WALAILAK JOURNAL

http://wjst.wu.ac.th Engineering and Physical Sciences

Identifying IDS Agent Nodes Based on 3-Layered Key Management Framework for MANET

Marjan KUCHAKI RAFSANJANI[1,2,*]

[1]Department of Information Technology, Institute of Science and High Technology and Environmental Science, Graduate University of Advanced Technology, Kerman, Iran
[2]Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran

([*]Corresponding author's e-mail: kuchaki@uk.ac.ir)

Received: 31 December 2012, Revised: 5 May 2013, Accepted: 16 December 2013

Abstract

Nowadays, Mobile Ad Hoc Networks (MANETs) have become one of the most important networks in advanced technologies. However, MANETs are more vulnerable than wired and wireless networks to active and passive attacks. So, security and intrusion detection are very important in these networks. In this paper, we have presented a method of identifying IDS agent nodes in MANET. Whereas, IDS agent nodes due to monitoring activities in Intrusion Detection Systems (IDSs) need more battery energy than other nodes in the network. In the first step, our method uses a 3-layered key management framework in order to authenticate and then in the second step, nodes with higher battery power from among authorized nodes as IDS agent nodes are considered. Therefore, with this method, some authorized nodes contribute in monitoring activities and the network lifetime will be increased and also communication cost in the 3-layered key management framework is less than other frameworks, thus communication performance will be increased.

Keywords: Mobile Ad hoc Network (MANET), authentication, intrusion detection, key management, IDS agent node

Introduction

Mobile Ad hoc Networks (MANETs) have many well known applications in military tactics, law enforcement, emergency rescue, and other security-sensitive environments. So, there is an increasing need to develop highly secure Mobile Ad hoc Networks [1,2]. The security of MANET is a more complicated problem than security in other networks, because of the open nature, lack of fixed infrastructure, absence of centralized control, wireless node's mobility and change of dynamic topology. Therefore, security is a very important issue and in order to detect intrusion in these networks, it is necessary to identify the authentication of the participating nodes in the network [3].

Security solutions have relied on cryptography and proposed the existence of an infrastructure for providing and managing keys, but key management in MANETs due to the lack of any central infrastructure is a challenge [4]. 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 [3]. Intrusion detection can be considered as a second line of defense for network security, and IDS agent nodes have an important role in intrusion detection systems.

The rest of the paper is organized as follows. Intrusion detection is defined in the next section. Then, we summarize key management and access control as well as some approaches to them in MANET. After that,our proposed method is described, so that it includes nodes' authentication and identifying IDS agent nodes. In the next section, we analyze the communication cost and the energy consumption in our method. Finally, we conclude the paper and give future research directions.

Intrusion detection

Intrusion mainly refers to unauthorized use of system resources, which may cause deletion and damages to system data and even such results as the system refusing to offer services to legal users. Intrusive behaviors occur due to either illegal use of system resources by external intruders or unauthorized use of system resources by internal intruders [5].

Intrusion Detection System (IDS) can detect and identify intrusive behaviors in a computer system by monitoring and analyzing network packet or system audit log, and then send intrusion alerts to system administrators in real time [6]. 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 grow too. Intrusion detection is the 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 IDSs. 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, the 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. IDSs can be divided into 3 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 neighbouring nodes, it is responsible for detecting signs of intrusion locally and independently. However, neighbouring nodes can collaboratively exchange messages in the case of an unauthorized situation or confirmed intrusion detection [10].

Key management and access control

There are many authentication protocols for wireless networks that most of them are designed for fixed infrastructure networks and their re-authentication procedures are slow and costly. So, these protocols are not suitable for MANET nodes. Recently, several authentication schemes have been presented that have reduced authentication time. However, they rely on a centralized authentication authority inside the network, that MANETs are lack of these control centers. Protocols for authentication without a centralized Certificate Authority (CA) and fast re-authentication have been proposed, but these protocols often assume nodes are not mobile or nodes have a lot of resources [11].

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 CA. Security requirements are very important for CAs because they can encounter many attacks.

In conventional networks, the 2 main solutions for public key management are Pretty Good Privacy (PGP) [12] and the X.509 public key infrastructure. The X.509 in comparison to PGP has a strong hierarchy. Ad hoc networks have been trying to eliminate the need for a centralized CA in key management methods. In the first method, there is one CA with distributing parts of the secret key on several nodes [13].

Hubaux *et al.* [14] proposed a public key distribution based on a trust building scheme for Ad hoc networks. In this scheme, there are no central certificate directories for the distribution of certificates. In fact, Zhou and Haas [13] were the first to address public key management in the MANET, and also applied a threshold approach to make it decentralized and robust.

