A Hybrid System for Detecting Misbehaving Nodes in Ad Hoc Networks

Alireza Shahrbanoonezhad, Dina Sadat Jalali, and Ali Harounabadi

***Abstract*—In this paper we express a new intrusion detection system based on counters and a cache memory to detect malicious nodes and selfish nodes in ad hoc network. Network survivability, networks performance and network security are important issues in mentioned networks. The presented work enhances the mentioned factors because it doesn't need heavy computation and also its speed and accuracy in detecting suspicious nodes are great. We simulated our methods by NS2 software. The simulation results show that the proposed method has significant performance.**

***Index Terms*—Intrusion detection system, malicious node, security, ad hoc network.**

I. Introduction

Wireless network architectures are divided into two types: networks with no infrastructure and infrastructure based network. Networks with infrastructure include fixed work stations for routing in network. In this architecture, each node is at least covered by one fixed work station and communicates with other nodes through this work station. The second type of wireless network architecture has no infrastructure. Ad hoc networks usually use this kind of architecture [1].

A typical Ad hoc network is a network consisting of some nodes dispersed in an area without any kind of fixed infrastructure and able to contact to each other via wireless communications [2]. Due to the lack of having a fixed network infrastructure, they can be implemented in any place and at any time, easily and very quickly [3]. Particular type of network nodes within the Ad hoc network with moving nodes is called mobile ad hoc networks (Manet).

Ad hoc networks have some characteristics such as low bandwidth and memory and energy limitations. The mentioned features prevent designing the complex security algorithms with heavy computing for the network [4].

On the other hand the nature of network communication media (radio waves) leads it to be vulnerable while encountering with sabotage actions and attacks. Routing in these networks is very important and routing protocol for the ad hoc networks can be divide to three types described in [5], [6] :

Manuscript received February 29, 2012; revised April 26, 2012. This work was supported by computer department of Islamic Azad University, Iran.

A. Shahrbanoonezhad is a member of scientific board of Islamic Azad University, Dehloran branch, Dehloran, Iran. Ad hoc is his research fields.

D. Sadat jalali works in the Azad university. Ad hoc is her research fields.

A. Harounabadi works in the Azad university of Tehran Markaz as a member of scientific board. Software engineering is his research fields.

A. Proactive Protocol

In this protocol, routing information to reach all the other nodes in a network is always save in the routing table at each node. When the network topology changes, many of routes will change and update the routing table at every node which causes increasing the networks overhead. An example of proactive protocols is FSR (Fisheye State Routing) protocol [7].

B. Reactive Protocol

In this protocol, discovering a route will be done just when a node wants to send data to another node in the network. When a route is discovered, it will be stored in the temporary cache at the source node until an event occurs in the network that imposes a need to new route discovering. Overhead of this protocol is less than proactive protocol. Examples of reactive protocols are DSR (Dynamic Source Routing) protocol [8] and AODV (Ad hoc On Demand Distance Vector) protocol [5].

C. Hybrid Protocol

A proactive protocol for a large network needs a large routing table at every time, thus, it is not useful for a large network. On the other hand, due to route discovery, a reactive protocol for a large network has delay. Thus, using a protocol which combines both reactive and proactive protocol may be a better solution for Manet. An example of hybrid protocols is ZRP (Zone Routing Protocol) [9].

Routing in ad hoc network is performed by using existing network nodes, Hence, existing one or more aggressive and selfish nodes can make some problems for routing and data transmission, thus network performance will be reduced [3]. That's why in recent years providing security solutions for these networks has been under more attention.

The proposal detects three types of destructive action: Drop of routing packets, Drop of data packets and changing in routing packets.

The rest of the paper is organized as follows: the second section presents the related works. Next we present the problems of previous intrusion detection systems in the third section. In fourth section, we describe designing and mode of operations of our method. In fifth section, we show the simulation results of our method resulted from NS2 software. Finally, sixth section draws a conclusion with a future work.

II. Related Works

In this section, we review 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 five main categories [10], [11].

A. Stand Alone Intrusion Detection System

In this architecture, intrusion detection algorithm is running on each node independently and uniquely to detect intrusion. Each decision is adopted only based on information collected by its node and no cooperation between network nodes will exist, so no information will move between them [12]. The need to heavy implementation mechanisms and the lack of information exchanging between network nodes are the main disadvantages of this architecture [13].This architecture is suitable for flat networks structures.

B. Distributive and Cooperative Intrusion Detection System

Considering moving property of the nodes and needing to cooperate between nodes in Manet networks have led to propose this architecture. A Distributive and cooperative intrusion detection system is proposed in[14], where each node contributes in the process of intrusion detection and responding to this process, so there will be data transferring between nodes. Beside benefits of this architecture some disadvantages also exist such as transferring a lot of packets between nodes which causes a lot of traffic on the network.

