Performance and Security Enhancement of AODV Protocol under Black Hole Attack

Mrs. Chandrika C N
Asst.prof Dept of CSE
SVIT, Bangalore
Email:chandikacn@gmail.com

Adarsh D V
4th sem M.tech Dept of CSE
SVIT, Bangalore
Email:adarshadhunti@gmail.com

Abstract:-As in the convention of the wireless there are two types of wireless networks namely with base station (cell phone technology) and adhoc networks without base station. As adhoc networks play an important role in military based applications as centralized base station cannot be placed. So, the adhoc networks came into existence.

As in the conventional adhoc networks the routing protocols are AODV. The AODV is based on IEEE802.11 the AODV uses destination based routing. As AODV cannot withstand blackhole attack. So the SAODV came into existence. In this paper we will present multihop adhoc networks and then the security for AODV is discussed.

Keywords: *AD-HOC networks, AODV, SAODV, BLACKHOLE ATTACK*

*****

I. Introduction:

A multihop adhoc network is a decentralized wireless network where each node acts as transreciever (transmitter and receiver) and each individual nodes are responsible for route establishment[1][2]. Research on multi hop adhoc networks has evolved rapidly and profoundly during the past decades. By far the majority of the research experiments has been using simulators only, namely ns2, Glomosim …..etc[4].

AS in the multihop adhoc networks there are two types of routing protocols are present namely proactive and reactive protocols[3][5].

Proactive protocol: Traditional distributed shortest-path protocols, based on periodic updates. It has high routing overhead and also prevents an attacker from launching attacks through various cryptographic schemes. Even if there is no data to send but the nodes will be keep updating it's routing table. So, the wastage of memory and even in a small change in the network all the nodes should update the routing table. The unusual message transfer for updating the routing table is present in the proactive protocols EX: OLSR, TBRPF

Reactive Protocol: Seeks to detect security threats and react accordingly. Discover routes when needed. Source-initiated route discovery, because of this we go for reactive protocol. Whenever there is a data to be sent then only the source requests for the route and only necessary nodes will update the routing table. since there is less message transfer so the memory and frequent update of routing information is less. EX: AODV, DSDV, DSR.

The mechanism for MANET, must require low computational complexity and small number of appended messages to save the node energy.

it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones.

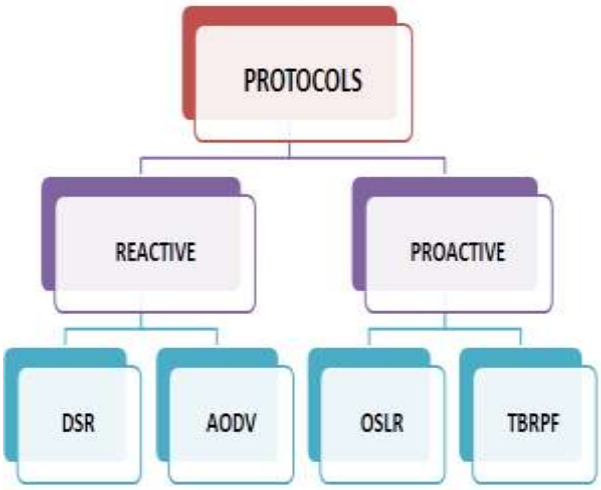

Fig 1 types of protocols in NS2

II. Existing System:

The AODV Routing protocol is an on-demand reactive protocol. that is,whenever the source wants to send the data then only the route establishment phase takes place. The sequence numbers are used in AODV to identify the last used route. In AODV protocol, the intermediate nodes and the source node stores the next-hop's information.

In reactive routing protocol, the source node broadcasts the RREQ packet in the network whenever a route is not available for the destination.

If the RREQ packet reaches the destination it prepares RREP packet as AODV uses reverse path forwarding technique. If RREQ reaches intermediate nodes it simply again broadcasts the RREQ to its neighbours. The intermediate nodes looks for the sequence numbers in RREQ packet. The duplicate RREQ packet is dropped in AODV. AODV's RREQ packet broadcasts in tree manner and does not form a cycle.

A timer is placed in source in case if the RREP is late to ensure qos and then the RREP is discarded if it arrives after the clock expires.

Fig 2 RREQ message in AODV

Fig 3 RREP message in AODV

The main disadvantage of this existing system is black hole attack.The working of the blackhole attack is whenever the source wants to send the data, the source broadcasts the RREQ at the same time the attacker sends RREP as pretending as destination. So the data transmission will takes place as depicted in the below figure.

