Security Improved Ad-Hoc on Demand Distance Vector Routing Protocol (SIm AODV)

Mr. B.Karthikeyan[1*], Dr. S.Hari Ganesh[2], Mrs. N.Kanimozhi[3]

[1]Assistant Professor in Dept. of Computer Application, Bishop Heber College, Tiruchirapalli, 620017, TamilNadu, India.
[2]Assistant Professor, H.H. The Rajah's College, Madurai Road, Pudukkottai 622 001, TamilNadu, India.
[3]Lecturer in Department of Computer Science, Shrimati Indira Gandhi College, Tiruchirapalli, 620002, TamilNadu, India.
bkarthikeyanms@yahoo.com,bkarthikeyanphd@gmail.com, hariganesh17@hotmail.com,

Abstract

One of the most wanted wireless networks is Mobile Ad hoc Network (MANET). MANET can configure easily without using any facility which one is available at present as an infrastructure oriented wired or wireless network. It is one of the infrastructures less network consist of mobile devices. Individually each and every device in the Mobile ad hoc network will act as a router as well as node which provide the flexibility in the physical topology, optimal routing and data communication.

In this paper, A Security improved AODV (SIm AODV) routing protocol is proposed for Ad-hoc networks which typically suits to resolve the security issues like Link Failure, Black Hole Attack, and Malicious Node Intrusion Attack. The proposed SIm AODV algorithm is incorporated and evaluate with OMNetpp 4.3 simulation.

Keywords: OMNetpp 4.3; AODV; SIm AODV; MANET;

INTRODUCTION

Mobile Ad-hoc Networks (MANET's), nodes are moving in the network don't have any precise infrastructure and they are connected dynamically in a temporary arbitrary way.

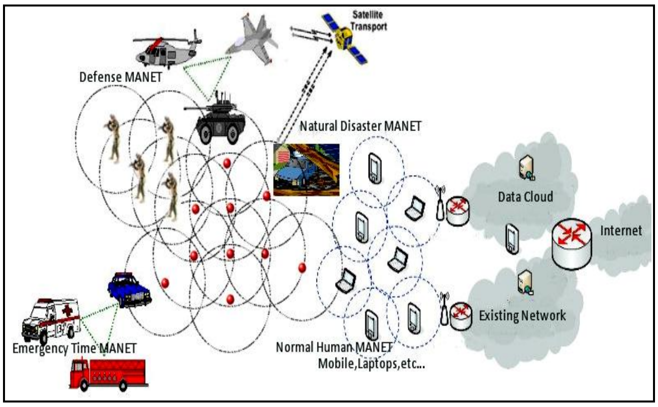

Fig.1. Mobile Ad-Hoc Network (MANET)

Nodes within each other's radio ranges communicate directly throw radio communication links, suppose the destination is in outside of radio rage the node has to enlist its neighbour nodes and use neighbour nodes as intermediate in between hops. Each and every node in the MANET will act as node as well as router. It will discover, maintain, and terminate the optimal route. Mobile device in mobile ad-hoc network travel dynamically; consequently keeping track of the network topology is a difficult task to achieve communication. The fig.1 shows the MANET. MANET has the lot of challenges so that network needs some standardized way (routing protocol) to make a communication between two mobile nodes with more security and less time.

1.1. Security in MANET Routing

Security in MANET is a major problem as to provide secure communication between the nodes in the infrastructure less wireless network. As ad hoc network is self-configuring, open radio communication link between node to node, frequent changeable physical topology, and modified assets. Following qualities describes secure network:

1. Confidentiality – To keep the information secret from the unknown users. It maintains the information safe and secure from the attacks.
2. Integrity of Message – To keep the accuracy and consistency of the data during its transit from one node to another node. So, that the data is not restricted by the node.

3. Availability of Nodes –As in MANET for communication the nodes are required to be available all the time so that the information can be relayed over such path.
4. Authorization –it specify the permissions of the entity to take part in the communication over network.

AODV

According to the author's early survey AODV is a most widely used protocol and it is based on distance vector routing protocol that has been specially design for MANETs. AODV is an on demand protocol and reactive in nature as it finding the routes only when sender wants to send data to packet receiver. AODV makes use of known sequence numbers in control packets to avoid the problem of routing loops. When a node is wished to make a communication with its destination, it broadcasts a RREQ packet to all its neighbour nodes. Request ID is contained by each Route Request packet and it also has originator node and the destination node IP addresses and sequence numbers along with a hop count and flags field in its packet format.