C. Host Based Intrusion Detection System

In this architecture, intrusion detection algorithms on each host are running. The purpose of this architecture is discovering changes in system files and finding repeated file accesses. Excessive network resources consuming can be noted as disadvantage of this architecture [15], [16].

D. Network Based Intrusion Detection System

This architecture looks for different types of attack within the network using network traffic monitoring. The ability of working with several layers of network protocol is one of the strengths of these systems. Examples of these systems are mentioned in [17],[18].

E. Hierarchical Intrusion Detection System:

This system can be considered as the wide mode of second system which is suitable for multi layer network structures. In this category, most of clustering techniques are used to divide the network into some parts [19].

III. Problem

Most of presented methods for intrusion detection and malicious node detection, depending on network status, are able to discover one or two types of attacks like Drop data packets or route request packets. Major problem occurs when these methods encounter with a malicious node which attack isn't the one that network searches for. Other problems in intrusion detection methods can be the need of some methods to exchange large packets between nodes and thus imposing too much load on the network traffic. While this requires a huge amount of processing and occupied bandwidth and causes excessive resources consumption of the nodes. This will reduce the amount of received packets on the target under any circumstances. Also, it severely reduces the Network performance [3], [19].

The proposed model has tried to identify two or three types of the attacks (data packets Drop, Drop of route request packets and changing the route request packets) at the same time in the network regarding the restrictions of the Ad hoc network. In addition, it reduces the number of False Alarm by selecting a suitable factor for final detecting of malicious nodes.

IV. Proposed Method

In the proposal, based on the performance of each node within the network, detection of three types of attacks such as data packets Drop, Drop route request packets and changes in the received packet are applied. A dynamic clustering model is used for implementing this plan. Such that one of the nodes in each cluster is selected as the header, periodically at any time and based on some factors. The header task is receiving some information from other nodes in the cluster, such as their opinions about the suspicious nodes and then making final decision about the malicious node to understand whether it is failure or not. In this algorithm, five counters are used to check the performance of the nodes and also there is a limited memory to store incoming packets within each node temporarily. Name and job of the counters are as follows:

ID (input data): represents the number of incoming data packets to the node.

IRR (input route request): represents the number of route request packets to the input of the node.

CP (changed packet): represents the number of changed packets within nodes.

OD (output data): represents the number of outgoing data packets from the node.

ORR (output route request): represents the number of output route request packets from the node.

Considering the performance of this algorithm, it can be a combination of multiple intrusion detection systems, such as Standalone IDS and Hierarchical IDS. The mentioned IDS is running on each node and both of its performing and its location are between the physical layer and the data link layer, and each packet arrival or departure of nodes will be estimated by IDS then the necessary action would be done, show in figure1.

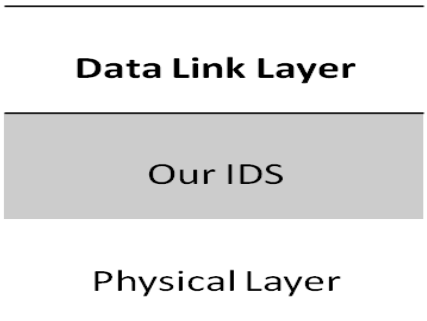

Fig. 1. The position of our IDS in the OSI model

The operation is performed as follows: when the node receives a data packet or a route request packet, first IDS increments the corresponding counters and also stores a copy of the path requested packet into its memory. After reviewing the input packet by the node and if outputting the packet from the node is necessary (Forward / Reply), the outputting packet will be re-examined by the IDS. To identify whether the packet is correct or incorrect and change its corresponding counters. In parallel with time lapse and

changing in the IDS counters, if the equation results for data drop and route request drop exceed the detection threshold or CP counter changes, the malicious nodes will be detected by the IDS and its name will be sent for the cluster header.

$$Data\ drop\ \text{percent} = \frac{\text{ID} - \text{OD}}{\text{ID}} \times 100 \quad (1)$$

$$Route\ request\ drop\ percent = \frac{\text{IRR} - \text{ORR}}{\text{IRR}} \times 100 \quad (2)$$

Cluster Head introduces the malicious nodes to all nodes within the cluster by considering the information received from different IDS. The benefits of this method in comparison with the previous designs can be mentioned as follows:

