A New Method for Malicious Node Detection Based On a Clustering Algorithm

A. AlirezaShahrbaneezhad, B. DinasadatJalalifar, C. Mohammad Mehrani

Department of computer, Islamic Azad University, Dehloran Branch, Dehloran, Iran
Sama Technical and Vocational Training College, Islamic Azad University, Shoushtar Branch, Shoushtar, Iran
Department of computer, Islamic Azad University, Shoushtar Branch, Shoushtar, Iran

Abstract:

Mobile ad hoc networks (mobile ad hoc network) are wireless networks without a constant infrastructure, so it is easy to set up and use this type of network such that this trend is expanding. In these networks, nodes existing in the radio range of each other can communicate, directly. Also, the network has some characteristics such as the nature of the transmission medium, power and energy, limited bandwidth and limited resources such that because of them intrusion and sabotage actions can be done, easier. Mobile ad hoc networks don’t have a certain defense mechanism; this matter causes providing some competitions to represent the security and intrusion detection methods. Routing is the most important issue in mobile ad hoc networks which is performed by network nodes themselves in this kind of networks. The possible problem is the existing of a malicious node among other nodes in the network which may make some difficulties for the routing issue in the network. In this paper, a new method of intrusion detection will be presented which uses a simple method in monitoring the behavior of neighboring nodes to distinguish those of destructive nodes who change the incoming packets (changing packet) or avoid forwarding these packets. So the rate of misdiagnoses (False alarm) decreases. Simulation results indicate the superiority is performed.

Keywords: MANET, Security, Intrusion Detection, malicious nodes, clustering algorithm, FEED Clustering Method, dropping packet, changing packet.

I. Introduction:

An Ad hoc network is a wireless network without fixed infrastructure so it can be setup and used easily(Otrok et al, 2008), (Subhadrabandhu et al, 2004). Also all the computers in such networks should be in the radio range of each other to make communication. These networks along with positive attributes, they also have disadvantages that include: Memory limitation, bandwidth limitation, low-level processing power and also limitation of nodes lifetime. All of this, along with features of media between nodes (radio frequency), has led the network to be vulnerable (Sterne et al, 2005) (Chen et al, 2005). Routing is one of the most important problems in ad hoc networks 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, so routing at these networks is more difficult than other network factors and requires its own algorithm. On the other hand, the proposed routing algorithms for these networks have low level of security and also 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 (Razak et al, 2008), (Shahrbanonezhad et al, 2008). Routing in these networks is very important and routing protocols for the ad hoc networks can be divided into three described types:

A. **Proactive protocol:**

The name of this protocol is table-based routing protocol or table-oriented protocol. In this routing protocol, routing information are already saved in the routing tables at each node and if the topology changes, the changes will be notified to all nodes in the network and the routing tables are updated and the source node identifies the route to the destination node using the information from the routing tables at each node (Shahrbanonezhad et al, 2008).

B. **Reactive protocol:**

This is a demand-driven routing protocol. In this protocol, routes are discovered when the source node attempts to communicate with other nodes. At this time the source node calls the route discovery procedure, and often flooding is used for this purpose. This routing protocol is used in ad hoc networks. DSR and AODV routing algorithms are examples of this kind of routing methods. In the AODV routing algorithm, the source node generates a RREQ packet and denotes the source and destination node set, and then emits the so-called RREQ packet to its neighbors. Each node that has a route to the destination node in its memory generates the RREP packet; otherwise emits RREQ packet to its neighbors (Shahrbanonezhad et al, 2011) (Jiang et al, 2004).

C. **Hybrid protocol:**

This routing protocol is a combination of proactive and reactive routing protocols which main goal is reducing delays in the network. In large networks, the network is divided into some regions and within each region a reactive routing protocol is used and active routing protocol is used for routing between clusters (Shahrbanonezhad et al, 2011) (Perkins et al, 1999).

The first section has presented the introduction. The reminder of this paper is organized as following: 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. Finally, sixth section draws a conclusion.
II. RELATED WORKS:

In this section, we review related works 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 (Cabrera et al., 2008).

A. Host based intrusion detection system (HIDS):

This intrusion detection system is installed on each node and the node will be looking for signs of attack. The mentioned intrusion detection system monitors all the activities of a node and when an attack is detected a warning message would be sent to the supervisor or neighboring nodes (Mishra et al., 2004), (Cretu et al., 2006).

B. Network based intrusion detection system (NIDS):

This IDS, by observing and controlling the network information, looks for signs of attacks that are being carried out on that part of the network, in fact, the so-called IDS is monitoring all the network. This model doesn’t have very many usages for Ad Hoc networks because in every period of time the data belonging to the nodes that are linked together in the same radio range is available and ids should operate intrusion detection operation using this information (Shahrbanoonezhad et al., 2011), (Kim et al., 2006).

C. Anomaly detection:

Detecting abnormal behavior would be performed by using a normal model of network behavior, such that the pointed normal model of network behavior is obtained from all the normal behavior models of network activities, and any deviation from the normal model of the network, if higher than the threshold, would be detected as the network attack.

D. Stand-alone IDS:

In this architecture an intrusion detection system is to be installed on each node. Then the mentioned system discovers the occurred attack to the node according to data collected from that node. In this intrusion detection architecture the nodes do not participate and cooperate with each other 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.

E. 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 neighbor nodes. Also, if IDS observes dissonance in the received information then it’ll cooperate with other nodes to perform attack detection process (Boppana et al., 2008).

F. 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 attend 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 the information obtained from the nodes.

