ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure AODV Routing Protocol Using Digital Signature

K.Ramya Madhavi
M.Tech Student,
Department of Computer Science and Engineering,
M.V.S.R Engineering College,
Nadergul Telangana, India .

Sesham Anand, MS
Associate Professor,
Department of Computer Science and Engineering,
M.V.S.R Engineering College,
Nadergul Telangana, India .

Abstract:

Ad Hoc On-Demand Vector Routing (AODV) protocol is a reactive routing protocol for ad hoc and a mobile network that maintains routes only between nodes which need to communicate. In MANET, attacks can be broadly classified in two categories: routing attacks and data forwarding attacks. Any action not following rules of routing protocols belongs to routing attacks. The main objective of routing attacks to mislead or disrupt normal functioning of network by advertising false routing updates. On the other hand data forwarding attacks include actions such as modification or dropping of data packet that does not disrupt routing protocol. The routing messages do not contain information about the whole route path, but only about the source and the destination. The data message contains the message which can be attacked like denial of attack etc. Authorization may require other security services such as authentication and integrity. Techniques like digital signatures are used to provide these services.

Keywords: AODV, non- mutable, routing attack, authentication and integrity, DSA.

1.INTRODUCTION:

Ad-hoc network is a network formed by the group of nodes communicating with each other without any fixed infrastructural elements. The connection establishes only for the purpose of communication between the nodes in a specific range. Here each node will serve as a router which supports the communication protocols without any centralized controlling system and called as self organized also. Apart from the above characteristics the ad-hoc network is adaptive in nature. It can take different forms and has highly variable mobile characteristics such as power and transmission conditions, traffic distribution variations, and load balancing.

Ad-hoc network is having the wide range of protocols for supporting the motion based communication with dependencies of mobile devices. Thus the requirements must be satisfied in lightweight medium. Fundamentally the routing protocol delivers the messages from source to destination with enhanced performance in terms of delay and security. The functionality of routing protocol is to discover network topology along with the route formation for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes [1]. The routing protocol is mainly classified into three categories based on their functionality: Reactive (On Demand), Proactive (Table Driven) and Hybrid. The security attacks in mobile ad hoc network fall into two categories: passive attacks and active attacks. In passive attack, malicious node does not affect the normal operation of data so it is very difficult to detect. It includes traffic analysis, monitoring and eavesdropping. Encryption algorithms are used to prevent passive attacks. In active attack, malicious node disrupts the normal functioning of system by performing either external attacks or internal attacks. External attacks are from malicious nodes that do not belong to network. External attacks can be prevented by using cryptography techniques such as encryption. Internal attacks are from either compromised or hijacked nodes which attempt to disrupt the normal routing function in order to consume the network resources. Internal attacks include modification, impersonation, jamming, sleep deprivation and denial of service attacks which are very difficult to prevent. We need to address these five major security services in order to prevent the security attacks: Availability, Confidentiality, Authentication, Integrity and Non-repudiation [4]. However ad hoc network routing protocols do not need confidentiality as intermediate nodes process routing messages before forwarding in the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The security mechanism based on cryptography is useful for preventing external attacks. It cannot prevent the internal attacks if it is from compromised or hijacked nodes as adversary can get secret information such as private keys of other nodes. We need intrusion detection system to prevent such type of attacks. Moreover security mechanism based on asymmetric key cryptography is not efficient. The asymmetric key algorithm is very slow and consumes more CPU processing power and battery power which is not feasible as nodes in MANET is resource constrained[2].

2.RELATED WORK:

The researches have studied about the prevention of attacks on routing protocols. All attacks may not be prevented but major issues can be resolved. Many researchers have surveyed on security attacks and their solutions are given below: The author's Anil Suryavanshi and Dr. Poonam Sinha [6] suggested a solution as an extension to AODV called Secure AODV (SAODV). Mainly the security in MANET is served here using IPSec which was discussed earlier. The work assures that the IPSec implementation can use as a selector the TCP and UDP port numbers. Network communication contains two types of packets data and control. Thus the security mechanism must allow the control packet directly without change and the data packet is verified using cryptographic primitives. Y.C. Hu, A. Perrig, and D. B. Johnson [7] proposed a secure routing protocol Ariadne. Ariadne protocol uses message authentication code (MAC) to maintain the message integrity and digital signature for authentication. In Ariadne protocol, the source node generates the route request (RREQ) message and appends a hash value to RREQ message. Each intermediate node appends its identifier, digital signature and per hops value. When destination node receives RREQ packet it verifies source node and intermediate nodes, then sends back RREP message.

3.PROPOSED SCHEME:

AODV routing protocol requires at least two security services: Data origin authentication at each receiving node and routing message integrity. Message integrity is of the most concern in AODV routing. A malicious node may change sequence number or hop count fields in RREQ /RREP messages or impersonate the sender of routing packets.

