ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

Security requirements to the routing information of a Adhoc On-demand Distance Vector (AODV) routing protocol in Mobile Adhoc Networks (MANET)

J RAJESHWAR[1], Dr G NARSIMHA[2]

Department of Computer Science and Engineerin , Research Scholar, , JNTUH College of Engineering JNTUH, Kukatpally, Hyderabad A.P, India[1]

Department of Information Technology, Assistant Professor, JNTUH College of Engineering,Kondagattu, Jagityal, Karim Nagar, A.P, India[2]

Abstract: A mobile ad hoc network (MANET) is an infrastructure less and autonomous network where a set of nodes are connected by wireless links where each node works both as a router and an end system. Due to vulnerable features of MANET it is prone to several attacks from insider as well as outsider. Routing is one of the most basic networking functions in mobile ad hoc networks. AODV is chosen as the best routing algorithm for MANET by IETF. It is best routing protocol in trusted environment, but in the presence of malicious node, compromised and selfish nodes several attacks can be launched against AODV, as there is no proper security to its routing information This paper is proposing security mechanism to protect the routing information of AODV. The security mechanism is using digital signature (MAC) and hash chain to the routing information. In hash chain a secure MD-5 algorithm is used. The proposed method is compared with the basic AODV routing protocol and proven to be the best. The analysis can be done using NS2 or GloMoSim network simulating tools. In this paper NS-2 is used.

Keywords: MANET, AODV, Digital signatures, MD-5 Hash function.

I. INTRODUCTION

A self configured moving nodes forming as a group to communicate each other is called as Mobile Ad Hoc Networks (MANET). Now a day's MANET's became very much popular and they have been used in most of the systems due to its flexibility in forming a network with less infrastructure requirement, its speed of configuration and they can be easily deployable.

MANETs became very much popular due to their wide variety applications, they are Law of enforcement operations automated military applications like Battlefield communications, Rescue & disaster recovery operations, Interactive lectures and Data sharing in classrooms, Meeting events and conferences, intelligent building and logistics etc.

MANETs are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load).

Many of the ad hoc routing protocols that address security issues rely on implicit trust relationships to route packets among participating nodes. Besides the general security objectives like authentication, confidentiality, integrity, availability and non-repudiation, the ad hoc routing protocols should also address location confidentiality, cooperation fairness and absence of traffic diversion.

During the last few years, we have all witnessed a continuously increasing growth in the deployment of wireless and mobile communication networks. Mobile ad hoc networks consist of nodes that are able to communicate through the use of wireless mediums and form dynamic topologies. The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

exist. Therefore, a network layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols [1]. Unfortunately all of the widely used ad hoc routing protocols have no security considerations and trust all the participants to correctly forward routing and data traffic. This assumption can prove to be disastrous for an ad hoc network that relies on intermediate nodes for packet forwarding.

In this paper presented the performance impacts faced by the ad hoc network environment and made a comparative analysis between the proposed system and original AODV (Ad hoc On Demand Distance Vector).

This paper is organized in the following way chapter 1 describes the introduction of MANET and its security concerns, chapter 2 tells about the functionality of AODV, chapter 3 describes the proposed system, chapter 4 discusses the result analysis and the chapter 5 with the conclusion.

II. RELATED WORK

A. Original AODV Routing Protocol [2]

It is an on-demand routing protocol it is also called as reactive protocol. It developed for routing operation of mobile ad hoc network. This protocol provides self starting, dynamic, loops free, multi hop routing [3, 4]. Using this protocol routes can be quickly established in the environment where links are often broken thus forming the dynamic topology. Inactive nodes information is deleted, new routes are discovered as per the requirement only. AODV protocol's functionality is divided in to two categories a) route discovery process and b) route maintenance process.

B. Route discovery process in AODV

It uses Route Request (RREQs), Route Reply (RREPs) and Route Error (RERRs) messages. The routing messages contain information only about the source and the destination. When a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbors to find the optimal path. RREQ message contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. When a node sends any type of routing control message like RREQ/RREP, it increases its own sequence number. Every node should include the latest sequence number for the nodes in the network in its routing table. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. It is used for maintain fresh routes as well as for preventing loops and faster convergence. Hop count represents the distance in hops from the source to destination. Each node receiving the RREQ message sets up reverse path back to the sender of the request so that RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and discards the RREQ. If the intermediate node receives RREQ with 'G' flag set, it must also unicast gratuitous RREP to the destination node. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP travels along the reverse path. Once the source node receives the route reply, it establishes a route to the destination and sends data packet along forward path set-up.

