Proc. of the Intl. Conf. on Advances in Computing and Communication – ICACC 2013

ISBN: 978-981-07-6260-5

Quantitative Behavior Based Intrusion Detection System for MANETS

S.Mamatha,
Associate Professor, Dept of CSE,
Bhoj Reddy Engineering College for Women, Hyderabad.

Dr A Damodaram
Professor, Dept of CSE,
JNTU College of Engineering, Hyderabad.

Abstract **-** The use of wireless links makes a Mobile Ad hoc Network(MANET) susceptible to malicious attacks, ranging from passive eavesdropping to active interference. In wired networks an attacker has to pass through a set of firewalls and gateways to access the network. Whereas MANETS does not have firewalls or gateways so attacks can take place from all directions. Every node in a MANET is an autonomous unit in itself and free to move independently. So any node without adequate protection is very much prone to be captured or compromised. Intrusion prevention techniques like encryption and authentication can reduce the risk of intrusion but cannot completely eliminate them so a second level of defense is needed. We propose a new quantitative method of intrusion detection system to detect intrusion in MANETS with mobile nodes. The proposed method is a behavioral anomaly based system which is dynamic, scalable, configurable and robust. For simulating the proposed system we use AODV routing protocol. It is observed that the malicious node detection rate is very good and the false positive detection rate is low.

Keywords- AODV routing protocol, Intrusion Detection System, Mobile Ad hoc Network (MANET).

1. INTRODUCTION

A Mobile Ad hoc Network(MANET) is an autonomous system of mobile hosts connected by wireless links , the union of which forms a communication network .As it does not depend on predefined infrastructure to keep the network connected, it is also known as infrastructure-less network. In a MANET each node can communicate with all the nodes that are in its radio transmission range and takes help of intermediate nodes to communicate with the nodes beyond the transmission range [1].Also as the network topology of a MANET changes unpredictably the nodes need to exchange the topology information frequently. Thus the functioning of the MANET depends on the cooperation and trust between nodes.

The mobile ad hoc networks due to their characteristics like dynamic topology, cooperative algorithms, lack of centralized monitoring, bandwidth constraints, energy constraints and limited physical security are more prone to various types of attacks. The mobility and resource constraints of nodes, make the intrusion detection techniques of wired networks not suitable for MANETS. An intrusion detection system is a method that determines whether a process or user is attempting something unexpected and works on the basis of examining an activity on a specific machine or network and deciding whether the activity is normal or suspicious.

The Intrusion Detection System(IDS) are classified in different ways.Based on the audit data, IDS can be classified as network-based or host-based. A network-based IDS captures and examines network packets that go through the network hardware interface, while host-based IDS relies on the operating system audit data to monitor and analyze the events generated by the users. Intrusion detection can further be classified into three categories based on the detection techniques as anomaly-based detection, misuse-based detection and specification-based detection [2][3][4]. In anomaly-based detection, a normal profile of user is kept in the system and then the captured profile is compared. Any deviation from the normal behavior is detected as an attack. In misuse-based detection also known as signature-based system, a predefined pattern or signature is used to match an attack. In specification based detection the system monitors current behavior of system according to specification that describes functionality for security critical entities. Any mismatch is reported as an attack.

In this paper we propose a new intrusion detection system based on the anomaly and agents. We show how to separate the intrusion and abnormal behaviors from expected and normal behavior. We have proposed a quantitative and statistical based algorithm for identifying malicious nodes. We verified our method by running simulations with mobile nodes using Ad hoc On Demand Distance Vector (AODV) routing protocol.

The rest of the paper is organized as follows; section2 specifies the related work done. Section 3 describes proposed system. Section 4 presents the simulation study. Section 5 concludes the paper.