PGP-like (PL) is one of the survival key management initiatives for MANETs [15]. This system handles the public key management problem and proposes a fully distributed self-organizing public key management infrastructure. PL is based on the PGP and each node is responsible for creating its public and private keys. Certificates in PL are stored, distributed and managed by the nodes in a fully self-organized manner. Joshi *et al*. [16] proposed a fully distributed certificate authority scheme based on secret sharing and redundancy called Joshi's approach (JA). URSA is a ubiquitous, decentralized, self controlled and robust access control solution for MANETs, where no single node monopolizes the access decision or is assumed to be completely trusted. Certifications are based on the RSA cryptosystem and on threshold cryptography based signature [17,4].

Clustered Mobile Ad Hoc Network makes it more scalable. The MANET is clustered into 2 layers: the gateway nodes are the first layer; the cells under each gateway node are the second layer. Many key management schemes have been proposed based on this 2-layered virtual infrastructure. The 2-layered key management approach is used to improve computational efficiency [18,19]. It applies a centralized key management scheme to the cells and a distributed key management scheme to the gateway nodes to avoid a single point of failure.

In the 2-layered virtual infrastructure for MANET, because of the locations and the connections, many nodes are located in the first layer, and the first layer will be separated into 2 layers. Thus, the MANET will have a 3-layered virtual infrastructure. In this case, a 3-layered key management approach is needed. Therefore, there are four possible key management architectures for 3-layered MANET: centralized, distributed, 2-distributed-1-centralized (DDC) and 2 centralized-1-distributed (DCC). The centralized and distributed ones are not suitable for large MANET [20].

Sun and Yu [20] introduced the 3-layered key management architectures. The MANET nodes in the first layer are the gateway nodes; the MANET nodes in the second layer are second layer gateway nodes or sub-gateways and the third layer MANET nodes are called cells.

Our proposed method

Our method contains 2 steps which are described in detail below;

Detecting authorized nodes based on DCC framework

This step of our method is based on one of Sun's frameworks. It is the 3-layered group key management architecture [20]. With this architecture, the identity of nodes would be specified. When MANET is initialized, the MANET group key should be generated and distributed to all nodes. The group key management architecture that we apply for authentication is a DCC (2-centralized-1-distributed) framework. In DCC, each gateway node in the first layer will generate and distribute a sub-group key for the sub-gateways under its control using a centralized key management scheme. Then, the sub-gateway will distribute this key as its cell-group key to the cells under its control. The group key for the MANET will be calculated based on each sub-group key using a distributed key management algorithm. Thus, in this framework, the first layer uses a distributed key management scheme, but the second and third layer use a centralized key management scheme.

When one node connects to MANET, the group key should be refreshed to guarantee the backward security in order that the new node cannot access information before its connection. If the connection of the new node makes a new gateway or sub-gateway, the group key should be initiated. Otherwise, the new node is a cell, the cell-group key should be refreshed, and then the sub-group key and the group key should be recomputed layer by layer again.

On the other hand, when one node leaves the MANET, the group key should be changed to guarantee the forward security in order that the left node cannot access the MANET again. Connecting and leaving a node are different under the situation of the gateway layer and the sub-gateway layer. The group key will either be initiated or be recomputed from the related bottom layer to the top layer singly. When one node comes into the MANET, in spite of the network topology changing, the group key doesn't need to be refreshed at once. The group key refreshes periodically to make the key management framework suitable for MANET [20]. So, nodes in the MANET are authorized nodes and they can have access to specific applications or services in the network.

Identifying IDS agent nodes

IDS agents set up on some nodes and contribute in intrusion detection, so that collect and analyze all packets in the communication area. So, these nodes use the extra resources and energy. In the most of the existing intrusion detection systems for MANETs [9,21,22] IDS agents in order to detect intrusions load and run on all the nodes. So, all nodes are monitoring nodes in the MANET.

Since, the battery power of the nodes in MANETs is limited, there is a need for an efficient method of utilizing these resources to construct intrusion detection systems. The network lifetime is the time that the first node failure happens due to a decrease in the power of the battery [23]. So, in order to improve the network lifetime, a method in selecting IDS agent nodes is needed so that a required level of detection intrusion in MANETs would be provided. Therefore, in the proposed method, after the nodes' authentication step, then, from among them, the nodes which have higher battery power would be selected as the IDS agent 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 IDS agent node which is searched for every node i, according to equation (1);

$$i^* = \arg\ \max_{j \in N^i} P_j \tag{1}$$

In ad hoc networks, each node sends a periodically controlled packet including battery power value of its neighbouring nodes. So, all nodes always know their neighbouring node's battery power value. Then, each node must vote to select the IDS agent node. The node which receives at least one vote becomes an IDS agent node and the agent sensors on the network is loaded and executed. Whenever the condition of the connectivity changes or whenever the remaining battery power of an IDS agent node becomes lower than the lowest battery power among the neighbouring nodes according to (2), the process of identifying an IDS agent node must be performed again [24,25]. In (2), N^{i^*} is the set of neighbouring nodes of the IDS agent node *i**.

