Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol (OpTiB-AODV)

B. Karthikeyan
Assistant Professor in Department of Computer Application, Bishop Heber College
Trichy, Tamilnadu,India – 620 017

S. Hari Ganesh, PhD
Assistant Professor,
H.H. The Rajas College,
Pudukkotai – 622001,
Tamilnadu, India.

J.G.R. Sathiaseelan, PhD
Head, Department of Computer Science,
Bishop Heber College
Trichy, Tamilnadu, India – 620 017

ABSTRACT
Ad-Hoc On demand Distance (AODV) routing protocol is one of the reactive on-demand routing protocol. It is one of the multicast routing protocol. The basic AODV protocol does not have and mechanism to reduce the end to end time delay. The proposed algorithm Optimal Time Bound (OpTiB)-AODV routing protocol introduce five different way to reduce the end to end time taken. This proposed OpTiB AODV implemented and tested by the use of OmNet++.

Keywords
AODV; OpTiB; OmNet++;

1. INTRODUCTION
Mobile Ad-Hoc Network (MANET) is one of the heterogeneous, self-organizing and self-configured infrastructures less Ad-hoc mobile network. It will not utilize any existing infrastructure. In the MANET each and every node will act as node as well as router. Here all the nodes are movable. Each node has limited radio transmission range. According to Ad-Hoc On-demand Distance Vector (AODV) routing protocol, a node want to communicate with its destination. If the destination is available within the source node's radio transmission range, it will communicate directly. Suppose the destination is may be in different location. The source has to enlist its neighbors and by the use of neighbor (intermediate) node it transfer packets to its destination.

So routing in the Mobile Ad-Hoc Network is very difficult one. Because, all the nodes are mobile nodes, static optimal path is not possible in this network. Dynamic optimal path is possible. This network will have only unstable path between source and destination.

In MANET nodes all are movable and it does not have any topology so security and end to end time delay is very difficult. The security is achieved by the author it is described in contribution 5 and 6.

1.1 Contribution 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 [6] is moderate protocol for all networks.

1.2 Contribution 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 [7] and scalability.

1.3 Contribution 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 [8]. If the security is enhanced it delivers better.

1.4 Contribution 4
Four different kind of customized algorithm [9] 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.

1.5 Contribution 5
The *SIm AODV* [10] has the capable to prevent packet loss owed by *Black Hole Attack, Cosmic Dust Attack, Link Break, and Node Intrusion* by the malicious and un believable nodes. But *SIm AODV* has two major problems one is it does not has the mechanism to prevent active attacks[5]. Second one is end-to-end delay is more compare to the normal AODV.

1.6 Contribution 6
The *En-SIm AODV* [11] overcomes the data change or theft by the malicious node *(*active attacks*)*. This *En-SIm AODV* algorithm uses *PrKeyP (Private Key – Parity Bit)* algorithm

for key based encryption[11] and decryption[13][15][16] and parity bit check.

The proposed work in this paper is concentrate to reduce the end to end time delay

2. LITERATURE SURVEY

Xiaoxia Qi [1] *et al* EM-AODV proposed in this paper is a kind of multi-path routing protocol that uses the node and network comprehensive energy as the main basis.

Manoj Tolani [2] *et al* AODV 512 bits is best packet size, These all values are f or congestion less medium, in congested medium higher packets causes high load and they are dropped so that wireless medium have very noisy environment packet size is very sensitive. In future analyze the packet size of Wi-MAX based MANET.

Shruti Bhalodiya [3] *et al* Flooding attack in MANET results in exhaustion of battery power, degradation of throughput and wastage of bandwidth. In this paper, author is analyzed different techniques to detect and prevent flooding attack on AODV routing protocol in MANET. Main issue present in majority of proposed solutions is not to recover malicious node after punishment. RFAP is a technique for mitigating the RREQ flooding attack, which can recover the malicious node after the reasonable punishment and protect the network against attacker. It has ability to stop and isolate flooding attack with no extra burden on the network resources.

Alisha Dua [4] *et al* The paper modifies the AODV routing and introduces the HAODV for the heterogeneous environment. In the HAODV packet format, one field named rc i.e. routing cost is added to evaluate the routing cost. The rc is calculated based on the link quality and the traffic demand.