Modification of routing information may lead to inconsistency in network. Routing table may contain false information about network topology. Change in sequence number may result in routing loops etc [2]. In AODV protocol, routing messages RREQ or RREP have two types of information: Mutable and Non Mutable. The hop count is only mutable field as intermediate nodes increment the hop count field while forwarding the RREQ. The rest fields such as sequence number or IP address are non mutable fields as they remain unchanged. Digital signature with public key used to secure AODV messages. This mechanism calculates signature using appropriate algorithm for all the fields of an AODV message. It also calculates signature with public key and then both signatures will be transmitted along with the AODV messages. The following process generates the signature using DSA and forwards the packet:

1)Initialize the reagents
2)Generate the prime number
3)Using RSA algorithm generate the keys
4)Generate the signature using DSA.
5)Signature is attached to the data. (The signature of the message M will be a pair of the numbers r and s which will be computed from the following equations.
$r = (g^k \bmod p) \bmod q$
$s = (k\text{-}1(SHA(M) + xr)) \bmod q$
k-1 is the multiplicative inverse of k (mod q). The value of SHA(M) is a 160-bit string which is converted into an integer according to the SHS standard.)
6)While receiving the data verify the signature. (If both of the conditions are satisfied then we will compute
$w = (s')\text{-}1 \bmod q$
$u1 = ((SHA(M'))w) \bmod q$
$u2 = ((r')w) \bmod q$
$v = (((g)u1\ (y)u2) \bmod p) \bmod q$
Then if $v = r'$ then the signature is valid and if not then it can be assumed that the data may have been changed or the message was sent by an impostor.)
7)If signature matches then forward the packet. Else consider it as malicious node and re route the node. These processes continuous till all the nodes are verified and generate the authenticated node communication.

4.SIMULATION AND RESULTS:

All simulation experiments are developed and simulated on an Intel(R) Core 2 Duo 1.83GHz machine using Ubuntu 12.4.0 with 2 GB RAM and the network simulator NS2 version NS-2.34.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

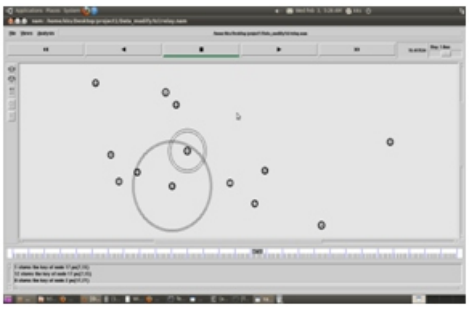

Figure 3.1 Node Verification

In figure 3.1 shows the nam output of verification i.e., identifying the authenticated nodes.

Calculating Performance Metrics:

1.Packet Delivery Ratio:

Packet Delivery Ratio = Total Packets Received / Total Packets Sent. The ratio of the number of data packets successfully delivered to the destinations to those generated by CBR sources

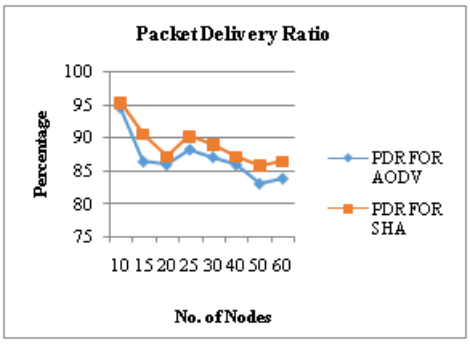

Figure 3.2 Packet delivery ratios

In figure 3.2 shows packet delivery ratio. The packets may travel through malicious node in AODV. Hence the delivery ratio of DSA is better than that of AODV. The packet delivery ratio of DSA is 3% higher than that of AODV.

2.Packet Loss:

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion.

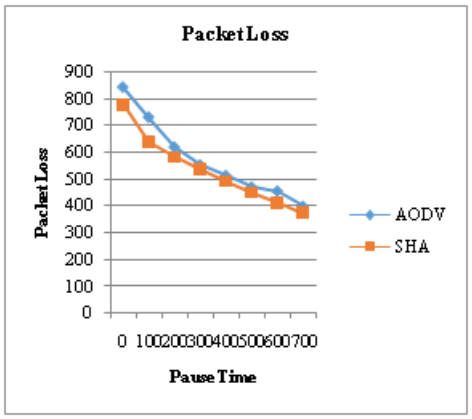

Figure 3.3 Packet Loss

In figure 3.3 shows Packet Loss decreases as the pause time increases. The loss of packets decreases by 0.4% in DSA when compared to AODV.

5.CONCLUSIONS:

Mainly the security here deals with the authentication and confidentiality of the data packets. The packets information here is encoded after separating them into categories or mutable information contained in them. Authentication is performed using DSA. Normally the approach verifies the non mutable information with the unique signature associated with the packet. Encryption is performed with the RSA based public key cryptosystem. Thus the approach authenticates a sender and all the intermediate nodes in a multicast environment of mobile ad hoc network with a low computation overhead. The protocol assumes each node has pre-distributed secret key.

REFERENCES:

1.Sanket Nesargi and Ravi Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network", IEEE Transaction, ISSN:07803-7476-2/02,v2002

2.Preeti Sachan and Pabitra Mohan Khilar "Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

3.Ms Darshana Patel , Ms Vandana Verma "Security Enhancement of AODV Protocol for Mobile Ad hoc Network" International Journal of Application or Innovation in Engineering & Management Volume 2, Issue 1, January 2013

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4.Dr. Indumathi .J1 , Anish A2 "Secure Data Transmission through Trusted Node in Mantes using AODV Routing Algorithm: SATEM" International Conference on Cryptography and Security 2014(ICCS 2014)

5.Jagrati Nagdiya and Shweta Yadav, "Secure Autoconfiguration in Mobile Ad hoc Networks using Rabin cryptosystem", IJETAE, ISSN 2250-2459, Volume 4, Issue 4, April 2014

6.Anil Suryavanshi and Dr. Poonam Sinha, "Efficient Techniques for SAODV in Mobile Ad-Hoc Network", Journal of Global Research in Computer Science, Volume 2, No. 8, August 2011.

7.Y.C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure Ondemand Routing Protocol for Ad hoc Networks", Proceeding of 8th Annual International Conference on Mobile Computing and Networking.