of the 2nd IEEE Wireless Communications and Networking Conference, Chicago, pp: 1268-1273.
7. Ngai, E.C.H., M.R. Lyu and R.T. Chin, 2004. An Authentication Service Against Dishonest Users in Mobile Ad Hoc Networks. In Proceedings of IEEE Aerospace Conference, pp: 1275-1285.
8. Zhou, L. and Z.J. Haas, 1999. Securing Ad Hoc Networks. IEEE Network Magazine Special Issue on Network Security, 13(6): 24-30.
9. Asadpour, M., B. Sattarzadeh and A. Movaghar, 2008. Anonymous Authentication Protocol for GSM Networks. International Journal of Security and Networks, 3(1): 54-62.
10. Zhang, Y. and W. Lee, 2000. Intrusion Detection in Wireless Ad-hoc Networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, pp: 275-283.
11. Zhang, Y., W. Lee and Y. Huang, 2003. Intrusion Detection Techniques for Mobile Wireless Network. Wireless Networks J., 9(5): 545-556.
12. Komninos, N., D. Vergados and C. Douligeris, 2007. Detecting Unauthorized and Compromised Nodes in Mobile Ad Hoc Networks. Elsevier Ad hoc networks, 5(3): 289-298.
13. Kong, J., 2002. Adaptive Security for Multi-layer Ad Hoc Networks. Special Issue of Wireless Communications and Mobile Computing, John Wiley InterScience Press.
14. Kuchaki Rafsanjani, M. and A. Movagahr, 2008. Identifying Monitoring Nodes in Mobile Ad Hoc Networks using Zero Knowledge Technique in Mathematics Science. In Proceedings of the 3rd Intl. Conf. Mathematical Sci., (ICM2008), UAE.
15. Chang, J.H. and L. Tassiulas, 2000. Energy Conserving Routing in Wireless Ad-hoc Networks. In Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM2000), pp: 22-31.
16. Feeney, L.M. and M. Nilsson, 2001. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM2001), pp: 1548-1557.
17. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment. In Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp: 255-265.
18. Nadkarni, K. and A. Mishra, 2003. Intrusion Detection in MANETs - the Second Wall of Defense. In Proceedings of the 29th IEEE Indust. Elect. Soc. Conf., pp: 1235-1239.
19. Manikopoulos, C. and L. Ling, 2003. Architecture of the Mobile Ad-hoc Network Security (MANS) System. In Proceedings of the IEEE International Conf. Syst., Man Cybernetics, pp: 3122-3127.
20. Partwardhan, A., J. Parker, A. Joshi, M. Iorga and T. Karygiannis, 2005. Secure Routing and Intrusion Detection in Ad-hoc Networks. In Proceedings of the 3rd IEEE Intl. Conf. Pervasive Comput. Comm., pp: 191-199.