Neha Agarwal [5] *et al* In this paper, a new energy efficient routing protocol in MANETs using genetic algorithm has been proposed. In the literature it has been found that Genetic algorithms can be used in routing protocols for mobile ad hoc networks. Genetic algorithm can find an optimal path between nodes of the MANET to transfer data. It can also be used to find an energy efficient path to transfer data between two nodes. In this work a new algorithm using GA has been proposed to find energy efficient path(s) between two nodes. The proposed algorithm also finds alternate paths which can be used when any of the one links fails in the best path.

3. PROPOSED WORK

Early work satisfies the security issues which one available in the AODV routing protocol. The En-SIm AODV protocol reduces the security issues. But it not suitable to provide minimize end-to-end delay.

The proposed work will reduce the end-to-end time delay by the use of following five techniques

1. AODV Packet Size Regulator (PSR) [2]: If the packet size increase the network need more bandwidth or the end to end time delay is more.
2. Multi Path Route Discover (MPRD) [1]: if AODV uses uni-direction route request. It is optimal for security not for the time.
3. Avoid Flooding Attack (AFAN) [3]: If AODV is MPRD it will have the flood message it increase the end to end time.
4. Multiple Optimal Routes to Destination (MORD) [4] : AODV uses the MPRD and AFA it will have more optimal path. If the AODV use priority based more optimal path it will reduce the end to end time for packet delivery.
5. Multiple Packets to Destination (MPD): if the AODV uses more paths every path will get one packet so the deliver time of the packet will reduce.

3.1 Issue 1: AODV Packet Size Regulator (PSR)

```
Struct dpkt{
        char type;
        Bit flag[5];
        Bit res[11];
        char HCount;
        char DestAdd[4];
        char OrginSeqNo[4];
};
```

Step 1: Start
Step 2: Update rdpkt table
Step 3: is data.size>160
Step 4:
//split method split the data as 160 bits and the split data will be in the array rdpkt[]

```
If (data.size>160)
{
        split(data,160)
}
```

//the rdpkt[] data is added with flags, destination address, and originator sequence no. these packet is saved in the dpkt[] array.

```
dpkt(rdpkt,type,flags,hc,DestIP,OrginSeqNo)
```

The PSR algorithm is used to reduce the packet size of the AODV protocol. This protocol is reduce the size of the packet as 256.

3.2 Issue 2 Hello Node Message Packet according to LiFP(Link Failure Prevention)

loop: Watch all incoming packets
if(Received HNREP)

```
{       If(HNREP.dest_Seq_No==( HNREQ.Seq_No+1))
        {       If(HNREP.Hop_Count==0)
                {       Add information to OHNeNT
}       }       }
```

The link failure is prevent by the use of OHNeNT table this table will contain one hop nodes only. If the protocol uses the nodes which one is available in this table, available node will be nearer as well as one hop nodes. This is done by the LiFP algorithm.

3.3 Issue 3: Avoid Flooding Attack by Neighbor (AFAN)

//R_RREQ=Received Rout Request Packet

```
        for (first entry in OHNeNT; OHNeNT!=NULL;
OHNeNT++)
{
        If (OHNeNT.NeN_IP ==R_RREQ.NeN_IP)
        {
                Discard packet;
        }
}
```

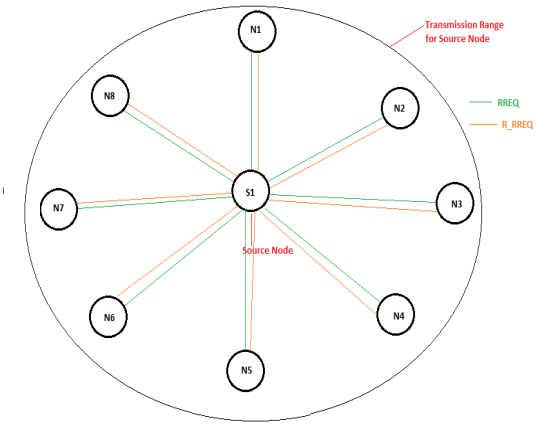

Fig.1. Flooding Attack By Neighbor

The AFAN algorithm prevents the same route request form its neighbors. The above diagram shows the flooding attack the red line shows the flood attack.