The Request ID fields uniquely recognize the RREQ packet; freshness retains by the sequence numbers. The number of intermediate nodes between the source and the destination maintains by the hop count. Receiver node of the RREQ packet that has not find the Source IP and ID pair or doesn't maintain a fresher (larger sequence number) route to the destination again it broadcasts the same packet after incrementing the hop-count. When destination receives the RREQ packet, it generate packet Route Reply called as a RREP packet and sent back to the originator node. RREP packet contains the destination node sequence number, IP address of the originator and the receiving node, hop count along with a route lifetime and flags. RREP packet received by intermediate node, increments the hop count field and it establishes a Forward Route to the source of the packet and transmits the packet on the Reverse Route. When a link break is detected for a next hop of an active route a RERR (Route Error) message is sent to its active neighbors that were using that particular route.

1.2. Issues in AODV

Black hole Attack, Intrusion Detection, Link failure problem, Malicious node attack, Cosmic Dust Attack, Intelligence Pulse Jamming Attack (IPJA), Performance and Throughput, Drop Ratio of Packets, Detecting Good Neighbors, Power-Hop, Link-timeout, Energy-aware mechanism, Path breakages, Large Scale and Fast Changing Topology, Local Route Maintenance, Multipath Contribution.

LITERATURE SURVEY

Naincy Juneja, *et al* (2014) [5] - This paper proposes the TID security policy over the AODV MANET routing protocol. The TID security policy performs its intrusion detection mechanism locally in the previous node of the attacker node in contrast with the RID security policy, which performs its intrusion detection mechanism by means of the route node.

Neeraj Saini, *et al* (2014) [6]- The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. This protocol uses the concept of Core.

Rajdeep S. *et al* (2014)[7] - This work is used hash chain mechanism to protect the increment, decrement and forward of equal HOP_COUNT value which is mutable field in control packet. We have used hash scheme followed by digital signature verification to protect the non-mutable information in control packet.

Shabnam, *et al* (2014)[8] - The cosmic dust attack problem is one of the security attacks that occur in mobile ad hoc networks (MANETs). It shows two feasible solutions. The main is to find more than one route to the destination. Another is to exploit the packet sequence number included in any packet header.

Radha Krishna Bar *et al* [9]- Trust value is calculated depending upon the ability to forward packets and the RREQ forwarding capability of a node. To obtain this capability the number of packets received and the number of packet sent is counted. Two weight factor value W1 and value W2 are introduced. Value W1 is the ratio of number of packets sent from a node to the number of packets received to that node. A higher ratio value indicates that, the node has a excellent ability to forward the packets.

EARLY WORK ON AODV

According to First early survey [1] DSDV is most suitable for small networks where changes in the topology are limited. Also DSDV could be considered for delay considered for delay constraint networks. TORA is suitable for operation in large highly dynamic mobile network environment with dense population of nodes. The main advantage of TORA is its support for multiple routes and multicasting. Thus TORA often serve as the underlying protocol for light weight adaptive multicast algorithms. DSR is suitable for networks in which the mobiles move at moderate speed. It had lowest control overhead in terms of number of control packets. This is suitable for bandwidth and power constraint network. AODV is moderate protocol for all networks.

Second early work [2] the AODV routing protocol has been analyzed. As an AODV protocol transmits network details only on-demand. The route maintenance is a limited proactive part. The AODV protocol is loop-free and avoids the counting to infinity problem by the use of sequence numbers. This protocol offers fast adaptation to mobile networks with low processing and low bandwidth utilization. The limitation of AODV includes its latency and scalability.

Third early work [3] the security issues of AODV and analyze its functionality and performance measurements, and various existing security techniques were surveyed so that to come up with new algorithm to integrate with the basic AODV protocol. The evaluation with the AODV and Integrated new AODV protocols, it emphasize more on security. If the security is enhanced it delivers better.

Fourth early work [4] four different kind of customized algorithm is used to prevent the security threads. The Typical Intrusion Detection Security (TyIDSe) over AODV algorithm gives very good delivery ratio, when network has more node. But the time(End-to-End Delay) factor is not satisfied one. Block Hole Attack Detection(BHD) –AODV Algorithm gives very good delivery ratio, when network has more nodes. End-to-end delay gives poorest output. Sleep and Awake Mechanism(SAM)-AODV Algorithm gives moderate delivery ratio and it gives minimal end-to-end delay time when the network has more nodes. Local Neighbor Node Maintenance(L2NM) -AODV Algorithm gives average delivery ratio and it gives minimal end-to-end delay time when the network has more nodes.

