Indian Journal of Science and Technology Vol. 3 No. 10 (Oct 2010) ISSN: 0974- 6846

Generalized mechanism for intrusion detection in mobile ad hoc networks

Marjan Kuchaki Rafsanjani
Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran
kuchaki@mail.uk.ac.ir

Abstract

In recent years, intrusion detection techniques have been the research spots in the field of Mobile Ad hoc Networks (MANETs). Whereas, as kind of wireless and mobile networks, network traffic and network scale increase continually, some current intrusion detection methods can't meet the requirement of the network security for network lifetime efficiency and communication cost. In order to improve authentication and monitoring activities for Intrusion Detection Systems (IDS) in Mobile Ad hoc Networks, a method for recognizing monitoring nodes with authorized nodes and higher battery power is designed and analyzed. Therefore, with this method, some authorized nodes contribute in monitoring activities and the network lifetime will be increased and also communication cost will be decreased.

Keywords: Authentication, DCC framework, Energy power, Intrusion detection, Mobile Ad hoc Network (MANET), Monitoring node.

Introduction

Mobile Ad hoc Networks (MANETs), unlike traditional networks, have no fixed infrastructure and central management where Intrusion detection Systems (IDSs) can be deployed. Therefore, each node may need to run an IDS and also cooperate with other nodes to ensure network security (Mohammed *et al*., 2009). This problem is not efficient about energy consumption since mobile nodes have limited energy.

Many methods have been presented to resolve this problem. For example, the approaches that use clustering; the nodes in each cluster select a cluster head to work as the IDS for the whole cluster. The selection process of the cluster head can be either randomly or based on the connectivity of nodes (Huang & Lee, 2003; Kachirski & Guha, 2003). The goal of these methods is reduced the overall energy consumption of intrusion detection systems in the network. Since the nodes have different energy power, so, with these methods some nodes will die faster than others.

Although it is obviously desirable to scales the resource consumption of IDSs among nodes, but this aim is difficult to attain. On the other hand, nodes might be unauthorized nodes in the network. Furthermore, even when all nodes can be authorized nodes, it remains a challenging issue to select an optimal collection of monitoring nodes to balance to overall resource consumption.

The problem of energy balancing exists in many applications especially in IDS schemes. Selecting of monitor node is needed for routing (Basagni, 1999), key distribution (Bechler *et al*., 2004; DeCleene *et al*., 2001) and intrusion detection systems in MANET.

Node Authentication and Key Management

There are two basic key management approaches; public key-based and secret key-based schemes. The public key-based scheme utilizes a pair of public/private keys and an asymmetric algorithm to establish session keys and authenticate nodes.

In the secret key-based scheme, a private key is a symmetric key shared by two nodes, which is used to verify the data integrity. Although a public key management system can be totally self-organized, the initial trust among the nodes in a network is still built by using external mechanisms. For example, in (Capkun *et al*., 2003) proposed such a system by constructing a local Certificate Repository (CR) for each node. At first, there is a Public Key Infrastructure (PKI) or Certificate Authority (CA) to distribute the knowledge among users. Therefore in this approach, there is a dynamic maintenance mechanism in building up the certificates.

There are several methods to set up the shared keys: the first method is bootstrap the shared keys from a PKI, which might be a tough assumption for MANETs. The second method, use a key distribution center, which has a shared key for each node, to construct a shared key between two nodes by using the Kerberos protocol, and the third method, embedding the shared keys in each node during its initialization. The third method is more practical for many MANET applications (Yu *et al*., 2009).

There are protocols on authentication without a centralized CA and fast re-authentication, but these protocols often assume nodes are not mobile or nodes have a lot of resources (Chang et al, 2009).

Zhou and Haas (Zhou & Hass, 1999) are the first to address public key management in MANET, and also applied threshold approach to make it decentralized and robust.

PGP-like (PL) is one of the survivable key management initiatives for MANETs (Capkun et al, 2003). 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. Joshi et al. (Joshi et al, 2005) proposed a totally distributed certificate authority scheme based on secret sharing and redundancy is called Joshi's approach (JA). And URSA is a ubiquitous, decentralized, self

Indian Journal of Science and Technology Vol. 3 No. 10 (Oct 2010) ISSN: 0974- 6846

controlled and robust access control solution for MANETs (Stallings, 2006; Lima *et al*., 2009).

