A Novel Method Intrusion Detection Based on Sending and Checking Packet for Neighbored Nodes in MANET

Dina Sadat Jalali¹, Alireza Shahrbanooonezhad^{2,*}

¹Sama Technical and Vocational Training College, Islamic Azad University, Shoushtar Branch, Shoushtar, Iran

²Islamic Azad University, Dehloran Branch, Dehloran, Iran

*Corresponding Author: alireza_shahrbanooonezhad@yahoo.com

Copyright © 2014 Horizon Research Publishing All rights reserved.

Abstract Mobile Ad hoc network is a constant infrastructure wireless network whose installation and use are easy and in progress. In this network, nodes in each other's radio range can directly communicate. Furthermore, this network has such properties as nature of transfer medium, finite power and energy, low bandwidth and restricted resources which facilitate intrusion to and destructive action in it. Mobile Ad hoc network does not have special defense mechanisms, resulting in the competition to give strategies and make security and intrusion detection possible. Routing is the most important problem that with this network which is done by nodes. Existence of a malicious node is a problem the routing can handle. This paper will present one new method of intrusion detection that precisely identifies malicious nodes which change the received packets or prevent them through surveying adjacent nodes in a simple way. Through this method, rate of false alarm will be reduced as simulation procedures indicate its superiority.

Keywords Mobile Ad Hoc Network, Security, Intrusion Detection, Malicious Nodes, Dropping Packet, Changing Packet

1. Introduction

An Ad hoc network is a wireless network without fixed infrastructure; thus, it can be setup and used easily [1, 2]. Furthermore, all of the computers in such a network should be in the radio range of each other to make communication possible [3]. These networks along with positive attributes also have some disadvantages including: Memory limitation, bandwidth limitation, low-level processing power and limitation of nodes lifetime. All of this, along with features of media between nodes (radio frequency), has led to the network vulnerability [4, 5].

Routing is the most important problem in ad hoc network which is done by network nodes in a distributed way. An issue that may be difficult for the routing is the existence of a

malicious node between nodes at the network. Due to nodes mobility, the network has a variable topology; therefore, routing at these networks is more difficult than other networks routing and requires its own routing algorithm.

On the other hand, the proposed routing algorithms for this network have low level of security and no action has been performed to protect the network against attacks. Hence, in recent years some solutions have been presented to provide the network security [6, 7]. Routing in these networks is very important. The routing protocol for the ad hoc networks can be divided into three types described below.

A- Proactive Protocol

This protocol is named based on table or table driven. In this routing protocol, the previous routing information is in routing table of each node and, if topology changes, this information will be transmitted to all network nodes, and routing tables will be updated and origin node identifies route of the destination node with information of routing tables of each node and uses them [7, 8].

B- Reactive Protocol

This routing protocol is based on demand. In this protocol, routes are discovered when the origin node communicates to other nodes. Therefore, origin node calls process of route discovery and usually, flooding algorithm uses for route discovery and this routing protocol uses in Ad hoc network, more. Examples of routing algorithm are DSR and AODV. In AODV routing algorithm, origin node produces a RREQ packet and specifies source and destination nodes and then releases this RREQ packet for self adjacent nodes. If each node has a route to the destination node in its memory, it produces RREP Packet; otherwise, it releases RREQ packet for its adjacent nodes [7, 8, 13, 14].

C- Hybrid Protocol

This routing protocol consists of proactive and reactive

protocols whose purpose is decreasing the delay in the network. In large networks, network is divided into areas and a reactive routing protocol is used in each area while proactive routing protocol is used for routing between clusters [7, 9].

The remainder of this paper is organized as follows: the first section presents the introduction. The second section presents the related works. Then, we present the problems of previous intrusion detection systems. In the fourth section, we describe the design and operation mode of our method. In the fifth section, we show the simulation results of our method. Finally, the sixth section concludes the paper.

2. Related Works

In this section, we review the related work on intrusion detection systems for Ad hoc networks. Intrusion detection systems are very extensive in Ad hoc networks and can be divided into six main categories [4, 12].

2.1. Host-based Intrusion Detection System (HIDS)

This intrusion detection system is installed on each node and searches for signs to attack it. This intrusion detection system surveys all activities of a node and when discovers an attack, it sends an alarm to coordinator or adjacent nodes [15, 16].

2.2. Network-based Intrusion Detection System (NIDS)

This IDS searches for attack signs by observing and controlling transitory information in the network. In fact, this IDS supervises the whole network. This model is, then, rarely used for ad hoc networks, as there is information of nodes, which are communicating in same radio range, at each moment, and IDS must perform intrusion detection with partial information [7, 10].

