Secured Intrusion Detection System in Mobile Ad Hoc Network using RAODV

S.Sasikala
Head of UG Computer Science
Sree Saraswathi Thyagaraja College
Pollachi – 642 107, Coimbatore.

M.Vallinayagam
Research Scholar of Computer Science
Sree Saraswathi Thyagaraja College
Pollachi – 642 107, Coimbatore.

ABSTRACT

Wireless Mobile ad-hoc network (MANET) is an emerging technology and has great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance. MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc also contains wireless sensor network so the problems is facing by sensor network is also faced by MANET. While developing the sensor nodes in unattended environment increases the chances of various attacks. The Intrusion Detection is one of the possible ways in recognizing a possible attacks before the system could be penetrated. The encryption and authentication solution, which are considered as the first line of defense, are no longer sufficient to protect MANETs. Therefore, Intrusion Detection Systems (IDSs) is needed to be the second line of defense to protect the network from security problem. There are many security attacks in MANET and DDoS (Distributed Denial of service) is one of them. In this paper we discussed some attacks on MANET and DDOS also and provide the security against the DDOS attack.

Keywords

Manet, Intrusion detection, Distributed Denial of Service.

1. MOBILE AD-HOC NETWORK

Mobile ad hoc network is an autonomous system, where nodes/ stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile ad hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology.

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure [4]. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing), AOMDV (Ad-hoc On-Demand Multipath Distance Vector), and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.

1.1 NETWORK SECURITY

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them .

SECURITY GOALS

For analyzing the security of wireless mobile adhoc networks, we need certain parameters. The basic parameters for a secure system are:

- Availability
- Confidentiality
- Authentication
- Integrity
- Non-repudiation
- Scalability [5].

1.2 SECURITY MEASURES IN MANET

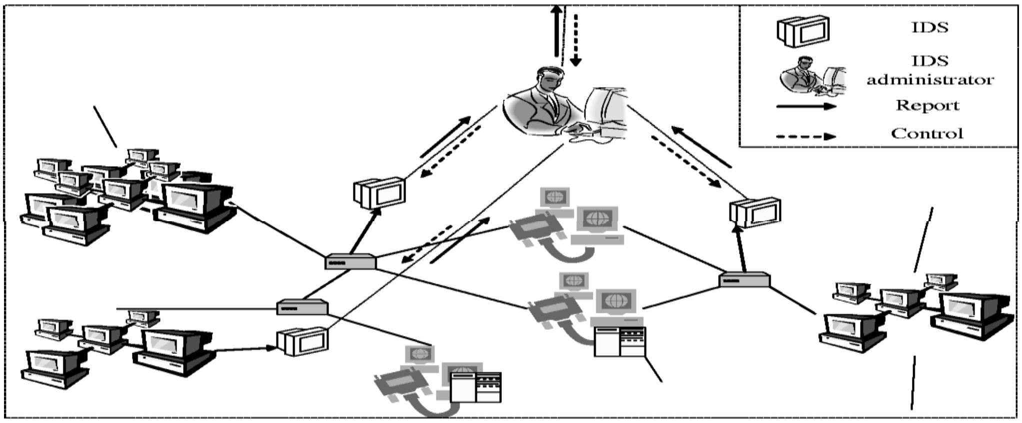
Security in Mobile Ad Hoc Network is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

1.3 INTUSION DETECTION SYSTEM

In general terms denial-of-service occurs when an entity cannot perform an action, access a service that he is entitled to. In the networking world this usually means that a legitimate node on the network is unable to reach another node or their connectivity is severely degraded.

A distributed denial-of-service attack occurs when the attackers use several machines to launch the attack, making it more powerful. With a few thousands of DSL-connected home computers an attacker could saturate the well provisioned link of a major website.The focus of this thesis is on the intrusion detection subsystem, which constitutes the first line of defense for a computer network system. There are a number of approaches in this field. Most of them fall into three primary categories: anomaly detection, misuse detection and hybrid schemes.



Intrusion detection can be classified into three broad categories:

- Anomaly Detection,
- Signature or Misuse Detection, and
- Specification based Detection.

1.4 NEED FOR INTRUSION DETECTION SYSTEM

The nature of mobility creates new vulnerabilities due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management points and up till now many of the proven security measures turn out to be ineffective. So there are needs more security mechanisms in mobile ad hoc network.

The security solution should protect each node in the network and the security of the entire networks relies on the collective protection of all the nodes. The security solution should not be for a single layer in the network. The security solution should protect the network from both the inside and outside intruders into the system .The security solution should encompass all three components of prevention, detection, and reaction that work in concert to guard the system from collapse. The security solution should be practical and inexpensive in a highly dynamic and resource constrained networking scenario. However an attacker succeeds in infiltrating the security system and causes them to misbehave. Node misbehavior can result in degradation of network performance. Therefore there is need of intrusion detection system for monitoring the anomalies and take necessary actions if an anomaly is detected. In the next session different types of attack in MANET are discussed.