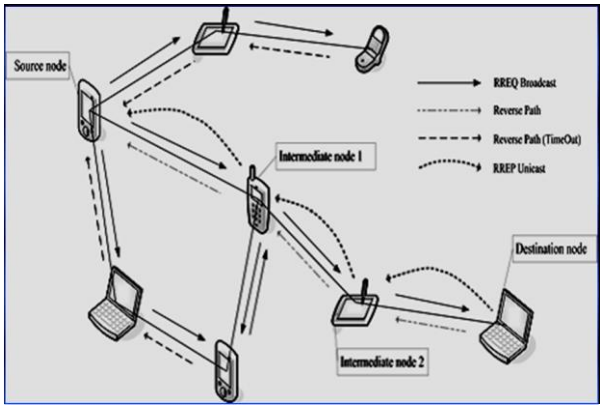


Fig-1. Route discovery process in AODV

C. Route Maintenance in AODV

It is performed with two additional messages HELLO and RERR messages. Each node broadcast Hello messages periodically to inform neighbors about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. When a node does not receive HELLO message within time period from a neighbor node then it detects that a link to that neighbor node has broken then it generates route error message (RERR). RERR message indicates those destinations that are unreachable, their IP address and destination sequence number. In order to inform the link failure information, each node maintains a precursor list for each routing table entry containing the IP address of set of neighboring nodes that are likely to use it as a next hop towards each destination. On receiving this RERR, each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link.

D. VULNERABLE FEATURES OF AODV

AODV routing protocol does not provide any security mechanisms to guard against attack. The routing messages RREQ, RREP and RERR can be easily attacked may be for impersonation or for tampering the message. There are two types of fields present in the routing information mutable field like hop count and non mutable fields like sequence number and IP address. The attacker concentrates on these fields for impersonation attacker gets non mutable fields and for tampering the message

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

attacker attacks on mutable fields. AODV should be guarded against end to end attack as well as from the attacks on intermediate nodes [5].

III. PROPOSED SYSTEM

In the proposed system digital signature is used to have end to end confidentiality for the packet and also to provide integrity to the message. To safe guard the routing information of the AODV in intermediate nodes one way hash verification is used, here the variant of hash function MD-5 is used. It is using the symmetric cryptography as it takes little time as it is having little computation when compared to asymmetric cryptography.

In the proposed system when source node generates RREQ it contains the extra field message authentication code generated for original RREQ (MAC), for non mutable fields and one way hash chain using MD-5 (h) for mutable fields and node list. At each node integrity of the RREQ and hop count is verified.

In RREP of the proposed system contains the fields like authentication code generated for original RREP (MAC), one way hash chain using MD-5 (h) and node list. At each node integrity of the RREP and hop count is verified.

In case of route failure RERR is generated to notify the originator. Simply hop count value or sequence number is set to infinity indicating that node cannot be reached and this information is passed to near by node as well as to the originator so that it can construct new route to the destination.

IV. RESULT ANALYS

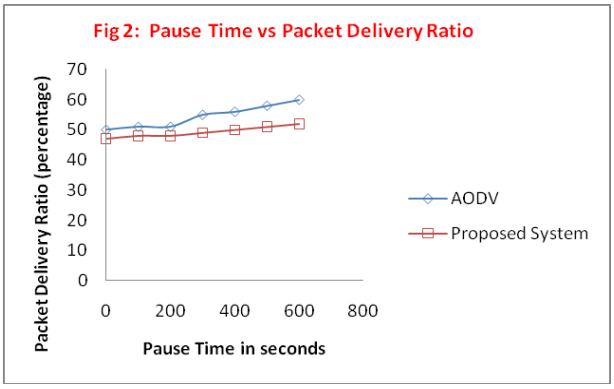
The simulation tool NS-2 is used for performance analysis the following metrics are assumed.

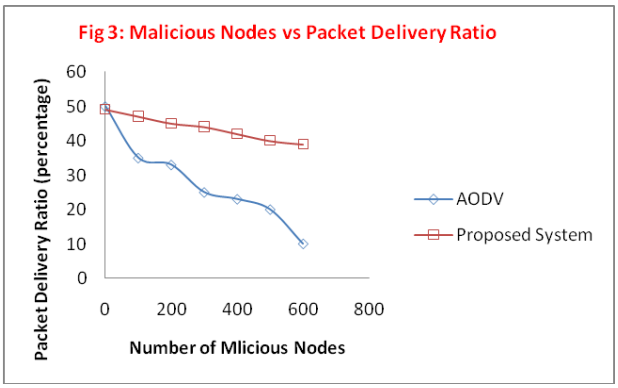
Table 1: Simulation Metrics

Simulation Parameters	Value
Simulator	NS-2
Simulation Time	600 sec
Number of nodes	50
Area Size	1000m * 1000m
Transmission Range	250m
Maximum Speed	0-20 m/s
Maximum Number of Connections	20
Application Traffic	Constant Bit Rate (CBR)
Packet Size	512 bytes
Traffic Rate	4 packets/sec
Node Mobility Model	Random Way-point Model

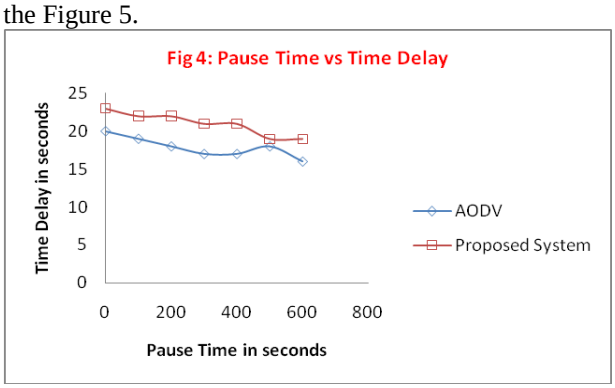
A. Packet Delivery Ratio: Packet Delivery Ratio = Total Packets Received / Total Packets Sent.