III. Problems of previous systems:

Detecting In general, mobile ad hoc networks have some features and limitations that will have a significant impact on the security of the network. Movement is one of the mentioned features and little processing power is one of the so-called limitations which avoid presenting methods with complex algorithm. On the other hand, most of the methods proposed to enhance the security of these networks are able to detect only one or two types of attack and by taking node mobility (movement) into account in the network the accuracy decreases and the rate of false alarms within the network increases. In the proposed method of this paper all the limitations of the network are considered and based upon the nodes movement as the main feature, three different attacks would be detected, simultaneously: drop route request packets, drop data packets and changing the content of routing packet to change the optimized route (Otrok et al., 2008) (Sterne et al., 2005).

These attacks can originate a number of other common attacks within the network like DOS attack. Furthermore, unlike previous approaches, by giving other opportunity to the suspicious the detection ratio will increase.

IV. Proposed method:

In the proposed scheme, nodes on the network should be grouped in some clusters which will be explained how to do this clustering. In clustering all the nodes in a cluster must be connected within each other. To perform clustering, initially all the network nodes broadcast a packet in one step (one hop) to notify each node's neighbors in the corresponding area of that node. By doing such the network will be clustered, completely. Then each node in the cluster will set a countdown timer with a random value (random counter), then each of them which timer reaches zero before all the nodes would be the cluster’s coordinator and will send a message to all the cluster’s nodes to inform them about this event. Thus, a coordinator will be determined in each cluster.
A. The clustering method:

The clustering algorithm used by the presented method is FEED (Fault Tolerant, Energy Efficient Distributed Clustering for Wireless Sensor Network). FEED selects the cluster heads based on factors such as: energy, density, centrality and distance between nodes. FEED algorithm executes in four phases. In the first phase each sensor node sends its \( id \) and coordinates to around neighbours and receives same messages from them. By doing such, each node can compute its density and centrality. A new method for computing centrality factor is also introduced in FEED algorithm. Each node calculates its first score by mixing energy, centrality and density factors and getting an average from them. (Hasannejad et al., 2013)

In the second phase, those of nodes that their energy and density factors are good introduce themselves as volunteers. Then in the third phase, each node gives second scores to its near volunteers by entering distance factor to first scores of the volunteers and reveals a volunteer with best second score as its deputy.

In the fourth phase volunteers calculates their final scores and according to that reveals themselves as CH, PCH or SN nodes. Then regular nodes join to nearer clusters. (Hasannejad et al., 2013)

This algorithm improves the network lifetime in a significant way in comparison with two well-known clustering algorithms LEACH (Heinzelman et al., 2000) and HEED (Younis et al., 2004). Furthermore, FEED algorithm leads the network to be fault tolerant. “Fig. 1” shows the improvement of network life time by FEED in comparison to LEACH and HEED algorithms. In FEED when the remained energy of a cluster head falls under a threshold, its supervisor node will replace it and the cluster can continue its activity by the new cluster head. This property leads network to be fault tolerant. According to “Fig. 1”, FEED algorithm improves network lifetime in comparison to two other algorithms. Supervisor node replacement can be a reason for this enhancement. (Hasannejad et al., 2013)

“Fig. 2” shows the percentage of total remaining energy of the network nodes after 1, 20 and 50 rounds. After one round, HEED algorithm outperforms the best, but in later rounds FEED algorithm performance is the best. After round 300 only FEED algorithm is still executing, but LEACH and HEED algorithms have terminated. “Fig. 2” shows that FEED significantly improves the network energy consumption. (Hasannejad et al., 2013)
The method of detecting malicious nodes in each cluster that change their own incoming packets would be as the following steps:

1- Assuming that each cluster contains N nodes, the coordinator node sends a message to all the nodes in its cluster ((N-1) nodes), “Fig. 4”, and would ask all of them to send the same messages to all other nodes of the clusters ((N-2) nodes), “Fig. 5”.

![Figure 4](image1.png)

**Figure 4.** Send a message from coordinator for all of the nodes in its cluster
2 – Regarding this note that all the existing nodes in the cluster have the original message of the coordinator as well as the messages received from other nodes they would be able to recognize the possible changes in the incoming packets by comparing these messages, then they will send the name of suspicious node to the coordinator. The coordinator by considering the received names of suspicious node sent by other nodes in the cluster would precede the final examination for detecting the malicious nodes and will send the corresponding messages to the cluster nodes.

3- If the number of nodes who try to detect the suspicious node is lower than the necessary threshold, the coordinator node will save the name of suspicious node in its memory and repeats the steps 1 and 2, except that the coordinator node would directly monitor the suspicious node’s performance and would make a careful decision about it.

To detect the packet dropping nodes, by regarding this note that all the cluster nodes are aware of the number of their neighbors, if the number of incoming messages is less than the expected number (number of neighbors) the node would be able to identify its packet dropping neighbor and send its name to the coordinator. So, the coordinator will re-implement the steps 1, 2 and 3 for final diagnosis over the packet dropping nodes.

V. Simulation Results:
Figures 6, 7 and 8 respectively show the results of the proposed method regarding delivery ratio of the destination, the malicious nodes detection ratio, false positive for the number of selfish nodes and also comparing the results with the previous scheme (Shahrbanoonezhad et al, 2011).
VI. Conclusion and future work:

In the proposed method, which is based on the performance of neighboring nodes in each node during receiving the packets, the malicious nodes that try to drop the route request packets, drop
the data packets and modify the received routing packets can be detected with high speed and accuracy. This method does not require complex calculations and algorithms to implement and can be very simple to implement and run on mobile adhoc networks. As the future work, the algorithm can be expressed with some changes to achieve at a new method which does not require that all nodes in a cluster are within each other's radio while having the ability to detect malicious nodes in the mobile ad hoc networks.

REFERENCES