1.5 DoS attacks in MANET

DoS attacks can be launched in two basic forms: software exploit and flooding, as illustrated in Figure 1. In the case of the **software exploits attack**, the attacker node will send few packets to exercise specific software bugs within the target node application, disabling this way the victim. They can usually be addressed by adequate software fixes. Flooding tends to inject a large amount of junk packets into the network. Flooding attacks are further classified to single (DoS) and multisource (DDoS).[10]

2. METHODOLOGY

In this proposed system is mainly focused on Intrusion Detection System making effective security using RAODV protocol. Because a trust relationship is established based on a dynamic evaluation of the sender’s “secure IP” and signed evidence, contained in the RAODV header. Ad hoc routing protocols have been designed to efficiently reroute traffic when confronted with network congestion, faulty nodes, and dynamically changing topologies.

2.1 OVERVIEW OF PROPOSED METHODOLOGY

A New Proposed Intrusion Detection Algorithm has been used for providing the secure MANET. In this proposed Intrusion Detection algorithm used the protocols RAODV and AODV for measuring the efficiencies of the network security. Compared to existing protocol AODV in RAODV protocol malicious nodes are detected. RAODV protocol gives the alarm to the neighboring nodes and also the performance time is increased when compared with AODV protocol.

The overview of proposed methodology is consists as such as follows

1. Proposed algorithm
2. Protocols
    - AODV
    - RAODV

The proposed algorithm gives the better security compared with AODV protocol and performance also increased.

2.2 PROPOSED ALGORITHM

In proposed algorithm firstly created an IDS node. Then set RAODV as a routing protocol. IDS node would check the configuration of the network. IDS node capture load by finding that if any node is in its radio range and also the next hop is not null, also it capture all the information of nodes in the network. Else it display nodes are out of range or destination unreachable. IDS node creates a normal profile with the help of this information obtained from the nodes. Profile contains information like type of packet, in our case (protocol is RAODV, pkt type TCP, UDP, CBR), time of packet send and receive and threshold. After creating normal profile the threshold checking is done in the network that is if network load is smaller than or equal to maximum limit and new profile is smaller than or equal to maximum threshold and new profile is greater than or equal to minimum threshold. If the condition satisfied means no attack present in the network. Else there is an attack in the network and find the attack. For finding the attack first compare normal profile with each new trace value. The trace value contains to check packet type, count unknown packet type, arrival time of packet, sender of packet, receiver of packet. After detection of any anomaly in that parameters then block that packet sender node (attacker node) and also produce the alarm.

The benefits of this IDS technique are that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack.

2.2.1 Modules

- **User Registration**

In this module, user registers his/her personal details in database. Each user has unique id, username and password and digital signature. After using these details he can request file from server.

- **Upload & Send files to users**

In this module, server can upload the files in the database. After verify user digital signature file could be transfer to correct user via mobile ad-hoc network.

- **Attack on Ad-Hoc Network**

In this module, to see what the attack on ad-hoc is network is Distributed Denial of Services (DDoS).

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

- **Simulation Results**

In this module, implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity.

a. Throughput
b. Packet delivery fraction
c. End to End delay
d. Normalized routing load

2.3 PROTOCOLS

The protocols AODV and RAODV are used in this proposed algorithm. The efficiency of proposed algorithm is based on selections of protocol. Because each protocols have its own aspects and drawbacks.

2.3.1 AODV protocol

Ad Hoc On-Demand Distance Vector Routing Protocol (AODV) is based on DSDV and DSR. A source node floods RREQ (Route Request) messages, and a destination node sends a RREP (Route reply) along the path with the most recent sequence number. An AODV node only records the next hop of the route. The packets need not store the route as they do in DSR.

AODV has a scalability problem because the size of the routing table grows linearly with the number of the nodes. The movement of the nodes may trigger frequent flood-searches, which is the combination of the overhead of DSDV state maintenance plus DSR flooding. AODV does not have any security mechanisms, so it is vulnerable to many attacks.

AODV has better performance than other MANET routing protocols. It is also the most discussed, compared, and extended protocol. Some research projects focus on AODV extension and improvement. Power aware AODV focuses on extending the battery life in the AODV environment. Multipath AODV uses a pair of link-disjoint paths to improve the fault tolerance of the route. Mobile agents based AODV uses ant-like technology to save the network resource. Secure AODV (SAODV) uses the public key algorithm and signature method to validate the traffic.

2.3.2 Reliable Ad-hoc On-demand Distance Vector Routing (RAODV) Protocol

The existing AODV has been extended to RAODV by adding two types of control packets: Reliable Route Discovery Unit (RRDU) and RRDU Reply (RRDU_REP). The RRDU messages are control packets sent by the source node along with RRDU-ID, to the destination at regular intervals and RRDU_REP message is the response of RRDU by the destination to the source node. RRDU_REP can only be generated by the destination. There is no impersonation i.e. no node other than the destination, can generate RRDU_REP on behalf of the destination.

