ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

An Efficient Algorithm to Mitigate Packet Drop Attack in AODV Protocol

Arunprasath.M[1], Mr.M.Mohana Sundharam[2]

Assistant Professor, Department of Electronics and Communication Engineering, SRM University, Kattankulathur, Tamilnadu, India[1]

M.Tech Scholars, II Year, Department of Communication Systems, SRM University, Kattankulathur, Tamilnadu, India[2]

ABSTRACT: MANET refers to network designed for special application for which it is difficult to use a backbone network. In MANET, applications are involved with sensitive and secret Information. Since the MANET assumes a trusted environment for routing, security is major issue. In this paper the vulnerabilities of a reactive routing protocol called AODV protocol in MANET is analyzed. Analyzing the attack, a mechanism is proposed to secure the AODV protocol from specific routing attack known as PACKET DROP ATTACK where the malicious node acts as a black-hole and drops packets. The simulator used for this proposed mechanism is NS2 simulator, which is able to detect any number of malicious nodes and improves PDR and through put and also reduces the packet drop.

KEYWORDS: MANET, AODV, security, Packet Drop Attack.

I. INTRODUCTION

In works (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. Such as military battle field, emergency rescue, vehicular communication, mining operation, etc.

These networks are subject to frequent link breaks which also every node can perform the role of host as well as router, thus nodes which are out of transmission range can be accessed by routing through the intermediate nodes. Because of the characteristic of dynamic wireless network, MANET presents the following set of unique challenges to secure. Dynamic network: the topology of MANETs is highly dynamic as mobile nodes freely roam in network, join or leave the network on their own will, and fail occasionally. Mobile users roaming in the network may request for anytime, anywhere security services. Resource constraints: the wireless channel is bandwidth constrained and shared among multiple networking entities. No clear line of defense: Moreover, the wireless channel is accessible to both legitimate users and malicious attackers.

The limitation of wireless network and mobile nodes poses an important challenge for implementation of cryptographic algorithms for providing security to these networks. Routing security is an important issue in MANET .The boundary that separate the inside network from the outside world becomes blurred. In MANET, two types of messages are used: data messages and routing or control messages. Data messages need end to end authentication and can be secured using point to point security mechanism. Routing messages are used for the route establishment and route maintenance. Routing messages are processed by intermediate nodes during their propagation therefore securing routing messages is more challenging compared with data messages.

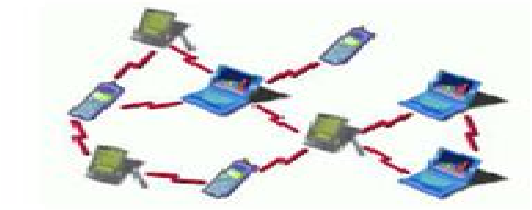


Fig I.Mobile Ad Hoc Network

In this paper the dealing is with misbehavior nodes in MANETs that drop packets instead of forwarding them towards the destination .This "Packet Drop Attack" is a serious threat to operational mobile ad hoc networks. Although the proposed method is focused on AODV protocol, the proposed solution is applicable to other routing protocols for MANETs.

II. SECURITY ATTACKS

Securing wireless ad hoc networks is a highly challenging issue. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

A. Passive Attacks

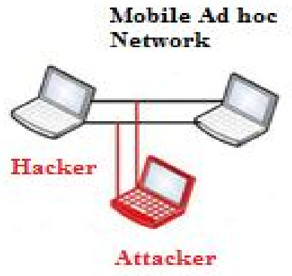


Fig II.A.Passive attack

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping. Detection of these attacks is difficult since the operation of network itself does not get affected. Encryption algorithms are used to prevent passive attacks.

B. Active Attacks

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network[8]. Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. It modifies the data stream or creation of false stream. Active attacks can be internal or external.

1. External attacks are carried out by nodes that do not belong to the network. This attack can be prevented by using cryptographic techniques such as encryption.

2. Internal attacks are from compromised nodes that are part of the network.

Internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation modification, fabrication and replication.

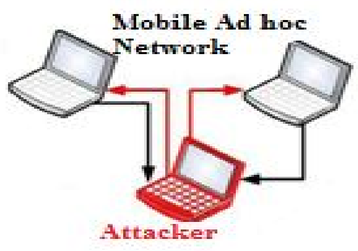


Fig II.B.Active attack

III. AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV) PROTOCOL

The Ad hoc On Demand Distance Vector Algorithm Our basic proposal can be called a pure on demand route acquisition system nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges Further a node does not have to discover and maintain a route to another node until the two need to communicate unless the former node is oaring its services. As an intermediate forwarding station to maintain connectivity between two other nodes when the local connectivity of the mobile node is of interest each mobile node can become aware of the other nodes in its neighborhood by the use of several Techniques including local system wide broad casts known as hello messages. The routing tables of the nodes within the neighborhood are organized to optimize response time to local movements and provide quick response time for requests for establishment of new routes. The algorithms primary objectives are

To broadcast discovery packets only when necessary

To distinguish between local connectivity management neighborhood detection and general topology maintenance

To disseminate information about changes in local connectivity to those neighboring mobile nodes that are likely to need the information AODV uses a broadcast route discovery mechanism as is also used with medications in the Dynamic Source Routing DSR algorithm Instead of source routing however AODV relies on dynamically establishing route table entries at intermediate nodes.