From the other point of view, clustered mobile ad hoc network makes it more scalable. The MANET is clustered into two layers: the gateway nodes are the first layer; the cells under each gateway node are the second layer. It uses 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. Many key management schemes have been proposed based on this two-layered virtual infrastructure. The two-layered key management approach is used to improve computation efficiency (Rhee *et al*., 2005; Sun & Yu, 2006).

In the two-layered framework schemes for MANET, many nodes will locate in the first layer, and the first layer will be separated into two layers. Thus, the MANET will have a three-layered framework. So, a three-layered key management approach is needed. Sun and Yu (Sun & Yu, 2009) introduced the three-layered key management architectures. There are four possible key management architectures for three-layered MANET: centralized, distributed, two-distributed-one-centralized (DDC) and two centralized-one-distributed (DCC). The centralized and distributed architectures are not suitable for large mobile ad hoc networks.

Intrusion Detection

Intrusion detection refers to detection of malicious activity (break-ins, penetrations, and other forms of computer abuse) in a computer related system. These malicious activities or intrusions are interesting from a computer security perspective. An intrusion is different from the normal behavior of the system (Phoha, 2002).

Intrusion Detection Systems classify into host based and network based intrusion detection systems (Denning, 1987). Host based Intrusion Detection Systems deal with operating system call traces. The intrusions are in the form of abnormal subsequences of the traces. The abnormal subsequences translate to malicious programs, unauthorized behavior and policy violations. So, host-based IDS, analyses the events taken place in application programs or the operating systems.

Network based Intrusion Detection Systems deal with detecting intrusions in network data. The intrusions typically occur as abnormal patterns though certain techniques model the data in a sequential mode and detect abnormal subsequences (Atallah *et al*., 2004; Gwadera *et al*., 2005). A network-based IDS, receives packets from the network and analysis them for detecting intrusions (Kuchaki Rafsanjani *et al*., 2008).

Intrusion detection and response systems should be both distributed and cooperative in mobile ad hoc networks in order to accomplish the needs of these networks. For instance, in the architecture proposed in (Zhang *et al*., 2003), 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 case of an unauthorized situation or confirmed intrusion detection (Nasser & Chen, 2007).

The proposed mechanism

In the first phase of the proposed method, a three-layered key management framework is used in order to authentication and then in the second phase, nodes with higher battery power from among authorized nodes as monitoring nodes are considered.

Authentication and Detecting Authorized Nodes

This phase is based on one of Sun's frameworks. It is the three-layered group key management architecture (Sun & Yu, 2009). 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. 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 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 centralized key management scheme. Then, the sub-gateway will distribute this key as its cell-group key for the cells under its control. The group key for the MANET will be calculated based on each sub-group key using distributed key management algorithm. Thus, in this framework, the first layer uses distributed key management scheme, but the second and third layers use 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 to information before its connection. If the connection of the new node makes 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.

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 to 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 separately. When one node comes in MANET, in spite of the network topology is changed, the group key doesn't need to be refreshed at once. The group key refreshes periodically to make the key management architecture suitable for MANET (Sun & Yu, 2009). So, nodes in the MANET are authorized nodes.

Indian Journal of Science and Technology Vol. 3 No. 10 (Oct 2010) ISSN: 0974- 6846

Monitoring Nodes Election

The MANET nodes have limited resources. An efficient approach for reducing the overall resource consumption of intrusion detection is for nodes to recognize a few monitoring nodes among all nodes in the network (Otrok et al, 2008). Monitoring nodes in IDS must collect and analyze all packets in the communication area. So, these nodes consume the extra resources and energy. In the most of the existing IDSs for MANET in order to detect intrusions, all nodes contribute in monitoring activities (Zhang et al, 2003; Sun et al, 2003; Steme et al, 2005). So, in order to improve the network lifetime, a method for selecting monitoring node is needed. Therefore, in the proposed method, after first phase, from among authorized nodes, the nodes which have higher energy resource would be selected as the monitoring nodes. Each node sends a periodically controlled packet including battery power value to its neighbouring nodes. So, all nodes know their neighbouring nodes' battery power value.