2. RELATED WORK

The difference in security of wired networks and mobile ad hoc networks provoked researchers to model an IDS that can handle new security challenges. Some of the existent research work that is related to our work is discussed. In [5] Huang and Lee proposed a cluster-based cooperative intrusion detection system which not only detect an intrusion , but also identify the source of attack with

Proc. of the Intl. Conf. on Advances in Computing and Communication – ICACC 2013

ISBN: 978-981-07-6260-5

statistical anomaly detection if the attack is within one hop. In [6] Zhang and Lee proposed an intrusion detection and response system in MANETS which is both distributive and cooperative. The proposed system detects anomaly in routing updates of both MAC and application layer. In [7] Albers et.al proposed architecture for local detection based on mobile agents. In the proposed system the ID agent running at each node for local dread can be extended for global dread by cooperating with other local agents. In this method two types of data called security data and intrusion alerts are exchanged among local agents. In [8] Sterne et .al has proposed a dynamic intrusion detection method that is potentially scalable to large networks with clustering. Here the nodes on the first level are cluster-heads and nodes on the second level are leaf nodes. Every node has the task of monitoring, analyzing and properly responding to the intrusion detected if enough evidence is available and report or alerts the cluster-head. The cluster-head in addition should perform data integration and data filtering, computation of intrusions and security management. In [9] the authors proposed an anomaly-based zone based intrusion detection system (ZBIDS). In this architecture the inter-zone nodes are responsible for collecting and aggregating the alerts from intra-zone nodes. Most of the related work gives a distributed solution involving the cluster-heads as the main source of communication. The main disadvantage with the above methods is that the cluster may become nonfunctional if an attacker targets the cluster-head. Also these cluster-heads are usually more resource concentrated and decrease survivability.

So we propose a dynamic, distributed and quantitative intrusion detection system for MANETS that involve mobile nodes in a non-cluster based environment.

3. PROPOSED SYSTEM

In our proposed system we attach local IDS agent to each mobile node. These agents run independently and monitor activities of the user and system as well as communication activities within their radio range to detect abnormal behavior. If an anomaly is detected in the local data or if the evidence is uncertain the IDS agents in the neighboring nodes will courteously participate in a global intrusion detection scheme. We try to implement a quantitative anomaly-based algorithm because it is expected that more types of attacks may be launched against MANETS in the future. The architecture of the proposed system is as shown in figure 1.

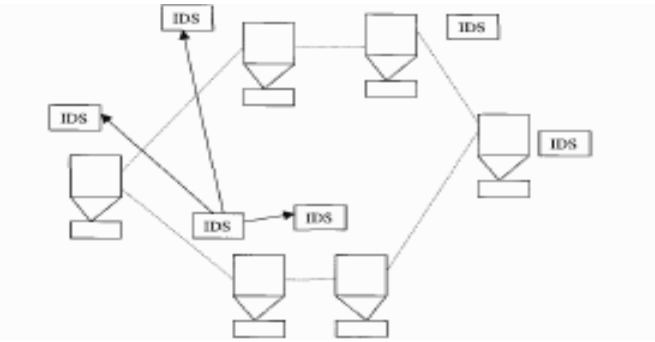

Fig 1: IDS architecture of the proposed system

The process of intrusion detection is composed of two steps. First, detection of malicious nodes, second their castigation and isolation from the network. The conceptual structure of an IDS agent is shown in figure 2. and consists of 4 modules: Data collection, Intrusion detection engine, Voting and Intrusion response modules.

Data Collection module

The main function of this module is to supervise the behaviors of the nodes for collecting security related data. We use a Data Transmission Quality function proposed by Alam in [10] to measure a node's communication quality. Using the DTQ function the sender node gets information on misbehaving and well-behaving nodes based on the ack received by the sender after forwarding the packets to other nodes. This function also helps in measuring the transmission quality of intermediate nodes. Each node has a DTQ table in which it keeps the quality of the intermediate nodes behaviors during packet forwarding.