$$P_{i^*} < \min_{j \in N^{i^*}} P_j \tag{2}$$

Analysis of the communication cost and energy consumption

The communication cost that we have applied in the first step of our proposed method for DCC key initialization is CDCC-I; for node connection it is CDCC-C and for nodes leaving it is CDCC-L;

$$C_{DCC-I} = 2*N3+3N2+N1*(\log_2 N_1+1) \tag{3}$$

$$C_{DCC-C} = \alpha * C_{DCC-I} + (1-\alpha)(2*\sum_{i=1}^{N2} P_{3i} * \log_2 N_{3i} + N1 * \log_2 N_1 + N2 + N1) \tag{4}$$

$$C_{DCC-L} = \beta * C_{DCC-I} + (1-\beta)(\sum_{i=1}^{N2} P_{3i} * \log_2 N_{3i} + N1 * \log_2 N_1 + N2 + N1) \tag{5}$$

In the above equations, *N* is the node number of the MANET. N_1 is the gateway nodes number (first layer). N_2 is the sub-gateway nodes number (second layer). N_3 is the cells nodes number (third layer). α and β are the possibility when nodes connect or leave the MANET and infrastructure needs to refresh. P_{3i} is the nodes connection possibility to the cells. N_{3i} is the cells nodes number under each sub-gateway node. When cells nodes averagely locate under the second layer sub-gateways, the key management cost will be optimized, and also when the number of gateways is limited in a relatively small range, the DCC key management scheme is appropriate for the 3-layered key topology [20].

To measure the performance in the second step of our method, IDS agent nodes collect all the packets in their communication area and analyze them in order to detect intrusions. The energy used by an IDS agent node during an interval of Δt is computed by (6);

$$E = (m^t s^t + b^t) + (m^r s^r + b^r) + (m^o s^o + b^o) + (m^m s^m + b^m) \tag{6}$$

In Eq. (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 [26]. Since in this method, IDS agent nodes are selected according to authentication, connectivity and battery power, therefore, they change continuously. Kim *et al*. [24] presented a monitoring node selection scheme for intrusion detection in a 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 IDS agent nodes are chosen among authorized nodes [27]. On the other hand, in the most of the existing intrusion detection systems for MANETs, an IDS agent in order to detect intrusions loads and runs on every node [9,21], but in our method some nodes identify as IDS agent nodes.

Conclusions

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. Sun and Yu showed that when the number of gateway nodes in the first layer in MANET keeps in a small scale, the 2-centralized-1-distributed (DCC) framework is more suitable. The 3-layered key management architecture can attain less communication cost compared with the 2-layered ones. Applying a centralized key management scheme for MANET is difficult due to lack of central management. Also the distributed key management schemes are not suitable for MANET because of large computation and communication cost. So, we applied a 3-layered key management framework (DCC) in the first step of our method for improving authentication efficiency. On the other side, power resources and rare computational of mobile nodes in MANETs impose heavy limitations on the functionality of an effective intrusion detection system. Our method in the second step selects the IDS agent nodes with largest energy power. Also we analyzed the performance of the proposed scheme theoretically. Our method could improve intrusion detection in the area of security. In the future, we will simulate the method and evaluate its performance to encounter some attacks and also we will consider detecting compromised nodes in this framework before identifying IDS agent nodes.

Acknowledgement

The author has been supported by Institute of Science and High Technology and Environmental Science, Graduate University of Advanced Technology, Kerman, Iran. The author is extremely grateful to the referees for giving valuable comments and helpful suggestions which helped to improve the presentation of this paper.

References

[1] N Saxena, G Tsudik and JH Yi. Efficient node admission and certificateless secure communication in short-lived MANETs. *IEEE Trans. Parall. Distr. Sys*. 2009; **20**, 158-70.

[2] M Yu, M Zhou and W Su. A secure routing protocol against Byzantine attacks for MANETs in adversarial environments. *IEEE Trans. Veh. Tech*. 2009; **58**, 449-60.

[3] MK Rafsanjani and A Movaghar. Identifying monitoring nodes with selection of authorized nodes in mobile ad hoc networks. *World Appl. Sci. J.* 2008; **4**, 444-9.

[4] MN Lima, AL Santos and G Pujolle. A survey of survivability in Mobile Ad hoc Networks. *IEEE Comm. Surv. Tuto.* 2009; **11**, 66-77.