The network consists of many nodes. To maintain the most recent routing information between nodes we borrow the concept of destination sequence numbers from DSDV. Unlike in DSDV, however each ad hoc node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes. The combination of these techniques yields an algorithm that uses bandwidth efficiently by minimizing the network load for control and data traffic is responsive to changes in topology and ensures loop free routing.

IV. PATH DISCOVERY

The Path Discovery process is initiated whenever a source node needs to communicate with another node for which it has no routing information in its table every node maintains two separate counters a node sequence number and a broadcast id. The source node initiates path discovery by broadcasting a route request RREQ packet to its neighbors. The RREQ contains the following fields
Source address, source sequence, broadcast id, destination address, destination sequence, hops count.

The pair source address broadcast id uniquely identifies a RREQ broadcast id is incremented whenever the source issues a new RREQ. Each neighbor either satisfies the RREQ by sending a route reply RREP back to the source or rebroadcasts the RREQ to its own neighbors after increasing the hop count.

When an intermediate node receives a RREQ if it has already received a RREQ with the same broadcast id and source address it drops the redundant RREQ and does not rebroadcast it if a node cannot satisfy the RREQ.

It keeps track of the following information in order to implement the reverse path setup as well as the forward path setup that will accompany the transmission of the eventual RREP[7]

1. Destination IP address
2. Source IP address
3. Broadcast id
4. Expiration time for reverse path route entry
5. Source nodes sequence number

A. Reverse Path Setup

There are two sequence numbers in addition to the broadcast id included in a RREQ the source sequence number and the last destination sequence number known to the source. The source sequence number is used to maintain freshness information about the reverse route to the source and the destination sequence number species how fresh a route to the destination must be before it can be accepted by the source .As the RREQ travels from a source to various destinations it automatically sets up the reverse path from all nodes back to the source[4] as illustrated in Figure1.

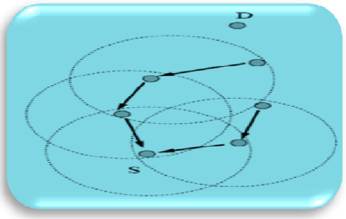


Fig.IV.A.Reverse path formation

B. Forward Path Setup

Eventually a RREQ will arrive at a node possibly the destination itself that possesses a current route to the destination. The receiving node request checks that the RREQ was received over a bidirectional link. If an intermediate node has a route entry for the desired destination it determines whether the route is current by comparing the destination sequence number in its own route entry to the destination sequence number in the RREQ. If the RREQs sequence number for the destination is greater than that recorded by the intermediate node the intermediate node must not use its recorded route to respond to the RREQ[7]. Instead the intermediate node rebroadcasts the RREQ. The intermediate node can reply only when it has a route with a sequence number that is greater than or equal to that contained in the RREQ. Figure2 represents the forward path setup as the RREP travels from the destination D to the source node S. Nodes that are not along the path determined by the RREP will timeout after ACTIVE ROUTE TIMEOUT msec and will delete the reverse pointers. A node receiving an RREP propagates the request RREP for a given source node towards that source. If it receives further RREPs it updates its routing information and propagates the RREP only if the RREP contains either a greater destination sequence number than the previous RREP or the same destination sequence number with a smaller hop count It suppresses all other RREPs it receives. This decreases the number of RREPs propagating towards the source while also ensuring the most up to date and quickest routing information. The source node can begin data transmission as soon as the request RREP is received and can later update its routing information if it learns of a better route.