In this paper the proposed (SIm AODV) single algorithm with AODV. It is used to avoid some security problem like Node Belief during Route Discover, Link Break, Cosmic Dust Attack, Black Hole Attack and Root Intrusion Detection.

PROPOSED WORK

The proposed Security improved AODV (SIm AODV) algorithm has the capable to reduce the security issues which one is available in the AODV routing protocol. The normal AODV protocol does not have any security measures. The existing Mobile ad-hoc network has the following issues:

Issue 1: The neighbor nodes may not believable, result is delay of *route discover*.

Issue 2: Out of radio range due to the nodes mobility, result is packet loss*. (Link Break)*

Issue 3: In MANET nodes are mobile. Because of it nodes distance (hop count) may change, result is packet loss. *(Cosmic Dust Attack)*

Issue 4: RREP from malicious node, result total data loss. *(Block Hole Attack)*

Issue 5: After RREP, Proceeding neighbor has to validate RRRP, result data packet loss *(Root Intrusion Detection)*

In this paper proposed Security improve AODV (SIm AODV) avoid the above Issues in the following way.

The Issue 1 is preventing by find, whether the node is believable or not. It is found by the use of how many packets is handled by the node. That is the ratio between total number of sent packet and total number of received packet. If ratio is near to 1, that node is believable node.

$$B = nsp/nrp \quad ....(1)$$

Where

nsp = Net Sent Packets (RREQ exclude its own packets).

nrp = Net Received Packets (RREP exclude its own packets).

```
if (B==1){
    Belief Node;
}
Else
{
        Not a Belief node;
}
```

Here nsp is the count of total packets which one is sent by the node not by the node's own purpose that is RREQ not originated by the node. The nrp is the count of total packets which is received as intermediate node. This ratio tells the transparency of the particular node. It should be between 1 and 0.8 then only a node, become as a belief node.

The Issue 2 is avoiding finding distance between node and its belief nodes. This is calculating by the use of counter (RC).

```
Create HNREQ;
Broadcast HNREQ; (Broadcast to all its neighbor, what all are the node within the radio boundary)
Start RC;
Loop: watch incoming packets
    if(HNREP received)
    {           Update L2T;
    }
LiNo [] =Find Minimum number in RC entry in L2T;
```

According to this proposed algorithm the node sends HNREQ to its neighbors, immediately it starts RC counter to calculate the time taken for HNREP from any one of its neighbor. Update Link on Time Table (L2T) for further communication. So the protocol SIm AODV make the further communication with only the node which one is available in the L2T. Updating L2T will be conduct periodically.

Issue 3 describe the nodes change its position due to this mobility, hop count may be changed (form 1 to 2). The packet transmit will be affected. Avoid this problem the proposed protocol make a list, who all are in the hop count one in periodic manner.

```
Loop: BNLT []
if (BNLT.Hop_Count==0)
            {       Add
information to OHNeNT     }
                Loop end: BNLT []
```

The route discovery mechanism according to the SIm AODV send its RREQ packets send to its neighbor who all are have Hop Count 1 and who is in the routing table. Change and choose will be done be done periodically.

During the Reverse Route the Issue - 4 & 5 will occur, for avoid the unauthorized malicious node's RREP the AODV protocol has the mechanism of *Route Intrusion Detection*. This is the technique done by the source node. This is the time-consuming mechanism. In the proposed algorithm route intrusion detection done by the node which one receives the RREP at first.

```
If ((CRREP.Orig_IP== RREP.Orig_IP) &&(CRREP.dest.IP==RREP.dest_IP))
    {
        if (Next node has route to both real destination and RREP transmitted
            node (assume attacker node))

  {  Discard CRREP & CRREQ Packets;
     Unicast RREP to Source node;
     }
     Else
     {      Discard both RREQ and RREP;
       Discard both CRREQ and CRREP;
          Broadcast alert message to all;
     }
```

1.3. Refershing Rate for all the Tables

According to the simulation model (Fig.2.) each and every mobile node has around 200 meters of radio transmission range. In this simulation each and every node moves around 10m/s its comes around 36kmph.

If the neighbor node comes in to the node's radio range between 400meters at maximum and 60meters at minimum. It comes around 40 seconds to 6 seconds. 40 seconds at maximum available time and 6 seconds at mimimum availabletime.