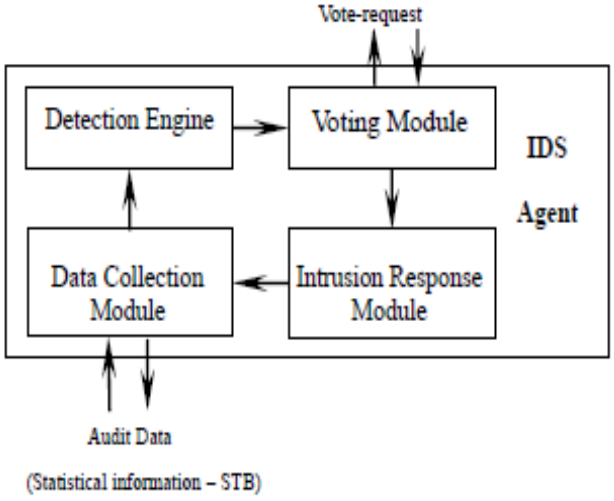

Fig 2: Structure of an IDS agent

Proc. of the Intl. Conf. on Advances in Computing and Communication – ICACC 2013

ISBN: 978-981-07-6260-5

To decrease the communication overhead caused due to Ack and statistical packets the concept of bucket is introduced. Every bucket is composed of some specified packets. Instead of sending ack packets for every data packet it is enough to send one ack for each bucket. Buckets can be two types. It can be either long-term bucket having the statistical information on the quality of forwarding of last N packets and second a short-term bucket that includes the statistic data on the recently sent M packets. M and N are so defined that N is dividable into M, so that N packets are divided into M short-term buckets. Each short-term bucket maintains the stastic related to the sent N/M packets and called as the STability of the nodal Behavior (STB).

At the end of each short-term bucket, the data is collected by the data collection module of the agent and send to the node. The node based on the statistic, updates the DTQ value in the corresponding DTQ table and also forwards to the nodes in its range.The data collection module of these nodes updates the DTQ table, based on the received data and the amount of D and E and send it to the detection engine.

The DTQ is defined as a function of STB(),probability of error in the channel p() and the energy needed to transmit data(E) as

$$DTQ = k \times \frac{D \times STB()}{E \times P()} \quad (1)$$

The STB() function

$$STB = \left(\frac{S(d_i, u_i)}{Z(d_i, u_i)} \right)^{\alpha} \quad (2)$$

Where d_i represent the successfully transmitted bytes and u_i represent the bytes expected to be transmitted.

In our proposed system we expect the packet to be atomic and also of fixed size and so we will have the STB as proposed in [11]

$$STB() = \left(\frac{\text{Total Ack packets for the last N/M packets}}{\text{Total Ack packets for the last N packets}} \right)^{\alpha} \quad (3)$$

So finally the DTQ function is given as :

$$DTQ = k \times \frac{D}{E} \times \frac{1}{P()} \times \left(\frac{\text{Total Ack packets for the last N/M packets}}{\text{Total Ack packets for the last N packets}} \right)^{\alpha} \quad (4)$$

where $k > 0$ and $\alpha > 1$.

Intrusion detection Engine

The main function of this module is to detect the malicious nodes. The detection of malicious nodes requires an appropriate definition of the term malicious. The detection engine also requires to specify an appropriate threshold between normal and abnormal acts. In our proposed method, we define the malicious nodes as those nodes which had abnormality in the process of packet forwarding. The threshold value is calculated as below.

Let N_{DTQ} be the set of nodes listed in DTQ table, $|N_{DTQ}|$ be the number of nodes, q_i be the DTQ value of node i. The threshold per group is defined as

$$Th = r \times \frac{1}{|N_{DTQ}|} \sum_{i \in NDTQ} q_i \quad (5)$$

Where $0 < r < 1$.