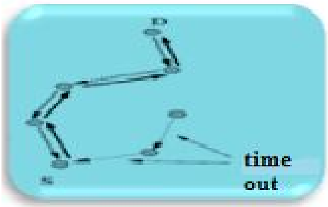


Fig.IV.B.Forward Path Formation

V. PACKET DROP ATTACK

From the analysis of basic Ad hoc on-demand distance routing protocol's operation, it is inherently understandable that the design assumes the participants to forward others packets, which is an unrealistic anticipation in an independent network like MANET. The consequence of not forwarding others packets or dropping others packets prevents any kind of communication to be established in the network. Hence given a choice between the necessity to secure services or to ensure basic functioning of the network, intrinsically the choice falls for the latter. Therefore, the need to address the packet dropping event takes higher priority for the mobile ad hoc networks to emerge and operate successfully. A packet may be dropped under various reasons, which in turn can be grouped into the following categories,

1) Unsteadiness of the medium,
A packet may be dropped due to contention in the medium.
A packet may be dropped due to congestion and corruption in the medium
A packet may be dropped due to broken link
2) Genuineness of the node,
A packet may be dropped due to overflow of the transmission queue
A packet may be dropped due to lack of energy resources
3) Selfishness of the node,
A packet may be dropped due to the selfishness of a node to save its resources
4) Maliciousness of the node,
A packet may be dropped due to the malignant act of a malicious node

The unsteadiness of the medium generally causes errors in the packet, which forces the benign node to drop the packet even if the node aspires to forward it. On other hand, a genuine node with zero options may drop the packets when it runs out its resources. Though a packet may be dropped in the similar manner by a selfish or a malicious node, they distinctly differ from the others because the packets are dropped intentionally. From the above examination, it is obvious that the intentional packet drop events have to be tackled, which we generalize as "Packet Drop Attack", contrast to the accidental packet drop events. However, we envisage that the proposal should also encompass mechanisms to detect the accidental packet drops and adjust dynamically according to them, thereby enhancing the basic operation of the protocol. Generally, there are two types of attackers: The type-1 attacker drops all the received packets. The type-2 attacker is smarter and drops only data packets and exchanges control packets normally. In this paper, we will investigate type-2 attackers.

VI. PROPOSED METHOD

In this proposed method, the security is raised by distinguishing the invalid path from the valid path. By discovering the valid path we can send our data packets through it. The invalid path consists of some malicious nodes yet it forwards the control packets similar as the normal intermediate node but during reception from the next node it discards data packets. The first process consists of route discovery and route reply mechanism. The validity of intermediate node is identified by forwarding the RREQ or RREP packets during each hop, this is the proposed model. In route discovery process source node send RREQ or RREP to the neighbor node, the neighbor node send back the CM packet (a small data packet) towards the sender node. The previous node which has forwarded the RREQ or RREP packet sends the ACK packet back to the intermediate node to identify the validity of the path along which the data packets are transmitted is shown in the following figure.

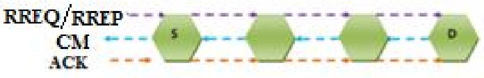


Fig.VI.a.Route Discovery Process

A validate algorithm to find out the malicious node in the network and sending of data packets through valid path is discussed. This algorithm is applicable during the route discovery process. If the previous node is the normal node which receives the small data packets, it is able to send the ACK to intermediate node. In case of malicious node it discards the data packets and it is not able to send ACK back. Once if node that receives the CM fails to reply, then the intermediate node increase the number of times of sending CMs. The intermediate node sends the CM packet three times and each time it waits for a reply. A normal node may be not able to send reply due to disconnection of link or its sources, so RREQ/RREP packet is discarded. The process is not continued because the assumption is made, that the packet has come from the malicious node. It alters the routing information and then drops all those packets. If the one intermediate node knows there is a malicious node in the network it will alert all other nodes in the network there is a malicious node. Then the data packets will be send through another valid path is shown in the following figure.

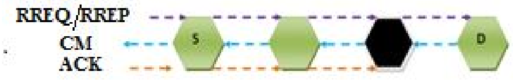
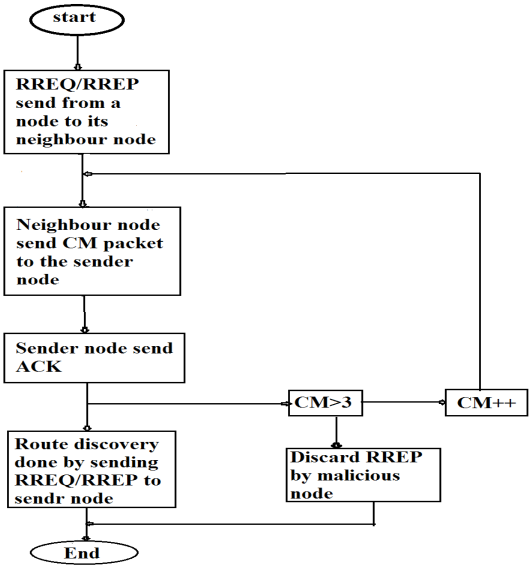


Fig.VI.b. Attacker drops CM packet (data packet)

VII. FLOW CHART


start
RREQ/RREP send from a node to its neighbour node
Neighbour node send CM packet to the sender node
Sender node send ACK
CM>3
CM++
Route discovery done by sending RREQ/RREP to sendr node
Discard RREP by malicious node
End

ALGORITHM

STEP 1: Start process

STEP 2: Initially the source node sends the route request or route reply to their intermediate node.