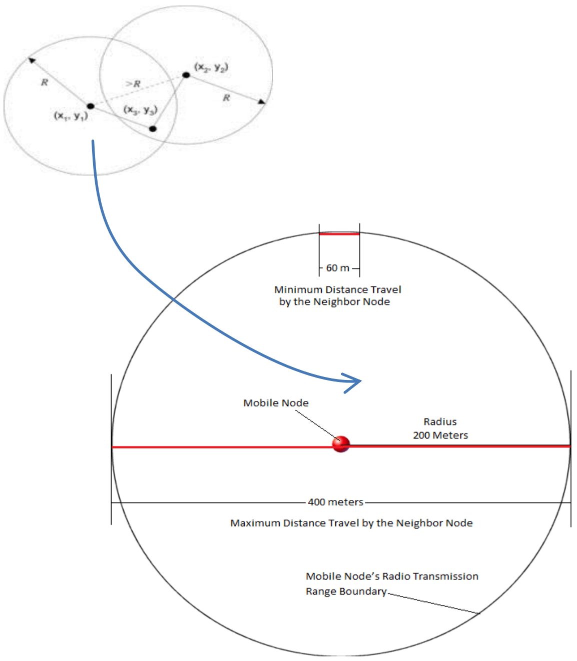
R
>R
(x1, y1)
(x2, y2)
(x3, y3)
R
60 m
Minimum Distance Travel by the Neighbor Node
Mobile Node
Radius 200 Meters
400 meters
Maximum Distance Travel by the Neighbor Node
Mobile Node's Radio Transmission Range Boundary

Fig 2. Radio Transmisssion Range of Each Mobile noade

- Table Refershing Time : 2sec once
- Node's Radio Transmission Range: 200 meters
- Mobile Node's Traveling Speed : 36 kmph (Kilo Meters Per Hour)
- Band Width: 2Mbps

IMPLEMENTATIONS OF AODV ROUTING PROTOCOL

There are many AODV routing protocol implementations AODVUCSB, AODV-UU, Kernel-AODV, and AODV-UIUC. Each implementation was developed and designed separately, but they all perform the similar operations. The first release of AODV-UCSB (University of California, Santa-Barbara) used the kernel alteration strategy. AODV-UU has the same design as AODV-UCSB. The main protocol logic is inside the user-space daemon; in addition, AODV- UU (Uppsala University) includes Internet gateway support. AODV-UU except it explicitly separates the routing and forwarding operation. Routing protocol logic takes place in the user-space daemon, while packet forwarding is handled by the kernel.

RESEARCH METHODOLOGY

In order to analyze the performance of the AODV routing protocols, with respect to the following metric: *Throughput or packet delivery ratio:* It is calculated by the numbers of packets sent out by the sender application and the number of packets correctly received by the corresponding peer application. *Average end-to-end delay:* This implies the delay a packet suffers between leaving the sender application and arriving at the receiver application.

SIMULATION

OMNeT++ is an object-oriented discrete event simulation environment. Its major use is in simulation of network communications. The developers of OMNeT++ predict that one might use it as well for simulation of compound IT systems, queuing networks or Hardware architectures, since OMNeT++ is built generic, flexible and modular. As the architecture is modular, the simulation kernel and models can be embedded easily into an application. C++ is the programming language used for the modules in OMNeT++. The Table 1 shows the simulation parameters.

Simulation Parameters

Table .1. Simulation Parameters

Parameters	Values
Network Size	600m X 600m
Number of Nodes	0-50
Max. Speed/Mobility	10.0ms/s
Pause Time	0-100s
Traffic Model	CBR
Routing Protocol	AODV UU with SIm AODV
Simulation Time	600s

RESULTS AND DISCUSSION

Table.2. Packet Delivery Ratio

No. of Nodes	Total Packets	AODV *(PPs)*	SIm AODV *(PPs)*
10	30	18	25
20	60	40	42
30	90	60	83
40	120	96	109
50	150	121	145

Compare to AODV, SIm AODV routing protocol gives more number of packet delivery. If the network has more number of nodes the packet delivery is almost 97%, it is listed in the above Table 2 and graph is plotted its show in the fig 3.