[5] X Bao, T Xu and H Hou. Network intrusion detection based on support vector machine. *In*: Proceedings of the International Conference on Management and Service Science, Wuhan, 2009, p. 1-4.

[6] W Yang, W Wan, L Guo and LJ Zhang. An efficient intrusion detection model based on fast inductive learning. *In*: Proceedings of the 6th International Conference on Machine Learning and Cybernetics, Hong Kong, 2007, p. 3249-54.

[7] P Brutch and C Ko. Challenges in intrusion detection for wireless ad-hoc networks. *In*: Proceeding of the Symposium on Applications and the Internet Workshops, USA, 2003, p. 368-73.

[8] M Kuchaki Rafsanjani, A Movaghar and F Koroupi. Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes. *In*: Proceedings of the World Academy of Science, Engineering and Technology, Italy, 2008, p. 351-5.

[9] Y Zhang, W Lee and Y Huang. Intrusion detection techniques for mobile wireless network. *The ACM/Cluwer Wirel. Net. J.* 2003; **9**, 545-56.

[10] N Nasser and Y Chen. Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. *In*: Proceedings of the IEEE International Conference on Communications, Glasgow, 2007, p. 1154-9.

[11] JT Chang, S Gundala, TS Moh and M Moh. VESS: a versatile exrensible security suite for MANET routing. *In*: Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2009, Victoria, BC, 2009, p. 944-50.

[12] PR Zimmermann. *The Official PGP User's Guide*. MIT Press, Cambridge, MA, 1995.

[13] L Zhou and ZJ Haas. Securing ad hoc networks. *IEEE Network Mag.* 1999; **13**, 24-30.

[14] JP Hubaux, L Buttyan and S Capkun. The quest for security in mobile ad hoc networks. *In*: Proceedings of the 2nd ACM International Symposium on Mobile ad Hoc Networking and Computing, New York, 2001, p. 146-55.

[15] S Capkun, L Buttyan and JP Hubaux. Self-organized public key management for mobile ad hoc networks. *IEEE Trans. Mobile Comput.* 2003; **2**, 52-64.

[16] D Joshi, K Namuduri and R Pendse. Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: an analysis. *EURASIP J. Wireless Comm. Network.* 2005; **4**, 579-89.

[17] W Stallings. *Cryptography and Network Security*. 4th ed. Prentice Hall, 2006.

[18] KH Rhee, YH Park and G Tsudik. A group key management architecture for mobile ad-hoc wireless networks. *J. Info. Sci. Eng.* 2005; **21**, 415-28.

[19] S Bin and Y Bin. A hierarchical key management scheme for MANET. *In*: Proceedings of the International Conference on Communication Technology, Guilin, China, 2006, p. 1-4.

[20] S Bin and Y Bin. The Three-layered group key management architecture for MANET. *In*: Proceedings of the 11th International Conference on Advanced Communication Technology, Phoenix Park, 2009; **2**, 1378-81.

[21] B Sun, K Wu and UW Pooch. Alert aggregation in Mobile Ad Hoc networks. *In*: Proceedings of the 2nd ACM Workshop on Wireless Security, New York, 2003, p. 69-78.

[22] D Steme, P Balasubramanyam, D Carman, B Wilson, R Talpade, C Ko, R Balupari, CY Tseng, T Bowen, K Levitt and J Rowe. A general cooperative intrusion detection architecture for MANETs. *In*: Proceedings of the 3rd IEEE International Workshop on Information Assurance, Washington, DC, 2005, p. 57-70.

[23] JH Chang and L Tassiulas. Energy conserving routing in wireless ad-hoc networks. *In*: Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies, Tel Aviv, 2000, p. 22-31.

[24] H Kim, D Kim and S Kim. Life-time enhancing selection of monitoring nodes for intrusion detection in Mobile Ad Hoc Networks. *Int. J. Electro. Commu.* 2006; **60**, 248-50.

[25] M Kuchaki Rafsanjani, AA Khavasi and A Movaghar. An efficient method for identifying IDS agent nodes by discovering compromised nodes in MANET. *In*: Proceedings of the 2nd International Conference on Computer and Electrical Engineering, UAE, 2009, p. 625-9.

[26] LM Feeney and M Nilsson. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. *In*: Proceedings of the 12th Annual Joint Conference of the IEEE Computer and Communications Societies, Anchorage, AK, 2001, p. 1548-57.

[27] M Kuchaki Rafsanjani, AA Khavasi and A Movaghar. An effective approach for determining IDS agent nodes in MANET. *In*: Proceedings of the 3rd International Conference on Internet Technology and Applications, UK, 2009, p. 458-65.