In the MANET, consider a node, for example node *i*, its neighbouring nodes are placed about one-hop from it. N^i is the set of the neighbouring nodes which include the node *i* too, and the R_i is the remaining battery power of node *i*. The node *i** is the monitoring node which is searched for every node *i*, according to equation (1):

$$i^* = \arg\max_{j \in N^i} R_j \qquad (1)$$

Then, each node must vote to elect the monitoring node. The node which receives at least one vote becomes a monitoring node and the agent sensors of the network is loaded and executed on them. 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 according to equation (2), the process of recognizing monitoring node must be performed again (Kim et al, 2006; Kuchaki Rafsanjani *et al*., 2009a). In equation (2), N^{i^*} is the set of neighbouring nodes of the monitoring node i* (Kuchaki Rafsanjani *et al*., 2009b).

$$P_{i^*} < \min_{j \in N^{i^*}} P_j \qquad (2)$$

Analysis of the communication cost

The communication cost that has been applied in the first phase of the proposed method for DCC key initialization is $C_{DCC\text{-}I}$; for nodes connection is $C_{DCC\text{-}C}$ and for nodes leaving is $C_{DCC\text{-}L}$:

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

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

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

In above equations, N is the nodes number of MANET. N1 is the gateway nodes number (first layer). N2 is the of sub-gateway nodes number (second layer). N3 is the cells nodes number (third layer). *a, 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, the key management cost will be improved. Moreover, the DCC key management scheme is appropriate for the three-layered key architecture when the number of gateways is limited in a relatively small range (Sun & Yu, 2009).

Analysis of the resource consumption

The used energy by a monitoring node during an interval of Δt is computed by (6):

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

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 the varied and constant energy costs for each operation, and are derived experimentally (Feeney & Nilsson, 2001).

Kim et al. (Kim et al, 2006) presented a monitoring node selection scheme for intrusion detection in mobile ad hoc network, however the monitoring nodes can be unauthorized nodes. 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 (Zhang *et al*., 2003; Sun *et al*., 2003), but in the proposed method some nodes identify as monitoring nodes and another advantage of my method is that the monitoring nodes are chosen among authorized nodes.

Conclusion

Security solutions have relied on cryptography and suppose the existence of an infrastructure for providing and managing keys. Some MANET's characteristics, as the lack of any central infrastructure, make key management a challenge. So, using centralized key management scheme for MANET is difficult. Moreover, the distributed key management schemes are not suitable for MANET because of large computation and communication cost. Three-layered key management architecture, two – centralized – one - distributed (DCC) architecture, can achieve less communication cost when the number of gateway nodes in the first layer in MANET keeps in a small scale. Hence, the three-layered key management architecture (DCC) was applied in the first phase of the proposed mechanism to optimize node authentication efficiency. The proposed method in the second phase selects the monitoring nodes with higher energy power, therefore creates efficient network lifetime.

References

1. Atallah MJ, Szpankowski W and Gwadera R (2004) Detection of significant sets of episodes in event

Indian Journal of Science and Technology Vol. 3 No. 10 (Oct 2010) ISSN: 0974- 6846