1) Due to the limitations in the network nodes, in some cases at very short times, some nodes without aiming at damaging the network have relatively high levels of drops. Thus, the mentioned nodes erroneously had been introduced as the malicious nodes by the previous methods, and there wouldn't be any kind of sending or receiving for them. Also they would be deleted from routing table of all the nodes. But the proposed method gives the opportunity to some malicious detected nodes to re-enter to the network and participate in the works. In this approach, after a specified period a specified percentage of the drop of the detected malicious nodes will be reduced. After doing such, if the percentage of drop rate of the node is less than threshold then this node will have another chance to contribute in the network operations and also other nodes will deal with it as a normal node. If after a while the percentage of drop rate of the node doesn't increase then it will be reduced again. But if the node has drop with a percentage of more than the threshold for the second time then it'll be introduced as a certain malicious node and won't have any other chance to return to the network again. It should be noted that nodes that have a very high percentage of drop in the first round of malicious node detecting won't have any other chance to return back to the network either. Using this approach will reduce the rate of false alarm in the network and because of returning some nodes back to the network the network lifetime increases significantly. Also, a better balance within the network will be established in comparison with previous methods.
2) By selecting a formula to evaluate the performance of nodes (1 and 2), malicious node detection accuracy has significantly increased in comparison with previous similar works.

V. Simulation Results

We simulated our method by NS2 software. Our simulation conditions are as follows:

In our simulation, detection threshold is 10 percent. ad hoc routing protocol is AODV.In these simulations detection threshold is 10 percent network of 50 hosts placed randomly within an 1800 × 1000 m2 area. each node has a radio propagation range of 250 m and the channel capacity was 2 Mbps. The nodes in the simulation move according to the 'random way point' model. The minimum and maximum speed is set to 0 and 10 m/s, respectively. intrusion detection engine for 5, 10, 15 and 20 malicious nodes. The malicious behavior is carried between 50 and 200 sec. malicious nodes drop all data packet they receives. The nodes perform 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.

As shown in Fig 2 is Attack Detection Rate is the same for three types of the attack and won't change with time elapsing.

Fig 3 shows average True or False Positives in term of selfish nodes inside the network.

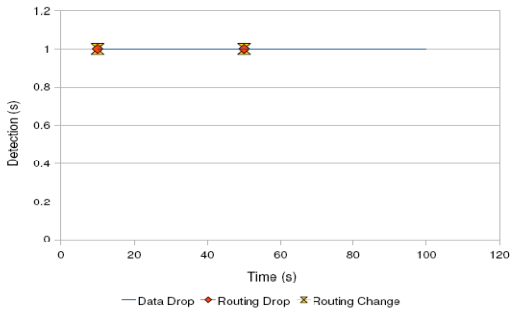

Fig. 2. Attack detection rate for different attacks

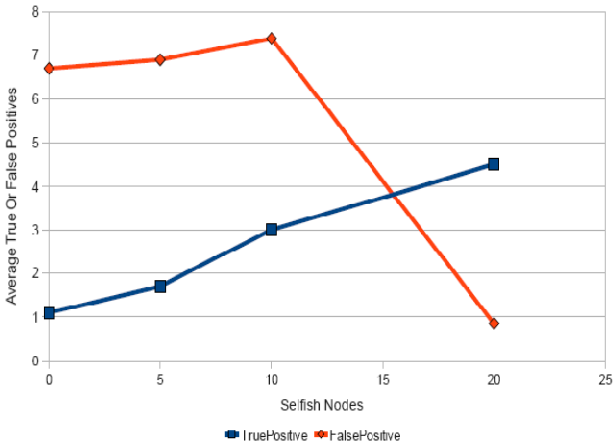

Fig. 3. True or false positives changes regarding to selfish nodes number

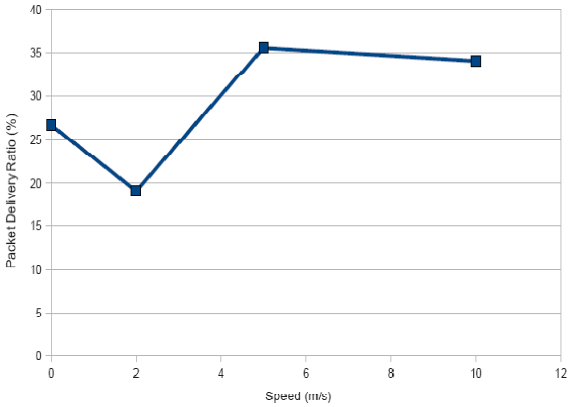

Fig. 4 . Packet delivery ratio changing with regard to nodes speeds for a 10-selfish nodes network

As can be seen, increasing selfish nodes inside the network, increases True Positive and decrease False Positive.

Fig 4 shows packet delivery rate relative to nodes speeds when there are 10 selfish nodes in the network. As it has been shown, packet delivery ratio decreases very slightly when the network nodes speeds increase.

Fig 5 shows the results for a 10-selfish nodes network and indicates that increasing nodes speed in the network decreases False positive.