STEP 3: Intermediate node send CM packet to sender node.

STEP 4: An intermediate node wait for the ACK from the sender node.

STEP 5: If CM packet count is less than 3 means the intermediate node sends the CM packets repeatedly till it receives the acknowledgement.

STEP 6: Else if CM packet count is greater than 3 means inter mediate note discard route request or route reply

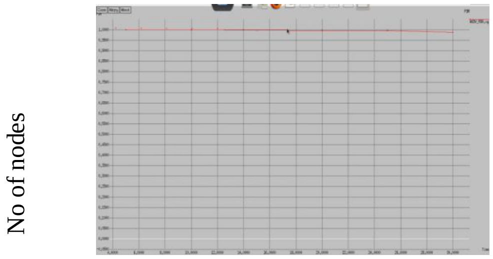
STEP 7: Source node receives the acknowledgement then it will identify that it is not a malicious node then it will send route request or route replay to another node.

STEP 8: End process.

We represent a validate algorithm to find out the malicious node in the network and send our data packets through validate path which contain valid node our algorithm is applicable during the route discovery process.

VIII. SIMULATION GRAPH

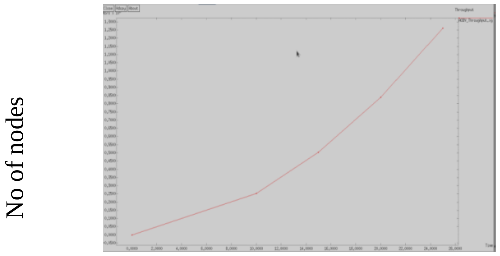
PACKET DELIVERY RATIO:



pdr

The packet delivery ratio increases as the number of nodes increases and after reaching a particular point the delivery rate remained constant and was maintained in a steady state.

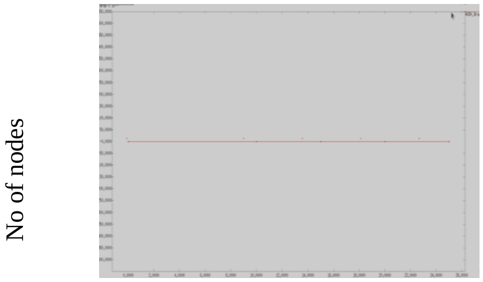
THROUGHPUT:



Throughput

The above graph shows that the throughput of the network increases as the number of nodes increases.

PACKETDROP:



Packet drop

The above graph indicates the performance of AODV in case of packet dropping. Though there are various secure protocols, this protocol improves efficiency of the network since it shows nil packet drop. Thus the results which are simulated above prove that our AODV protocol secure protocol is efficient compared with other protocols in terms of packet drop, throughput and packet delivery ratio.

IX. CONCLUSION

In this paper, we have presented a method based on End-to-End connection for securing the AODV protocol. Our method can detect many types of malicious node(s) that drop packet through the path between the source and the destination. The collaboration of a group of nodes is used to make accurate decisions. Discarding packets have come from malicious node(s) enables the source to select another trusted path to its destination. We achieved better performance results when action was taken to detect malicious nodes by validation operations. The simulation results showed that our method is able to detect any number of attackers and fictitious packets.

REFERENCES

1.Hu, Y., Johnson, D.B., & Perrig, A. (2002b). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), 3-13.

2.Hu, Y.C., & Perrig, A. (2004). A survey of secure wireless ad hoc routing. IEEE Security and privacy, 2(3), 28-39.

3.Perkins, C.E., & Royer, E.M. (1999). Ad hoc on-demand distance vector (aodv) routing. Proceeding of IEEE Workshop on Mobile Computing System and Applications. 90-100.

4.Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., & Royer, E.M.B. (2002). A secure routing protocol for ad hoc networks. Proceedings of IEEE ICNP, 78-87.

5.Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L.(2004). Security in mobile ad hoc networks:Challenges and solutions. Wireless Communications, IEEE, 11, 38-47.

6.M.S.Corson and A.Ephremides. A Distributed Routing Algorithm for Mobile Wireless Networks. ACM J Wireless Networks,1.jan 1995.

7. Perkins, C. E, Belding-Royer, E. M, & Das, S. R. (2003). Ad hoc on-demand distance vector (AODV) routing. Internet Request for Comments, RFC3561.
8. C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.
9.Z.Karakehayov, "Using REWARD to Detect Team Black-Hole Attacks in Wireless Sensor Networks," Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.
10. Venkatesan Balakrishnan and Vijay Varadharajan. Packet Drop Attack: A Serious Threat To Operational Mobile Ad Hoc Networks.