sequences. *The Fourth IEEE Intl. Con. on Data Mining*, 3-10.
2. Basagni S (1999) Distributed clustering for ad hoc etworks. *The IEEE Intl. Symp. on Parallel Architectures, Algorithms, & Networks (I-SPAN'99)*. 310-315.
3. Bechler M, Hof H, Kraft D, Pahlke F and Wolf L (2004) A clusterbased security architecture for ad hoc etworks. *The 23th Ann. Joint Con. of the IEEE Computer & Commun (INFOCOM)*. 4, 2393-2403.
4. Capkun S, Buttyan L and. Hubaux JP (2003) Self-organized public key management for mobile ad hoc networks. *IEEE Trans. on Mobile Computing*. 2(1), 52-64.
5. Chang JT, Gundala S, Moh TS and Moh M (2009) VESS: a versatile exrensible security suite for MANET routing. *The IEEE Pacific Rim Con. on Commun., Computers & Signal Processing*. 944-950.
6. DeCleene B, Dondeti L, Griffin S, Hardjono T, Kiwior D, Kurose J, Towsley D, Vasudevan S and Zhang C (2001) Secure group communications for wireless networks. *The IEEE Military Commun. Con. (MILCOM)*. 1, 113-117.
7. Denning DE (1987) An intrusion detection model. *IEEE Trans. of Software Engg*. 13(2), 222-232.
8. Feeney LM and Nilsson M (2001) Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. *The 20th Ann. Joint Con. of the IEEE Computer & Commun. Soci.*1548-1557.
9. Gwadera R, Atallah MJ and Szpankowski W (2005) Reliable detection of episodes in event sequences. *Knowledge & Info. Systems*. 7(4), 415-437.
10. Huang Y and Lee W (2003) A cooperative intrusion detection system for ad hoc networks. T*he ACM Workshop on Security of Ad Hoc & Sensor Networks*. 135-147.
11. Joshi D, Namuduri K and Pendse R (2005) Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: an analysis, *EURASIP J. on Wireless Commun. & Networking*. 4, 579-589.
12. Kachirski O and Guha R (2003) Efficient intrusion detection using multiple sensors in wireless ad hoc networks. *The 36th Hawaii Intl. Conf. on System Sci. (HICSS'03)*, 2, 57.1.
13. Kim H, Kim D and Kim S (2006) Life-time enhancing selection of monitoring nodes for intrusion detection in Mobile Ad Hoc Networks. *Intl. J. of Electronics & Commun.* 60(3), 248-250.
14. Kuchaki Rafsanjani M, Movaghar A and Koroupi F (2008) Investigating intrusion detection systems in MANET and comparing IDSs for detecting misbehaving nodes. *The World Acad. Sci., Engg. & Technol.* 351-355.
15. Kuchaki Rafsanjani M, Khavasi AA and Movaghar A (2009a) An efficient method for identifying IDS agent nodes by discovering compromised nodes in MANET. *The 2nd IEEE Int. Conf. on Computer Electronic Engg*. 625-629.
16. Kuchaki Rafsanjani M, Khavasi AA and Movaghar A (2009b) An effective approach for determining IDS agent nodes in MANET*, The Third Int. Conf. on Internet Technol. & Applications*. 458-465.
17. Lima MN, Santos AL and Pujolle G (2009) A survey of survivability in Mobile Ad hoc Networks. *IEEE Commun. Surveys & Tutorials J.* 11(1), 66-77.
18. Mohammed N, Otrok H, Wang L, Debbabi M and Bhattacharya P (2009) Mechanism design-based secure leader election model for intrusion detection in MANET. *IEEE Tran. on Dependable & Secure Computing*. 99.
19. Nasser N, and chen Y (2007) Enhanced intrusion detection system for discovering malicious nodes in Mobile ad Hoc Networks. *The IEEE Int. Conf. on Commun.* 1154-1159.
20. Otrok H, Mohammed N, Wang L, Debbabi M and Bhattacharya P (2008) A moderate to robust game theoretical model for intrusion detection in MANETs. *IEEE Int. Conf. on Wireless & Mobile Computing, Networking & Commun.* 608-612.
21. Phoha VV (2002) The Springer Internet Security Dictionary. *Springer-Verlag*.
22. Rhee KH, Park YH and Tsudik G (2005) A group key management architecture for mobile ad-hoc wireless networks. *J. of Info. Sci. & Engg*. 21(1), 415-428.
23. Stallings W (2006) Cryptography and Network Security. 4th ed., *Prentice Hall*.
24. Steme D, Balasubramanyam P, Carman D, Wilson B, Talpade R, Ko C, Balupari R, Tseng CY, Bowen T, Levitt K and Rowe J (2005) A general cooperative intrusion detection architecture for MANETs. *The 3rd IEEE Int. Workshop on Info. Assurance*. 57-70.
25. Sun B and Yu B (2006) A hierarchical key management scheme for MANET. *Int. Conf. on Commun. Technol.* 1-4.
26. Sun B and Yu B (2009) The Three-layered group key management architecture for MANET. *Proc. of 1th Int. Conf. on Advanced Commun. Technol.* 2, 1378-1381.
27. Sun B, Wu K and Pooch UW (2003) Alert aggregation in Mobile Ad Hoc Networks. *ACM Workshop on Wireless Security in conjunction with the 9th Ann. Int. Conf. on Mobile Computing & Networking*. 69-78.
28. Yu M, Zhou M and Su W (2009) A secure routing protocol against Byzantine attacks for MANETs in adversarial environments. *IEEE Trans. on Vehicular Technol.* 58(1), 449-460.
29. Zhang Y, Lee W and Huang Y (2003) Intrusion detection techniques for mobile wireless network. *The ACM/Cluwer Wireless Networks J.* 9(5), 545-556.
30. Zhou L and Haas ZJ (1999) Securing ad hoc networks. *IEEE Network Magazine Special Issue on Network Security*. 13(6), 24-30.