Fig 4 RREP message produced by Attacker

III. Proposed System:

In order to protect from the blackhole attack two datastructures are added to the AODV and this routing protocol is called SAODV.

SAODV (Secure AODV) uses two Mechanisms

Digital Signature:- the digital signatures are used to maintain the identity of a particular user. i.e., no two users have the have digital signatures.

It is used to protect the integrity of the non-modifiable data in RREQ/RREP messages.Such as SourceIp, DestinationIP, FLAGS.

Hash Chain:-It is used to Authenticate the hop count of RREQ/RREP messages. This technique is used to authenticate each and every hop.

Steps for generating Hash Chain:

1. Generates a random number (seed).
2. Sets the Hopcount_Limit field to the TimeToLive (TTL) value.
3. Sets the Hash field to the seed value.
4. Sets the Hash Function field to the identifier of the hash function that it is going to use.
5. Calculates Top Hash by hashing seed Hopcount_Limit times.

IV. Implementation:

In this section we will briefly discuss about how to implement the black hole patch for the AODV and the implementation of SAODV.

Blackhole Implementation:

As in this blackhole first we need to add an agent for the attack in the sendReply function that exists in the AODV.CC and we need to create an keyword for the attacker and and in this function whenever an route request occurs it should cache it and it needs to send route reply as if it is destination.

And in the tcl script we need to call it by that keyword and also we need to specify the the time at which it needs to start its function.

SAODV Implementation:

The SAODV needs minor changes in the AODV protocol. First step is to add the data structure to the RREQ and RREP message. The data structures added to the protocol are digital signature, hop count and hash value in the packet.cc file. Second step is to add a random function(built in function in Ubuntu as rand as keyword). Third step is to add the digital signature by adding 5 to the index in the sendRequest.

Digital_signature=index+5;

Fouth step is to compute the hash value to thethe hop count using the hash value algorithm.Add these values to the generating the generated RREQ packet

Fifth step is to make changes in the recvRequest. The received message is taken and the digital signature, hash value is calculated and it is verified in each and every hop.

Sixth step the necessary data structure such as digital signature, hopcount and hash value is added to the RREP packet. These data structures are added in the sendReply function that exists in AODV.CC file.

Seventh step is to verify the digital signature and hash value that is recived by sendReply function compared with recvReply.

If all the parameters such as digital signature and hash values are verified in all the necessary nodes then the source sends the data otherwise it drops the data packets..

V. Simulation:

All simulation experiments are developed and simulated on an Intel I3 machine using Ubuntu 12.04 LTS with 4 GB RAM and the network simulator NS2 version NS- 2.35.

In order to measure Packet Delivery Ratio and Routing Load, it is necessary to calculate total number of sent, received and forwarded AODV packets.

VI. Performance Metrics:

Packet Delivery Ratio:

It is the ratio of packets delivered to that generated by the traffic generator. It is given by received packets/sent packets. The packet delivery ratio is directly influenced by packet loss, which may be caused by general network faults or uncooperative behavior.

Routing Load:

It is the number of routing packets required to be sent per data packet delivered. It is given by routing packets/received packets.

Throughput:

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations.

Average End to End Delay:

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination.

VII. Conclusion:

This scheme fulfills almost all security requirements with using central certification authority and key management scheme which makes it more easily expandable and less complex in computation. According to the simulations that were performed in NS2, the newly proposed security scheme, built on top of normal AODV routing protocol, achieves an overall good results. Thus, the proposed scheme proves to be more efficient securing AODV routing protocol in defending against both malicious and unauthenticated nodes.

References:

[1] Pirzada, McDonald, “Secure Routing with the AODV Protocol”, 2005 IEEE pp.57-61

[2] Stephan Eichler and Christian Roman, “Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC”, Aug 2006.

[3] Lu Jin, Zhongwei Zhang, Hong Zhou, “Performance Comparison of the AODV, SAODV and FLSL Routing Protocols in Mobile Adhoc Networks”, 2007

[4] Alaa S. Dalghan, Mohamad M. Gamloush, Raji M. Zeitouny, and Yasser M. Shaer, “Securing Mobile Adhoc Networks”

[5] Yih-Chun Hu, “A Survey of Secure Wireless Adhoc SRouting”, IEEE, 2004