2.3. Anomaly Detection

Anomaly detection is done with a normal behaviour model which is obtained from the whole of network normal activities. Each deviation from network normal model is identified as an attack to network if this deviation is greater than the threshold level.

2.4. Stand-alone IDS

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

2.5. Distributed and Cooperative IDS

In the Ad hoc network, IDS systems must be distributed and cooperative to work together well and satisfy the need of Ad hoc network. In this architecture, each node in the network has its own IDS and collects all the local information of its neighboring nodes. In addition, if IDS observes dissonance in the received information, it will cooperate with other nodes to undertake the attack detection process [11].

2.6. Hierarchical IDS

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

3. Statement of the Problem

Mobile Ad hoc networks have some characteristics and limitations that extremely influence the network security. Possibility of nodes movement and limited process ability respectively are two examples of properties and limitations that prevent us from showing methods with complex algorithms. Besides, most of the presented methods increasing the security level of the networks can only detect one or two kinds of attack. In addition, the detection accuracy would be decreased and rate of false alarms would be increased into network with assuming possibility of nodes movement in these networks. In the proposed method in this paper, all of the limitations along with the nodes movement, as the most important property of the network, have been considered [1, 3, 17].

This method also attempts to detect three kinds of attack simultaneously, including drop route request packets, drop data packets and changing the content of routing packet to alter the optimized route which can cause several common attacks such as DOS. In addition, unlike previous methods, we will increase the detection ratio through giving another chance to suspicious nodes.

4. Proposed Method

In this proposed method, existing nodes in the network should be clustered. The clustering technique will be explained. In clustering, all of the nodes in one cluster must be in communication bounds of each other. For this clustering to work, all of the nodes broadcast a packet with hop count=1 to inform every node of the adjacent of its bounds. After doing so, the nodes of network will be clustered. To determine a node as a coordinator within every cluster, each node of the cluster sets a reversed counter with a

random amount and each of them arriving sooner its counter to zero than others will send a message based on being coordinator for the nodes of its cluster. Therefore, a node will be determined as a coordinator in every cluster. The stages of detecting malicious nodes that cause a change in received packets in every cluster include:

1. Supposing every cluster has N nodes, the coordinator node sends a message to all of the nodes available in its cluster ($N-1$ nodes) (figure 1), and asks all of them to send the same message for the rest of nodes available in cluster ($N-2$ nodes) (figure 2).

Figure 1. send a message from coordinator for all of the nodes in its cluster

Figure 2. send the same messages from each node to adjacent nodes

2. Given that, the nodes available in cluster possessing the original message from coordinator as well as the received message from the other nodes will be able to, comparing this message, distinguish probable changes in the received packets and send the name of suspicious node for the coordinator node of its cluster. The coordinator node, then, with attention to the name of suspicious and received nodes from all of the nodes available in the cluster, will take action to finally search for distinguishing the malicious node and send the information to nodes available in the cluster.
3. If the number of nodes that distinguish the suspicious node is not than sufficient to distinguish the malicious node, the coordinator node will save the name of suspicious node in its memory and repeats the stages 1 and 2 once more, with the mere difference that itself considers the operation of suspicious node directly until an appropriate decision is made.

To distinguish the dropping node, assuming that all of the

nodes available in the cluster are aware of number of their adjacent nodes, the node will be able to distinguish its dropping node and send its name to the coordinator, provided that the received message is less than the suitable amount (number of adjacents). In this case, the coordinator node will also do the final distinguishing operation with renewed execution of stages 1 and 2 and 3.

5. Simulation Results

We simulated our method using the NS2 software. Our simulation conditions were as follows: In our simulation, the routing protocol was AODV. In these simulations, a network of 50 hosts was placed randomly within a 1000×1000 m² area. Each node had a radio propagation range of 250 m and a channel capacity of 2 Mbps. The nodes in the simulation moved according to the 'random way point' model. The minimum and maximum speed was set to 0 and 10 m/s, respectively. Intrusion detection engine for 4, 8, 10 and 12 malicious nodes. The malicious behavior was carried out between 50 and 200 sec. Malicious nodes dropped all data packets they received. The nodes performed normally between 0 and 50 sec. 10 traffic generators were developed to send constant bit rate datagram to ten destination nodes. The mean size of the data payload was 512 bytes.

Figure 3 shows that the proposed method has a very good ability for delivery. Figure 4, and 5, respectively, illustrates the results the proposed method based on packet delivery ratio in the destination, detection ratio based on number of destructive nodes, and false alarm ratio based on number of selfish nodes and its comparison with the referenced paper.

