ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY PROVIDED TO MOBILE AD-HOC NETWORKUSING RSA – ASYMMETRIC KEY CRYPTOGRAPHY

Miss .Rashmi P. Shinde*, Mr. Sanjay S. Pawar
BhartiVidyapeeth's College Of Engineering Kolhapur, Maharashtra, India

ABSTRACT

Mobile ad hoc network (MANET) is a dynamic network consists of mobile devices connected together by wireless Network. Most of the time, the nodes in MANET are mobile and can request to connect or leave the network. As a result, the pathwill frequently change.The AODV is very wellknown protocol for MANNETFor most existing routing protocols of mobile ad hoc network (MANET), more efficient security mechanisms against the attacks from malicious nodes, authentication of nodes should be provided. Cryptographic algorithms can be used to provide security in MANNET.

KEYWORDS: MANET, RSA algorithm, Security..

INTRODUCTION

MANET has various type of routing protocols and normally they are classified into proactive and reactive type of protocols. AODV- Ad hoc on demand distance vector protocol is an example of reactive routing protocol for ad hoc network available today. Thus, no protection mechanism was built to detect the existence of malicious attack.. The one of the well known attack which is the most common attacks for AODV routing protocol where malicious node will pretend to have the shortest and freshest route to destination by constructing false node number in routing control messages. Once the network has been compromised, a attacker can perform various attacks such as eavesdropping, spoofing, control packet modification and denial of service[1][2].

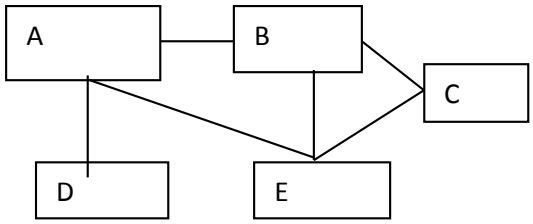

Fig 1. Mobile Ad-hoc Network

PROTOCOL USED FOR MANET

The term AODV- Ad hoc on demand distance vector routing protocol is derived from the basic protocol which is Destination-Sequenced Distance Vector (DSDV) routing protocol for wireless Ad hoc networks. It is a reactive type table oriented type of routing protocol in which the path is specified in routing table. That is, when each node has some packets to send, it first checks its routing table to find a valid and active path to the particular destination. If there was not any path, then it initiates path by sending a route request (RREQ) packet to its all-next neighbors. When an in between node receives a RREQ packet, if it is the destination of the packet, it sends back a route reply packet (RREP) to the source node through the reverse path. Otherwise, it looks up in its routing table to find any entry that matches to the destination. In case that an entry is found, it checks the freshness of the route by comparing destination sequence number in its routing table to the same one in the RREQ packet. If the sequence number in the routing table is greater than or equal to the sequence number of the packet, it sends back a RREP. The node rebroadcasts the RREQ to its neighbors [2][4][6] .

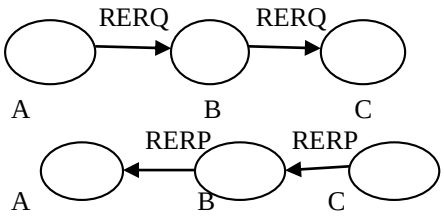

Fig 2.Route request Route Reply

ATTACKS IN AODV

Routing attacks in Ad Hoc networks are classified into two types passive and active attack. In a passive attack, the operation of a routing protocol is not been disturbed by the third party attacker but only

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

eavesdrops on the network.. In an active attack, the attacker must be able to inject some packets into the network. Active attack is harmful to AODV. Some types of active attacks, includes black hole attack, malicious node attack, denial of service.

SECURITY PROVIDED IN AODV

RSA algorithm can be used to provide security in AODV protocol.RSA algorithm is most popular asymmetric cryptographic algorithm. In RSA algorithm we can easily find and multiply large prime numbers together, but it is difficult to factor their product .Private key and Public key in RSA very large prime numbers are used which increases the complexity of the algorithm .The security provided can be seen in following frame formats.

Destination IP address
Originator IP Address
Timestamp
Digital Signature (Public Key)
Digital Signature (Private Key)

Fig3..Route Discovery message format

Destination IP address
Originator IP Address
Timestamp
Digital Signature (Public Key)
Digital Signature (Private Key)

Fig4.Route Reply message format.

ENCRYPTION AND DECRYPTION USING RSA ALGORITHM

1.Choose two large prime numbers R and S
2.Calculate N= R×S
3.Select the public key Q such that it is not a factor of (R-1) and (S-1).
4.Select the private key P which follows' following equation
(P× Q)mod (R-1) and (S-1) =1
5.For encryption, calculate the cipher text CT from plain text PT as:
$CT=PT^{Q}$ modN
6.Send CT as the cipher text to the receiver
7. For Decryption calculate the plain text PT from the cipher text CT as:
$PT=CT^{P}$[8].
Thus we can say that the RSA is useful algorithm in to obtain the security aware AODV protocol. This algorithm uses both the keys i.e. public key as well as the private key.

CONCLUSION

In this paper, we suggest a security to the AODV protocol by using asymmetric cryptography i.e RSA, to provide reliable efficient data transfer from source to destination. Here we are implementing the AODV-Ad hoc on demand distance Vector protocol by providing the security using RSA algorithm. The AODV network protocol comes in picture at the time of sending data packets. To prevent the data loss we have implemented the security using RSA algorithm. The encryption of message & decryption of message and reception of key(sent and received) are used for the security in AODV protocol. The Ad hoc on demand vector routing protocol uses the RSA algorithm for the encryption of the message to be sent. Thus we can make data secure with the use of RSA algorithm.The safe data transmission is possible in AODV using RSA.

REFERENCES

1. *Securing Routing Table Update in AODV Routing Protocol.BykamarularifinAbdJalil, Zaid Ahmad Jamalul- LailAb Manan2011 IEEE Conferece on Open systems (ICOS2011),SEPTEMBER 25-28,2011,Langkawi,Malasia[1]*
2. *SecureAODV against Maliciously Packet Dropping by Mohammad TaqiSoleimani. AbdorasoulGhasemi[2]*
3. *Privacy-Preserving Location-Based On-Demand Routing in MANETs Karim El Defrawy, Member, and Gene Tsudik, IEEE Journalon Selectedareas incommunications, VOL. 29, NO. 10, December 2011[3]*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

4. *An Efficient Secure AODV Routing Protocol in MANET by DurgeshWadbude, VineetRichariyaInternational Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012 274 [4]*
5. *Trust Based Secure AODV in MANET Pankaj Sharma,, Yogendra Kumar Jain[5]*
6. *Cryptography and Network Security by AtulKahate.[8]*
7. *A Survey paper on Secure AODV protocol in MANAET using RSA algorithm and Diffie-hellman algorithm by[9]*
8. *Prasad P. Lokulwar , Prof. YogadharPandey[10]*