A New protocol has been proposed titled RAODV modifying AODV Protocol. In RAODV protocol malicious nodes are detected. Then using NS-2 simulator a comparative study of protocols AODV and RAODV has been carried out for 10, 25 nodes .The simulation has been performed using TCL scripts. The simulation results have been obtained with the help of three metrics as Packet delivery ratio, End to End Delay and Throughput. The results of AODV and RAODV are represented in the form of Graph. Using these graphs AODV and RAODV performance comparison have been made. To carry out the analysis a malicious node has been introduced in the script. This node when comes in direct communication contact with the routing nodes, results in hacker attack. This causes fall of packets. This performance has been studied using extensive simulations with varying scripts. The proposed scheme takes care of this node and the authors remove this node and generate a new path. This new path will be secured and will result in stable and secured routing

Mobile ad-hoc networks devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other.

2.4 QUANTITY PARAMETERS

In our simulations used several performance metrics to compare the proposed RAODV protocol with the existing one. The following metrics were considered for the comparison were

2.4.1 Throughput

Number of packets sends in per unit of time.

2.4.2 Packet delivery fraction (PDF)

The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes. The performance of the protocols decreases as the pause time decreases & the performance of the protocols increases as the pause time increases.

$$\text{Packet Deliver Fraction} = \frac{\text{Total data packets received}}{\text{Total data packets sent}} * 100$$

2.4.3 End to End delay

This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets. Measure as the average end to end latency of data packets.

$$\text{End to End Delay} = \frac{\text{Time Received} - \text{Time Sent}}{\text{Total Data Packets Received}}$$

\

3. SIMULATION ENVIROMENT

Implementation of wireless ad-hoc networks in the real world is quite hard. The simulation is implemented in Network Simulator, a simulator for mobile ad hoc networks. The simulation parameters are provided in Table 4.1. Implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen 35 m/s. A packet size of 512 bytes and a transmission rate of 4 packets/s,

The Network Simulator is implemented in a simulator for mobile ad hoc networks. The simulation parameters are provided in Table 4.1.

TABLE: 4.1 Simulation Parameters for Case Study

Examined Protocol	RAODV
Number of nodes	25
Dimension of simulated area	800×600
Simulation time (sec)	32.94
Radio range	250m
Traffic type	CBR
Packet size (bytes)	512
Node movement	Random
Types of attack	DDOS

The simulation area is set to 800m x 600m, on which25 nodes with transmission range of 250m are initially distributed uniformly and randomly. IEEE 802.11 and RAODV are used for medium access control and routing protocol, respectively. The propagation model is two ray ground. Table 1 contains parameters of the investigated mobility models. The aim is to keep as much as possible realistic conditions of nodes movement.

3.1 PEFORMANCE COMPARISON OF AODV and RAODV

RAODV behaves as AODV in the absence of attack by malicious node. If there is no malicious or selfish node present in the network, the source will get one or more RREPs. It will choose a path for sending data packets as that of AODV. In case, a malicious or a selfish node is present in the system, AODV fails. On the other hand, RAODV will find an alternate path after a loss of few data packets. The lost packets are transmitted. Hence RAODV outperforms AODV in presence of attack. After some time if some reliable node comes in place of the malicious node and there is some shortest path to destination through it, the path through this node is included for all future communication when fresh RREQs are sent. Hence RAODV recovers from the attack and start behaving like AODV.

4..CONCLUSION

This work analyzed the routing security issues of MANETs, described the DDoS attack that can be mounted against a MANET. This work used a protocol called Ad-hoc On-demand Multipath Distance Vector Routing (RAODV) to avoid the DDoS attack in the AODV. The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self-organizing nature. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably.

This proposed system also emphasized the RAODV protocol performs better. In case of 25 nodes it detect almost all hackers as no of hackers are very less. As the no of nodes increases no of hackers also increases but RAODV protocol perform very well. It provides better security compared to other protocols like AODV. The proposed RAODV provides better security to data packets for sparse and significant security for denser medium.The scope for future enhancement these extend the nodes range with the maximum distance, reduce the reduction time and increasing the efficiency of the protocol. This will provide real life situations and provide a robust and effective solution for security.

6. REFERENCES

[1] IEEE Std 802-2002, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture, page 1, section 1.2: "Key Concepts Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] Gary A. Donahue (2007-06). Network Warrior. O'Reilly. Page No 5.

[3] Toby Skandier, Groth, David; (2005). Network Study Guide, Fourth Edition .Sybex, Inc.0-7821-4406-3. ISBN.

[4] S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312.

[5] Gaurav Kumar Gupt1, Mr. Jitendra Singh2, "Truth of D-DoS Attacks in MANET" in Global Journal of Computer science and technology,Vol.10 Issue 15 (Ver. 1.0) December 2010 Page-15.

[6] Kathole A.B, Pardakhe N.V, Kute D.S. and Patil A.S, "A review paper on comparison and analysis of different attack and intrusion detection system", International Journal of Cryptography and SecurityISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-18-21.

[7] F. Anjum, D. Subhadrabandhu and S. Sarkar, "Signature based intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[8] D. E. Denning, "An Intrusion Detection Model," IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222- 232, USA, 1987.

[9] Wei-Shen Lai, Chu-HsingLin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang," Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks", International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008).

[10] Mirjana Stojanovic1, Valentina Timcenko2, SlavicaBoštjancicRakas, "Intrusion Detection against Denial of Service Attacks in Manet Environment" in XXIX Simpozijum , December 2011.