ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

National Symposium On Emerging Trends In Computing & Informatics, NSETCI 2016, 12th July 2016, Rajagiri School of Engineering & Technology, Cochin, India

Cooperative Judgment Based Intrusion Detection System for Wireless Ad-hoc Network.

***Anjana K P and Preetha K G.**

Rajagiri School of Engineering and Technology, Cochin, India.

Manuscript Info

Key words:
Intrusion Detection System, Malicious Attack, Collective IDS, Trust Metric, Malicious List.

Abstract

The open-shared communication medium, highly in-stable network topology, limited resources makes the mobile ad-hoc networks an easy target for the network attackers. These attackers could execute a wide variety of attacks ranging from black-hole, wormhole, jamming to malicious attacks. To detect such attacks there is special system called the Intrusion Detection System (IDS). Currently, there are several IDS available, but, the entire detection and decision process is carried out by a single node. The proposed system is an IDS based on collective decision technique. Under this system all the nodes have to cooperate during the detection phase. This system works under four phases namely election, detection, collection and announcement. All the nodes in the network would be consulted before confirming a culprit node as a malicious node. Here if the culprit node is confirmed to be exhibiting malicious behavior then a global alarm is immediately generated by the leader.

Introduction:-

Collection of interconnected computers, using a wired or wireless medium is called a computer network. Establishment of such networks helps in data exchange, sharing of services and better utilization of resources. For most of the real world application like disaster management systems, monitoring vehicular movements, etc, a wireless network is preferred over a wired network because of simplicity in its setup and maintenance procedures (Marti et al 2000). Different forms of wireless networks include Mobile Ad-hoc Network (collection of mobile devices), Wireless Sensor Network (collection of sensors and sink nodes), Vehicular Ad-hoc Networks, etc.

In a wired network, each node/host is responsible for only generating and receiving the data. There are specialized network equipments like routers, firewalls, switches in the wired networks that take care of other functionalities like forwarding, routing, security, etc. On the contrary side the nodes/hosts in wireless networks don't have the support of such specialized network equipments, so they have to not only generate and process the data but also have to forward these data packets and route them along the correct paths.

Performance of each individual node in a wireless network determines the overall performance of the network. All the nodes are expected to perform their forwarding functionality properly in order to ensure that data from a sender is received at the appropriate receiver. But since these nodes have several in-built limitations like small memory, power constraints, etc, they tend to skip their usual functions in order to save the limited resources. This makes nodes more prone to attacks and thereby reduces the performance of network. A special system named intrusion detection system can be implemented in our wireless network to detect and avoid such attacks. Most of the existing systems work on a distributed approach. Under this approach each node individually identifies and notifies others about the detection of a misbehaving. This paper suggests a system that adopts a more collective approach while

detecting the misbehaving nodes in a given network. A subset of all the active nodes in the network is consulted before taking the final decision about a misbehaving node.

Background Theory:-

Security Issues:-

The development process of a security protocol for MANET is a difficult task because of the following issues:

1. Shared broadcast radio channel: There is only one communication medium available for wireless network and that is air, which is shared by all the nodes belonging to a particular network. Also the data transmitted by one node is received by all its neighbors, which may include malicious or attacker nodes.
2. Lack of centralized authority: In MANETs, the communication is completely peer to peer, without the involvement of any centralized authority to manage the entire network. As a result all the nodes have to perform dual roles of both a host and router.
3. Lack of Association: MANETs are highly dynamic in nature and so the network topology changes very frequently. Also any node can join or leave the network at any point of time with of restrictions.
4. Limited Resource Availability: All the resources needed by the MANET nodes like bandwidth, battery power, computational power, etc are limited.

There are two types of attacks possible on MANETs; they are passive attacks and active attacks. In a passive attack only the data been exchanged within the network is only extracted without any alteration, and the network operation is also not disrupted (Pallavi et al., 2009). In an active attack, the data is either altered or destroyed, which in turn affects the operations of networks. Active attacks are again classified into internal and external attacks. External attacks are performed by nodes that are not a part of the network, where as internal attacks are carried out the nodes within the network itself. Different kinds of attacks observed at different layer of MANET include Wormhole attack, black hole attack, byzantine attack, resource consumption attack, routing attacks like routing table poisoning, rushing attack, packet replication, etc at the Network Layer, Session hijacking at the Transport Layer and finally Repudiation at Application Layer.