If the detection engine finds one or some values of DTQ in the table are less than the threshold, then it realizes that there may be one or more malicious nodes present the group. In such a case the engine sends to the voting module a vote request about the suspected nodes. The voting result will determine the authenticity of the suspicious node. To prevent a malicious node from starting a false voting request continuously, a node may only start another voting request after 2^k times, if previous k-1 voting requests are vetoed by its group.

Voting Module

When a voting module of a node receives the vote request packet, it votes for or vetoes the suspected node according to the results announced by the detection engine and sends the result to the voting module of the node. During the process of voting it is not fair to account only the positive or negative votes, because the values of each node's DTQ are not the same throughout the group. The DTQ values with recent timestamps are more important than the older timestamps. We set a variable **w** as the weight of DTQ values, which ranges [0,1], and its value decreases with the elapse of time. Assuming there are n nodes vote to [illegible]ine the authenticity of node m. Let q_{im} be the DTQ [illegible]of node m in the DTQ table of node i, w_{im} be the [illegible] of q_{im}, we define the voting result as,

$$V_m = \sum_{i=1}^{n} w_{im} q_{im} v_{im} \quad (6)$$

where $V_{im} = 1$, if node i votes for node m and $V_{im} = -1$ if node i votes against node m.

Proc. of the Intl. Conf. on Advances in Computing and Communication – ICACC 2013

ISBN: 978-981-07-6260-5

At the end of voting process, voting module sends the result of voting (v_m) to its intrusion response module.

Intrusion Response Module

According to the results of the voting, the node m can be a well-behaving node and is set free or it can be a malicious node and should be penalized. If $V_m << 0$, then the response module belives that node m is a malicious node and should be dismissed from the group. All nodes within the group remove node m from their DTQ table and routing table. There after the intrusion response module prevents the nodes from cooperating with the dismissed node by not allowing no packets to be sent by the malicious node but also prevent from forwarding its packets by other nodes.

If $v_m >> 0$, then the response module believes that node m is a well-behaving node, and those nodes that have voted against it must update the amount of their DTQ. Suppose the ratio of FOR-votes and AGAINST-votes is f:a, then the nodes voted against node m update their DTQ values as follows,

$$q_m = q_m \times (1+ \frac{f}{f+a}) \quad . \qquad (7)$$

The equation decreases the difference between the voting nodes, and avoid frequent voting request about node m in near future.

If $v_m = 0$, then there is no consistent point of view because f:a=1:1, in such a case the group will split into two subgroups: FOR-group(including node m) and AGAINST group.

4. SIMULATION AND ANALYSIS

NS-2 simulator is used to simulate our model. And our simulation is done using AODV routing protocol .The simulation environment is set with channel capacity of mobile nodes to 2Mbps and transmission range to 250 meters. The mobility model is random waypoint model. The minimal speed of nodes is 5m/s and maximum speed is 15m/s. The size of all data packets is set to 512 bytes. The duration of each simulation is 2000seconds.The attacks that are simulated in this paper are flooding, black-hole and denial-of-service (DOS) attacks.

Flooding attack: In this attack, the malicious node pumps a great deal of useless and garbage packets to the network. In this way it crumbles the network resources like bandwidth and energy.

Black-hole attack : In this attack, the malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. Thus the attacker receive the traffic destined for other nodes and can drop or modify them.

Denial of Service (DoS) attack: In this attack the malicious node prevents other nodes from working together, by draining the resources like energy and bandwidth of the nodes and the network. Once the resources of the node are drained, the node prevents itself from assisting with other nodes and hence increases its lifetime.

The first simulation of these attacks was considered on the relation between the detection rate and number of nodes. The figure 3 below shows that most of the attacks are detected successfully. The detection rate of flooding and DoS attacks has decreased in high density networks. The reason is that in high densities, the amount of traffic is high and it is not possible to make out the networks normal status and it's under attack situation.