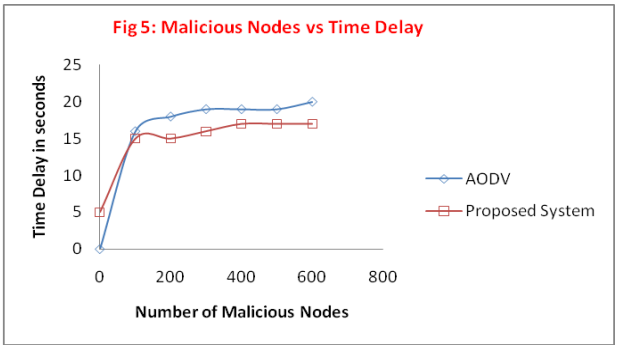
It is good for AODV when compared to the proposed system, but in the presence of malicious nodes AODV performance decreases as seen in the Figure 2 and Figure 3. Proposed system uses symmetric cryptography to secure the packets. In the presence of mobility nodes without malicious nodes AODV performs better than the proposed system but with increase of mobility and in the presence of malicious nodes it becomes tough job for AODV to construct routes thus packet delivery ratio decreases.





B. Time Delay Time delay of data packet is the difference between the time when the first data packet is received by the destination node and the time when the source node broadcasts a RREQ message. It is good for AODV when compared to the proposed system (Figure 4), but in the presence of malicious nodes AODV performance decreases i.e Time delay is more is seen in the Figure 5.



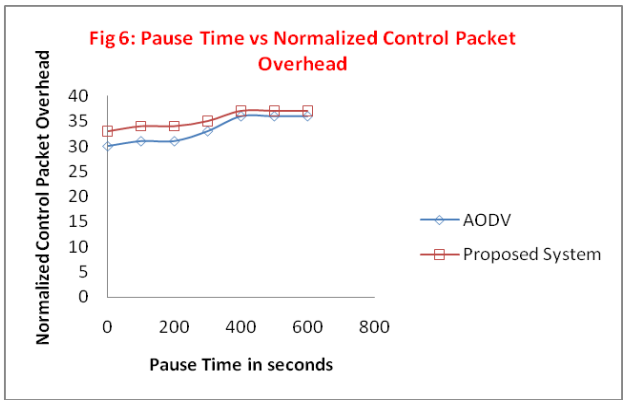


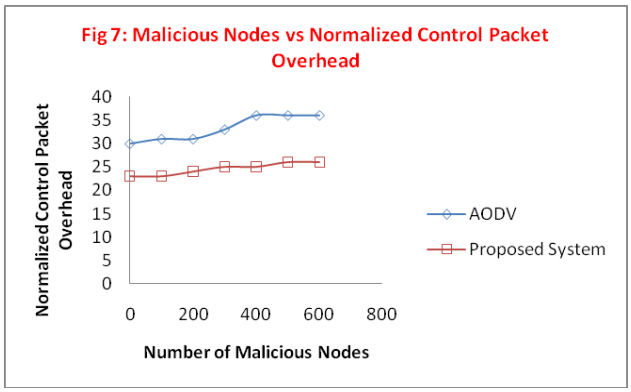
ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

C. Normalized Control Packet Overhead

Normalized Control Packet Overhead = (Routing Packets Sent * Size of Routing Packet) / (Received Data Packets * Size of Data Packet). The overhead is less for AODV when compared to the proposed system (Figure 6), but in the presence of malicious nodes AODV over head increases as seen in the Figure 7.





V. CONCLUSION AND FUTURE WORK

In this paper the MANET features are briefed and briefly explained the mechanism of routing process of AODV and then pointed out the vulnerabilities of AODV. This paper given a solution using the digital signature MAC and the one way hash function (MD-5) to guard against the attacks launched against the routing information (RREQ and RREP). Still there are areas of security which need to be explored in deep in case of routing and packet forwarding and delivery.

REFERENCES:

[1] Jane Zhen and Sampalli Srinivas, "Preventing Replay Attacks for Secure Routing in Ad HocNetworks", Dalhousie University, Halifax, NS, Canada, Springer-Verlag Berlin Heidelberg 2003, ADHOC-NOW 2003, LNCS 2865, pp. 140–150, 2003.

[2] C. E. Perkin, E. M. Royer, "Ad-hoc on demand distance vector(AODV)routing," The Second IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999.

[3] Perkins, C., Belding-Royer, E., Das, S.: Ad-hoc on-demand distance vector (aodv) routing, rfc-3561, network working group (July 2003).

[4] Perkins, C.E., Royer, E.M.: Ad hoc on-demand distance vector (aodv) routing. In: Proceeding of IEEE Workshop on Mobile Computing system and applications. pp. 90-100 (February 1999).

[5] Yih-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security & Privacy, vol. 2, no. 3, pp. 28-39, May-June, 2004