3.4 Issue 4: Multiple Optimal Routes to Destination (MORD)

```
Struct OptRout{
        int R_No;
        char RREQ_ID[4];
        char Orgin_IP[4];
        char Dest_IP[4];
        char Dest_SeqNo[4]
};
If (RREP)
{
        Update Optimal route(OptRout) Table;
// Optimal route table will sort every route replay received.
        sort(OptRout);

}

If(RERR)
{
        loop (OptRout)
        {
                If
(RERR.Dest_SeqNo==OptRout.Dest_SeqNo)
                {
                        Delete entry;
                        // Optimal route table
will sort every route replay
        received.
                        sort(OptRout);

}       }       }
```

MORD is one of the algorithm is used in the OpTiB-AODV. Normally all the routing algorithms will enlist optimal path and utilize the path which one is more optimal. This algorithm will do the same work but it will use more than one optimal path from shortlisted routes.

3.5 Issue 5: Multiple Packets to Destination (MPD)

```
Loop Optimal Path from  0 to 9
{

        pktAdd (OptRout.R_No, OP, dpkt[OP]);
}
//pk→Packet No
pk=0;
Loop Optimal Path from  0 to 9
{       pktSend(OptRout[OP],dpkt[OP]);
        dpkt[OP].Send_Status=true;
        pk++;  }
//rPK→ Remaining Packets
rPK=dpkt.count();
//tpk_no→Temp packet no
tpk_no=pk;
pk=pk-1;
If(PK_ACK)
{       loop(dpkt[pk] to dpkt[rpk] )
        {       OP=PK_ACK.R_NO;

        dpkt[PK_ACK.pk_NO].ACK_Status=true;
                pktSend(OptRout[OP],dpkt[tpk_no])
                dpkt[OpRout.pk_NO].Send_Status=true;
                OptRoute[OP].pk_NO=tpk_no;
                tpk_no++;

}
```

According to the MORD the OpTiB-AODV will use more than one optimal path.The MPD will choose more than one packet for more than one optimal route. This will be provides less end to end delay compare to the normal AODV.

4. SIMULATION

OMNeT++ is an object oriented discrete event simulation environment developed by Andr´as Varga at the Technical University of Budapest. 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 h/w architectures, since OMNeT++ is built generic, more flexible and modular. As the architecture is modular, the simulation kernel and models can be embedded easily into an application. C++ programming structure is used for the modules in OMNeT++.

4.1 Simulation Parameters

Table.1. Simulator Parameter

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

5. RESULT AND DISCUSSION

Table.2.Throughput or Packet Delivery Ratio

No. of Nodes	Total Packets	AODV (PPs)	SIm AODV (PPs)	En-SIm AODV (PPs)	OpTiB AODV (PPs)
10	30	18	25	24	19
20	60	40	42	40	41
30	90	60	83	78	58
40	120	96	109	102	95
50	150	121	145	130	120

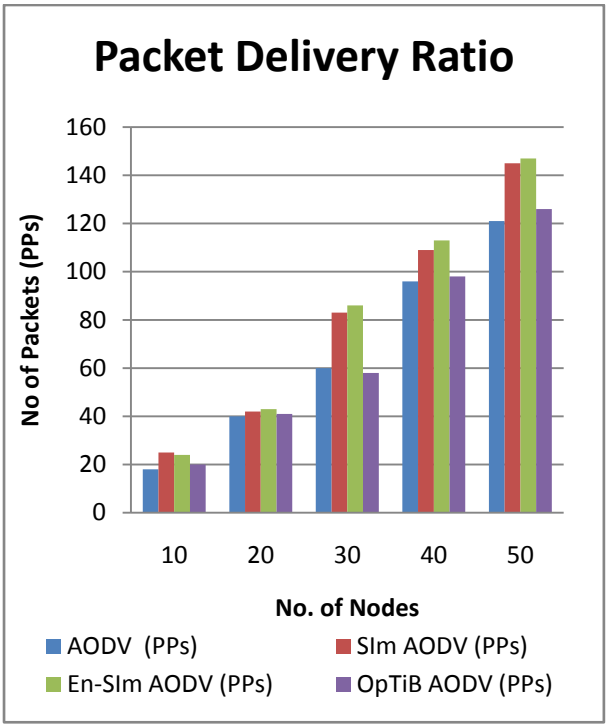

Fig.2. Packet Delivery Ratio

The above diagram shows the packet delivery ratio between AODV,SIm AODV, En-SIm AODV and OpTiB AODV alogrithms .The SIm AODV and En-SIm AODV provides good packet delivery ratio. But OpTiB provides less than the above two algrithm but above normal AODV.