In active attacks, the attacker node has to utilize its own resources, however in passive attack, the attacker nodes misbehaves in order to save its own resources (Aarti et al 2013). Misbehavior among the nodes often results in lack of cooperation within the network. Such nodes are termed as malicious nodes or selfish nodes. Selfish nodes themselves do not get involved in providing any services to other nodes however; they utilize the services provided by other nodes in the network. Different types of attacks caused due to lack of cooperation are as follows:

1. *Black hole Attack* : Under this a malicious node M advertises about having a valid route to a particular node say X, causing the other nodes to forward the packet to this malicious node whenever they have to send data to X. Because of this, M is able to extract messages without performing any forwarding operation.

2. *Wormhole Attack* : This attack can be performed with the help of two malicious nodes say M and N. Node M receives the data packets and sends them to node N, through a tunnel from where the packets are resent to network (G.Xiapeng et al 2007). Thus, both the malicious nodes are acting as two end points of the tunnel.

3. *Rushing Attack* : An attacker node receives a route request message from the source. It quickly floods this request throughout the network before other nodes do so. Nodes that receive legitimate Route Request packets assume them to be duplicate copies of the request it already received from the attacker and so discard them. As a result, any route discovered by the source would always contain this attacker node.

4. *Byzantine Attack* : Under this a single or a group of intermediate attacker nodes perform attacks such as routing loops, forwarding packets through non-optimal routes, etc.

Intrusion Detection System:-

Intrusion detection system is software running inside every node that allows the nodes to detect the source of any misbehavior in the network. There are two types of IDS, namely network-based and host-based IDS. Network-based IDS is employed at the boundaries of the network, where they analyze the packets crossing the boundary of the network. The host-based IDS are employed on the host itself, monitoring the process running on the host. Most of the existing systems are mainly classified into three categories:

1. *Credit-Based IDS*: Based on give and take policy. Every node gets paid by a source node for forwarding its packet. Every credit gained is used to send its own packet.

2. *Reputation-Based IDS*: Every node maintains a reputation metric for every other node in the network. This metric could be based on the feature like forwarding behavior pattern of the nodes. The metric value is then used to determine whether a node is malicious or not.

3. *Acknowledgment-Based IDS*: The system find out the malicious nodes of the network purely on the basis of reception of acknowledgment for a packet sent. Several existing IDS systems are based on one of above category. Few examples include Watchguard and Pathrator, Nuggets System, Two-ACK System, EAACK System (Enhanced Adaptive Acknowledgement Scheme), etc.

Proposed System:-

The proposed system works on any routing protocol implemented for mobile ad-hoc networks. In the existing methods a single node that detects the misbehaving node acts as the ultimate decision maker and at times it's decisions may not always be true. But in the proposed system the final decision is taken after considering the opinions of other nodes in the network. The method specified in this paper consists of four main segments namely election, detection, collection and announcement.

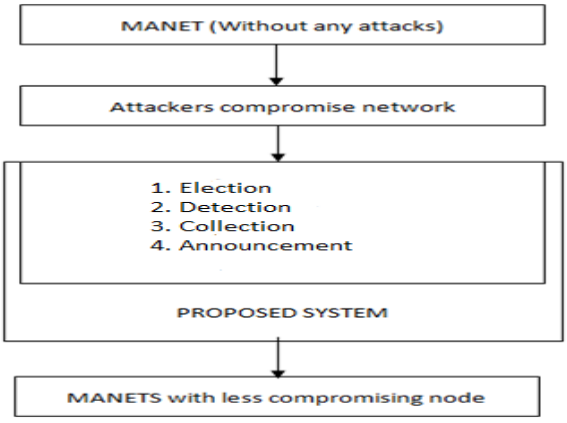

Figure 1. System Architecture

The first segment identifies a leader node in the network. In the next segment, determine the node that is misbehaving and informs the leader node. Next, the leader collects the decision from other nodes about the misbehaving node. If most of the nodes have the same opinions then activate the final segment. In final segment a notification about the confirmed malicious node is created and distributed within the network.

Procedure:-

1. Determine a leader node N_L in the network based on mobility and energy.
2. Inform all the nodes about the leader node.
3. Observe the behavior of the neighboring nodes and checks whether it is displays any kind of misbehavior.
4. If yes, the leader node is immediately informed and the misbehaving node is termed as a culprit node N_C.
5. The leader node collects the trust metric T_{Nc} associated with the culprit node from every other node in the network.
6. If a majority of the nodes have a similar opinion about the culprit node (i.e. it has low trust value), then step 7 is executed else step 8.
7. The culprit node is confirmed to be malicious node N_M and a corresponding notification message is spread throughout the network.
8. The culprit node is termed as a normal node and the warning is ignored.