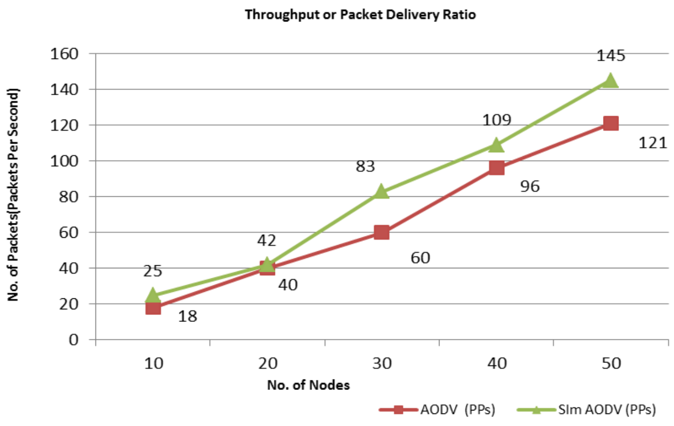

Fig. 3. Throughput vs. Number of Nodes

Table. 3.End to End Delay vs. Number of Nodes

No. of Nodes	AODV *(ms)*	SIm AODV *(ms)*
10	3.11	4.88
20	4	5
30	4.55	7.4
40	6.63	8.82
50	5.9	11

SIm AODV routing protocol took more time to deliver the packets compare to the Normal AODV Protocol. Because the proposed algorithm contains around five different algorithm to prevent packet loss. The end to end delay is listed in the table 3 and graph is shown in the figure 4.

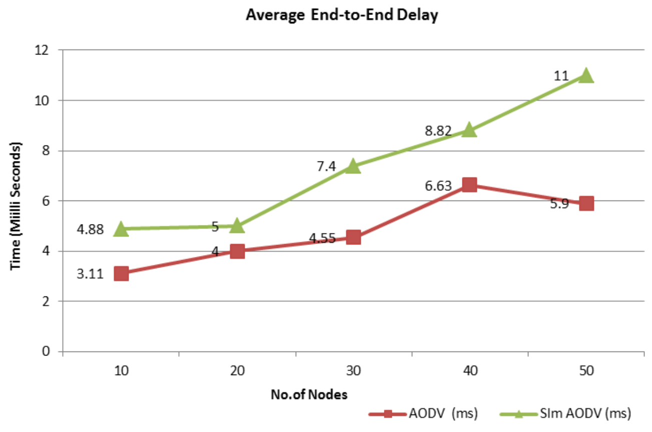

Fig. 4. End-to-End Delay vs. Number of Nodes

CONCLUSION

SIm AODV routing protocol gives excellent packet delivery ratio around 97%. Still the proposed algorithm does not have any encryption technique to provide the security. In this SIm AODV has around five different algorithms, to prevent the packet loss by the malicious and un believable nodes. But the end-to-end time taken is poor compare to the normal AODV.

FUTURE ENHANCEMENT

At present what the SIm AODV has is enough to prevent the packet loss. But this is not enough for the future MANET. Because, future network will become more dense and more big in size. So prevention of packet loss is not only enough, it needs security on data theft as well as more speed.

REFERENCES

[1]. B.Karthikeyan, N.Kanimozhi and Dr.S.Hari Ganesh, Performance and Analysis of Ad-Hoc Network Routing Protocols in MANET,NCAC,April 2013, pp 65-71.

[2]. B.Karthikeyan, N.Kanimozhi and Dr.S.Hari Ganesh, Analysis of Reactive AODV Routing Protocol for MANET|| , IEEE Explore, Oct 2014, pp 264-267.

[3]. B.Karthikeyan, N.Kanimozhi and Dr.S.Hari Ganesh, Complexity in Security Issues of MANET Pertaining to AODV Protocol|| , International Conference on Contemporary Trends in Computer Science (CTCS - 2014). Feb 2014, pp 264-267.

[4]. B..Karthikeyan, N.Kanimozhi and Dr.S.Hari Ganesh- Security and Time Complexity in AODV Routing Protocol, IJAER, pp15542- 155546, Vol 20,June 2015.

[5]. Naincy Juneja, Abhishek Mishra ,An implementation of security policy by using ID in Adhoc routing for mobile network, IJIACS,April 2014.

[6]. Neeraj Saini, Lalit Garg,Enhanced,AODV Routing Protocol against Black hole Attack, IJARCSSE, June 2014.

[7]. Rajdeep S. Shaktawat,Dharm Singh, Naveen Choudhary, An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV), IJCA, July 2014.

[8]. Shabnam, Jitendra Arora, Detection of Cosmic Dust Attack in MANET under AODV Routing Protocol, IJRASET, May 2014.

[9]. Radha Krishna Bar, Jyotsna Kumar Mandal, and Moirangthem Marjit Singh-QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack, 2013.