The folowing table shows the result of the end to end time delay between Normal AODV,SIm AODV,En-SIm AODV and OpTiB AODV. The OpTiB AODV Algrithm provides mimul End-to-End delay compare to other AODV's algorithm..

Table.3.End-to-End DelayTime

No. of Nodes	AODV (ms)	SIm AODV (ms)	En-Sim AODV (ms)	OpTiB AODV (ms)
10	3.11	4.88	3.72	0.92
20	4	5	4.26	0.9
30	4.55	7.4	6.12	0.83
40	6.63	8.82	7.26	0.71
50	5.9	11	9.5	0.6

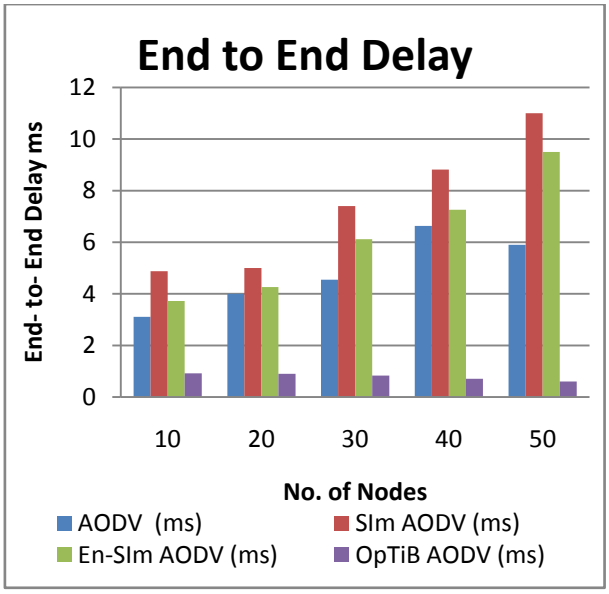

Fig.3. End-to-End Delay Time

6. CONCLUSION

The OpTiB AODV provides very less end to end delay with moderate security. The OpTiB AODV has around five different protocols. The OpTiB reduce end to end time delay compare to other AODV algorithms.

7. FUTURE ENHANCEMENT

This OpTiB AODV concentrates only on the end-to-end time taken. It has to implement with En-SIm AODV. Then only understand how much amount of time it will take with security.

8. REFERENCES

[1] Xiaoxia Qi ,Qijin Wang and Fan Jiang, " Multi-path Routing Improved Protocol in AODV Based on Nodes Energy", International Journal of Future Generation Communication and Networking Vol. 8, No. 1 (2015), pp. 207-214

[2] Manoj Tolani, Rajan Mishra,l " *Effect of Packet Size on Various MANET Routing Protocols*", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Volume 4– No.9, December 2012,PP:10-13.

[3] Shruti Bhalodiya and Krunal Vaghela, " *Study of Detection and Prevention Techniques for Flooding attack on AODV in MANET*" International Journal of Science and Research (IJSR), Volume 4 Issue 1, January 2015,PP: 433-436

[4] Alisha Dua, Sandeep Dalal and Kamna Solanki, "*Efficient Routing Technique in Heterogeneous Wireless Network*", International Journal of Computer Applications (0975 – 8887) Volume 127 – No.14, October 2015,PP:36-39.

[5] Neha Agarwal and Neeraj Manglani, "*A New Approach for Energy Efficient Routing in MANETs Using Multi Objective Genetic Algorithm*", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015pp 1780-1784.

[6] 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.

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

[8] 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.

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

[10] B..Karthikeyan, N.Kanimozhi and Dr.S.Hari Ganesh-Security Improved Ad-Hoc On-demand Distance Vector Routing Protocol, IJRE, pp, Vol ,On Print.

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