Initially all the nodes start the election segment. Here each node broadcasts its mobility and remaining energy value throughout the network. The node with the highest energy and least mobility elects itself as the leader (N_L) and informs the remaining nodes of the network. After this normal operation of data transfer begins in the network.

All the nodes observe the packet forwarding behavior of their neighbor nodes. Based on the packet drop ratio the node decides whether the neighboring node is misbehaving or not. If the drop is very high then that particular node is coined as a culprit node N_C and the detail of N_C is send to the leader. The leader node generates a trust request message and transmits it throughout the network. Those nodes that maintained a trust metric value (T_{Nc}) for the specified culprit node, must reply with a trust reply message. If a majority of the nodes term N_C as a malicious node then the warning is taken to be true and the next segment is activated. Else the warning is ignored. This segment gets activated only when confirmed news about a malicious node is obtained. The leader node generates an announcement message stating the malicious node N_M and broadcasts it throughout the network.

On receiving such an announcement from the leader node, all the nodes update their routing tables by deleting all the routes that contain the misbehaving nodes. Since no routes containing the misbehaving nodes are taken by any of the packets transmitted, the overall packet drop ratio is low and so the network performance also increases thereby.

Performance Evaluation:-

The proposed system is simulated using NS-3.24.1 The simulated network scenario used a mobility model named RandomWalk2MobilityModel. The simulation ran for 30 seconds. The metrics used for the simulation are shown in

Table 1.

Attribute	Value
Area	150*150
No. Of Nodes	25
Routing Protocol	AODV, Collective Judgment System
Packet Size	1024
Interval	0.1

Table1. Simulation Parameters

Figure 2 represents the packet delivery ratio for cooperative judgment system as well as AODV. Clearly we can conclude that the packet delivery ratio is slightly more for the cooperative judgment system than the AODV as the simulation time increases.

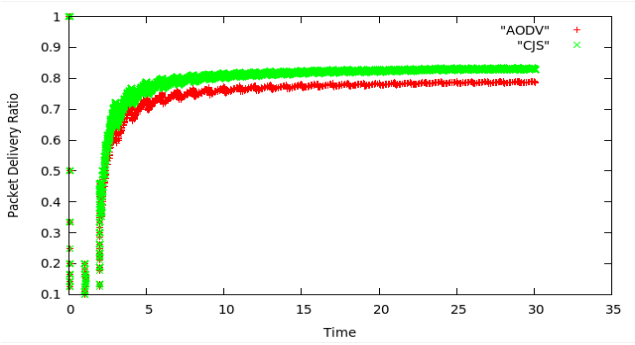

Figure 2: Packet Delivery Ratio

Conclusion:-

The system proposed in this paper is an intrusion detection system that works on a collective approach to identify the misbehaving nodes in a network. The system is divided into four segments namely election, detection, collection and announcement. During the first segment a leader node is identified, followed by a segment to identify the misbehaving nodes. Next the leader node takes an ultimate decision of whether a node is actually misbehaving or not after consulting all the other nodes in the network. The last segment is used to inform all the other nodes about any confirmed malicious nodes. This significantly improves the network performance factors like throughput and packet delivery ratio for networks with large number of nodes.

References:-

1. **K. Liu, J. Deng, P. K. Varshney and K. Balakrishnan.(2007).** "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," IEEE Transaction on Mobile Computing, vol. 6, no. 5, pp. 536-550.

2. **R.H Akbhani, S.Patel and D.C. Jinwala.(2012).**" DoS attacks in mobile ad-hoc networks: survey", Proceedings of ACCT 2nd International Meeting, pp. 535-541.

3. **Aarti and S. S. Tyagi.(2013).**, "Study of MANET: Characteristics, Challenges, Application and Security Attacks," in Proceedings of International Journal of Advanced Research on Computer Science and Software Engineering, vol.3, no. 5, pp. 252-257.

4. **S. Marti, T.J. Giuli, K. Lai and M. Baker.(2000).**, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in 6th International Conference on Mobile computing and Networking, MOBICOM '00, pp.255-265.

5. **L. Buttyan and J. Hubaux.(2003).**, "Stimulating cooperation in self-organizing mobile ad-hoc networks," in Mobile Networks and Applications, vol. 8, no. 5, pp. 579-592.

6. **G.Xiapeng and C.Wei.(2007).**, "A novel gray hole attack detection scheme for mobile ad-hoc networks," in IFIP International Conference on Network and Parallel Computing, pp. 209214.

7. **Pallavi Khatri, Sarida Bahadoria and Mamta Narworia.(2009).**, "A survey on Security issues in mobile ADHOC networks", in International Journal of Computing Science and Communication Technologies, vol. 2, no. 1, pp. 334-324.