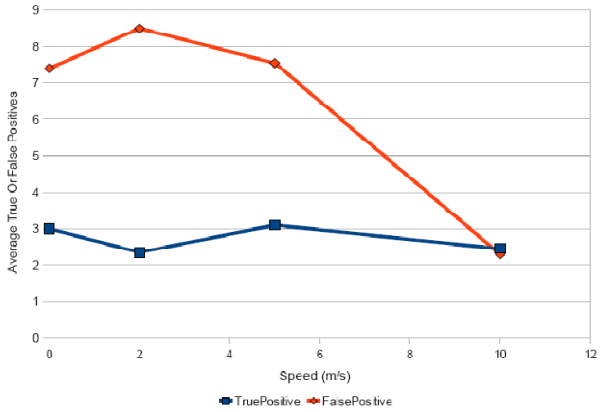

Fig. 5. Average true or false positives relative to nodes speeds

VI. Conclusion and Future Work

We proposed a method for intrusion detection and selfish nodes detection that is able to identify three type of the attacks(Data packet Drop,Drop of route request packets and Changing route request packets) at the same time in the network. Our method doesn't need heavy computation and also its speed and accuracy in detecting suspicious nodes are great. Also, with using double opportunity mechanism, our method severely reduces false positive in the network.

On the other hand, the important difference between our method and previous IDS and IDS-like methods, relates to clustering and combining two intrusion detection systems that results in a new system with all mentioned advantages.. At the end, for future works, it seems that as using more factors influences discovering intrusion detection and malicious nodes process, including battery life of suspicious nodes can increase accuracy and probably increase the amount of data received at the destination.

References

[1] Y. Zheng, "Security in Ad Hoc Networks," *be published in IEEE network, special issue on network security*, 1999.

[2] C. Basile, Z. Kalbarczyk, and R. K. Iyer, "Neutralization of Errors and Attacks in Wireless Ad Hoc Networks," in *Proc. of the International Conference on Dependable Systems and Networks* (DSN'05), *IEEE*, 2005.

[3] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," *Elsevier journal, Computer Communications* 31, pp.708–721. 2008.

[4] M. Yabandeh, H. Mohammadi, and N. Yazdani, "Multipath Routing in Mobile Ad hoc Networks:Design Issues," *12th International CSI Conference Computer (CSICC07) Shahid Beheshti University*, Tehran, Iran, 2007.

[5] C. Perkins and E. M. Royer, "Ad hoc On Demand Distance Vector (AODV) Routing," in *Proce. of the Second Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

[6] M. S. Corson and A. Ephremides, "A Distributed Routing Algorithm for Mobile Wireless Networks," *ACM Baltzer Wireless Networks Journal*, pp.61-81. 1995.

[7] A. Iwata, C. C. Chiang, G. Pei, M. Gerla, and T. W. Chen, "Scalable Routing Strategies for Ad hoc Wireless Networks," *Journal on Selected Areas in Communications, Special Issue on Wireless Ad hoc Networks*, pp.1369-1379. 1999.

[8] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networking," *Mobile Computing, Kluwer Academic Publishing*, New York, 1996.

[9] M. R. Peralman and Z. J. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol," *IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Adhoc Networks*, pp.1395-1414, 1999.

[10] M. M. Ibrahim, N. Sedak, and M. EL-Banna, "Prevention of Dropping Routing Traffic Attack in wireless Ad hoc AODV Based Network using Real-time Host intrusion detection," 2*6th national Radio science conference*, 2009.

[11] C. Ramachandran, S. Misra, and M. S. Obaidat, "A Novel two-Pronged strategy for an agent-based intrusion detection scheme in ad hoc network," *Elsevier journal*, pp. 3855-3869, 2008.

[12] T. S rinivasan, V. Vijaykumar, and R. Chandrasekar, "An auction based task allocation scheme for power-aware intrusion detection in wireless Ad hoc networks," *Thrid international conference on wireless and optical network*, 2006.

[13] Yi-An Huang, W. Lee, and Y. Zhang, "Intrusion detection techniques for mobile wireless network," accepted in *ACM MANET Journal,* 2003.

[14] P. Yi, Y. Jiang, Y. Zhong, and S. Zhang, "Distributed Intrusion Detection For Mobile Ad Hoc Networks," in *Proc. of the Symposium on Applications and the Internet Workshops*, 2005.

[15] Http: //osiris.shmoo.com/. (Accessed 18th september 2007).

[16] F. Anjum, D. Subhadrabandhu, and S. Sarkar, "Signature based intrusion detection for wireless ad-hoc networks: a comparative study of various routing protocols," *Vehicular Technology Conference*, 2003.

[17] H. kim, D. kim, and S. kim, "lifetime-enhaning selection of monitoring nodes for intrusion detection in mobile Ad hoc networks," *elsevier journal*, pp.248-250. 2006.

[18] G. Thamilarasu, A. Balasubramanian, S. Mishra, and R. Sridhar, "A Cross-layer based Intrusion Detection Approach for Wireless Ad hoc Networks," 2005.

[19] 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 *proc. of the 3th IEEE international workshop on information Assurance*, 2005.