Figure 3. Packet delivery ratio changing with regard to selfish nodes

Figure 4. Detection ratio per number of malicious nodes

Figure 5. False alarm changes regarding to selfish nodes number

6. Conclusion and Future Work

The purpose of the proposed method was to study the operation of adjacent nodes of every node. When the packets receive information, the malicious nodes that take action to the dropping of routing packets, data packets and changing received routing packets will be distinguished with a high speed and accuracy. These methods do not need calculations and complex algorithms and can be executed easily in the mobile Ad hoc networks. For further research, we can show a new method through making changes in the preceding algorithm that discovers the malicious nodes in the mobile ad hoc networks without the presence of all of the nodes available in cluster in the radio bounds.

REFERENCES

- [1] H. Otrók, N. Mohammed, L. Wang, M. Debbabi and P. Bhattacharya, "A Game-theoretic Intrusion Detection Model for Mobile Ad-hoc Networks," Elsevier journal, Computer Communications, vol 31, issue 4, pp. 708–721, 2008.
- [2] D. Subhadrabandhu, S. Sarkar and F. Anjum, "Signature Based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols," IEEE VTC, 2004.
- [3] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C-Y. Tseng, T. Bowen, K. Levitt and J. Rowe, "A General Cooperative Intrusion Detection Architecture for MANETs," in proceedings of the 3th IEEE international workshop on information Assurance, 2005.
- [4] Y. Zheng, "Security in Ad Hoc Networks," special issue on network security, IEEE, 1999.
- [5] Th. M. Chen and V. Venkataramanan, "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks," IEEE Computer Society, pp. 35–41, 2005.
- [6] S.A. Razak, S.M. Furnell, N.L. Clarke and P.J. Brooke, "Friend-assisted Intrusion Detection and Response Mechanisms for Mobile Ad-hoc Networks," Elsevier journal, Ad Hoc Networks, vol 6, issue 7, pp. 1151–1167, 2008.
- [7] A. Shahrbanooonezhad, M. Saniee Abadeh, A. Harounabadi and D. S. Jalali, "A Hybrid System for Detecting Misbehaving Nodes in Ad hoc Networks," International Conference on Intelligent Information Networks (ICIIN), IEEE, pp. 150–154, 2011.
- [8] J. DB and M. DA, "Dynamic Source Routing in Ad-Hoc Wireless Networking," Mobile Computing, Kluwer Academic Publishing, New York, 1996.
- [9] C. Perkins and E. Royer, "Ad hoc On Demand Distance Vector (AODV) Routing," Proceedings of the Second Workshop on Mobile Computing Systems and Applications, IEEE, pp. 90–100, 1999.
- [10] H. Kim, D. Kim and S. Kim, "Lifetime-enhancing Selection of Monitoring Nodes for Intrusion Detection in Mobile Ad-hoc Networks," Elsevier journal, International journal of Electronics and Communications, vol 60, issue 3, pp. 248 – 250, 2006.
- [11] R. V. Boppana, "An Analysis of Monitoring Based Intrusion Detection for Ad Hoc Networks," IEEE Computer Society Department, 2008.
- [12] J. B. D. Cabrera, C. Gutierrez and R. K. Mehra, "Ensemble Methods for Anomaly Detection and Distributed Intrusion Detection in Mobile Ad-Hoc Networks," Elsevier journal, Information Fusion, vol 9, issue 1, pp. 96–119, 2008.
- [13] C.E. Perkins, E. M. Royer, S. R. Das and M. K. Marina, "Performance Comparison of Two On-demand Routing Protocols for Ad-hoc Networks," IEEE Personal Communications Magazine special issue on Ad hoc Networking, pp. 16–28, February 2001.
- [14] P. Yi, Y. Jiang, Y. Zhong and Sh. Zhang, "Distributed Intrusion Detection for Mobile Ad Hoc Networks," IEEE Computer Society, 2005.
- [15] A. Mishra, K. Nadkarni and A. Patcha, "Intrusion Detection in Wireless Ad-hoc Networks," IEEE Wireless Communications, vol. 11, issue 1, pp. 48–60, February 2004.
- [16] G. F. Cretu, J. J. Parekh, K. Wang and S. J. Stolfo, "Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks," Department of Computer Science Columbia University New York, US, IEEE communication and networking conference, 2006.
- [17] S. Corson, J. Macker and G. Cirincione, "Internet-Based Mobile Ad Hoc Networking," IEEE Internet Computing, Jul/Aug 1999.