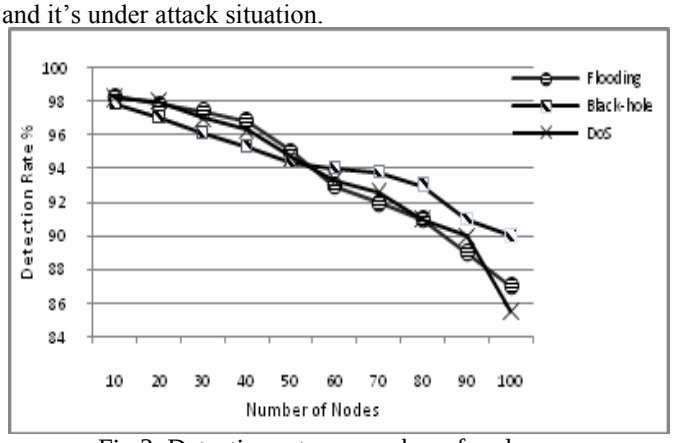

Fig 3: Detection rate vs number of nodes

The next simulation shows the relation between detection rate and percentage of malicious nodes and is as shown in figure 4.It is observed that most of the malicious nodes are detected successfully. As it was expected the networks with high percentage of malicious nodes the detection rate decreases due to the process of voting.

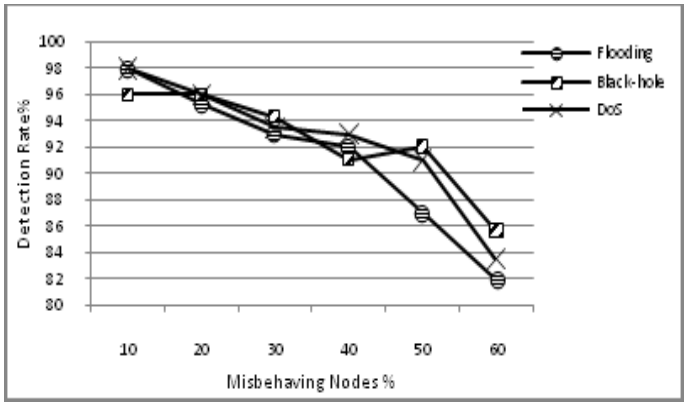

Fig 4: Detection rate vs percentage of misbehaving nodes

Proc. of the Intl. Conf. on Advances in Computing and Communication – ICACC 2013

ISBN: 978-981-07-6260-5

The next simulation shows the relation between the false positive and the number of nodes. As shown in figure 5 in the worst case the false positive rate has not been over 15% which is a good rate. In high density networks the false positive rate is high as the amount of traffic generated is high. This makes it impossible to identify whether the high rate of traffic is due to flooding attack or the normal situation of the network.

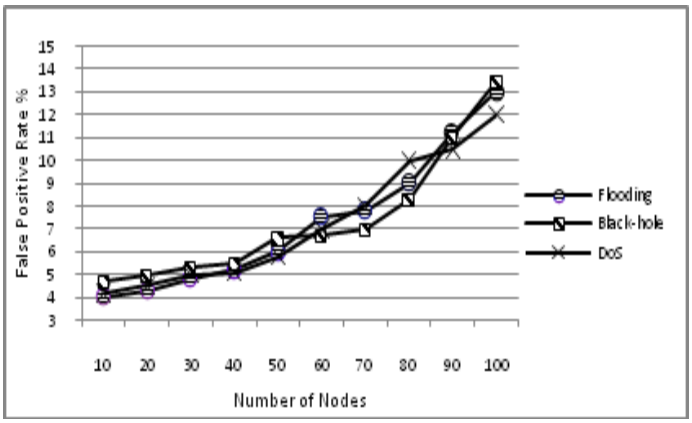

Fig 5: False positive rate vs number of nodes

Figure 6 shows the simulation result of the relation between false positive rate and percentage of malicious nodes. Initially though the percentage of malicious nodes is low, the false positive rate is high because in normal situation some packets may not reach the destination due to link devastation or congestion. This situation is mistaken for ill-behavior of nodes. But when the percentage of malicious nodes increases, the false positive rate also increases because under such circumstances the exactness of the voting process decreases.

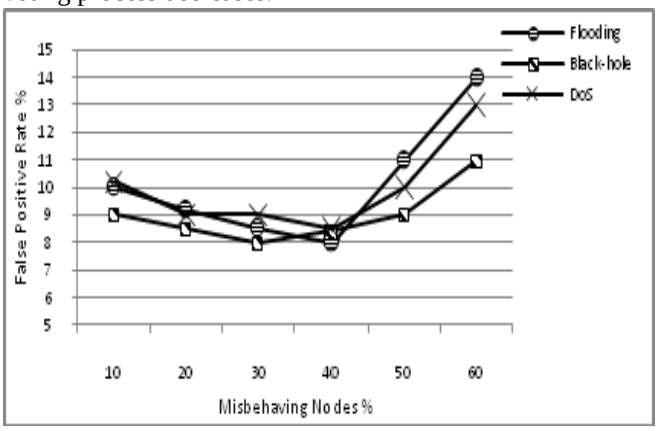

Fig 6: False positive rate vs percentage of misbehaving nodes

5. CONCLUSION

In this paper we tried to establish a method for identifying malicious nodes in a MANET with mobile nodes based on the behavioral attributes. We proposed a method in which the abnormalities in the behavior are defined quantitatively by observing the data exchange activity. Using the routing attacks as the threat model and AODV routing protocol we have carried out simulations in NS-2 and demonstrated the effectiveness of the proposed system. In our future work we plan to investigate more attack scenarios in MANETS, not only in routing layer but also other layers.

REFERENCES

[1] Yi p,Dai Z, Zhang S and Zhong Y. A new Routing attack in Mobile Ad Hoc Networks, Proceedings of the International Journal of Information technology,2005.

[2] Sahu S and Shandilya S.K. A Comprehensive Survey on Intrusion detection in MANET, Proceedings of the International Journal of Information Technology and Knowledge Management Vol 2, pp 305-310, 2007.

[3] Anantvalee T and Wu J . A Survey on intrusion Detection in Mobile Ad Hoc Networks, Book Series Wireless Network Security,Springer, pp 170-196, 2007.

[4] Mandala S, Ngadi M.A and Abdullah A.H. A survey on MANET Intrusion Detection, International journal of Computer Science and Security,Vol 2 ,2010.

[5] Huang Y,and Lee w. ACooperative Intrusion Detection System for Ad Hoc Networks, Proceedings of the 1st ACM workshop on security of Ad Hoc and sensor Networks
pp 135-147, 2003.

[6] Zhang y, Lee W and Huang y. Intrusion detection techniques for Mobile wireless Networks, Wireless Networks, Vol 9,pp 545-556,2003.

[7] Albers p, Camp O,et.al. Security in Ad Hoc Networks: a General intrusion Detction Architecture Enhancing Trust Based Approaches, proceedings of the 1st International worksop on wireless information Systems(WIS-2002),pp 1-12.

[8] Sterne D, Balasubramanyam p and et al. A General Cooperative Intrusion Detection Architecture for MANETS, Proceedings of the 3rd IEEE International workshop on information Assurance(IWIA'05)

[9] sun B, Wu K and Pooch U .W, Alert Aggregation in Mobile Ad Hoc Networks, Proceedings of the 2003 ACM Workshop on wireless Security(WiSe'03) in conjunction with the 9th Annual International Conference on Mobile Computing and Networking(MobiCom'03)

[10] Li T, Song M and Alam M. Compromised sensor node detection : A quantitative approach, Proceedings of the IEEE International Conferennce on Distributed Computing Systems, pp 352-357,2008.

[11] Kumar k.Intrusion detection in Mobile Ad Hoc Networks, Master's Thesis, The University of Toledo,2009.