RESEARCH ARTICLE OPEN ACCESS

Power Aware Encrypted Security Improved with Optimal Time Bound Ad-Hoc on-demand Distance Vector Routing Protocol (PA-En-SIm-OptiB AODV)

Dr. B.Karthikeyan
Assistant Professor
Department of Computer Science,
Bishop Heber College, Trichy
Tamilnadu -, India.

ABSTRACT

In Mobile Ad Hoc network security, transmission time and power utilization is difficult to achieve optimization. Because MANET form network by the use of movable nodes. Movable nodes continuously changes network topology. This topology change causes the un believe nodes, link break, Black Hole attack and security issues like data change and data theft. This paper proposes Power Aware, Encrypted, Security improved and optimal time bound (PA-En-SIm-OpTiB) algorithm over Ad-Hoc on-demand Distance Vector Routing protocol.

Keywords:- MANET, Security, Transmission Time, Power Utilization.

I. INTRODUCTION

Mobile Ad-hoc network is one of the self-organize and self-configure infrastructure less network. This temporary network does not utilize any existing infrastructure. Nodes which is available in this network will act as a node, intermediate node and router. So, node's has responsibility to invent temporary static route, establish the route, maintain the route, and terminate the route.

Route creation, establishment, maintenance, and termination is very difficult with this temporary topology. Routing with this movable nodes is very difficult. But existing routing protocols provides solution for this problems, although routing in MANET is one of the complex process for nodes.

Normally MANET routing protocol is classified into two major categories. Proactive (table driven) and Reactive (on-demand) routing protocol. MANET routing has another one type named as hybrid. It is the combination of the proactive and reactive. This work uses AODV (Ad-hoc on demand distance vector) routing protocol. According to the previous work of this author, AODV is the moderate routing protocol for moderate network.

Normal AODV routing protocol doesn't have any technique facility for to improve Packet Delivery Ratio (PDR), to reduce End to End Time Delay EETD), to improve Security and to reduce Power Consumptions.

The proposed work provides Power Aware Encrypted Security improved Optimal Time Bound path between source and destination in the MANET.

II. EARLY STAGES OF RESEARCH

A. Stage 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 [1] is moderate protocol for all networks.

B. Stage 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 [2] and scalability.

C. Stage 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 [3]. If the security is enhanced it delivers better.

D. Stage 4:

Four different kind of customized algorithm [3] 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-toend 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.

E. Stage 5:

The SIm AODV [4] 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.

F. Stage 6:

The En-SIm AODV [4] 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[16] and decryption and parity bit check.

G. Stage 7:

The OpTiB AODV [5] 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.

H. Stage 8:

The proposed work is concentrate to combine Power Aware, En-SIm AODV and OpTiB AODV [6] with intruders. So this proposed PA-En-SIm-OpTiB AODV is evaluated

III. PROPOSED WORK

The HiLeSec-OpTiB algorithm has around twelve different algorithms. The first five algorithm is used to provide security by avoid Link Break, Cosmic Dust Attack, Gray Hole Attack and Black Hole attack. This Five algorithm's bundle is called "Security Improved" (SIm) AODV. The "Encrypt Security Improved"(En-SIm) AODV has the next two Pr1KeyP-E and PrKeyP-D algorithms. By the use of these two algorithms sending and receiving packet will be encrypt and decrypt and also reduce data loss. The Optimal Time Bound(OpTiB) AODV has last five (Packet Size Regulator (PSR), Multi Path Route Discover (MPRD), Avoid Flooding Attack by Neighbor (AFAN), Multiple Optimal Routes to Destination (MORD) and Multiple Packets to Destination (MPD)) algorithms. These algorithms provide minimal amount on time delay between Source and Destination.

The PA (Power Aware) algorithm concentrate the power consumption of the optimal path. This algorithm finds the power conception of the optimal path by the use of Optimal Path Consume Power Ratio (OpPCPE). The PA is implemented over the En-SIm-OptiB. So the optimal path was found by

the early algorithm. The proposed utilized the optimal path from the early.

A. PA-En-Sim-OpTiB Pseudo Code

Step 1: Start
Step 2: Create HNREQ (Host Neighbor Request)
Step 3: Broadcast HNREQ (Host Neighbor Request)
Step 4: Start RC (Route Counter)
Step 5: Check is (data) then Step 6 else Step 8
Step 6: Check is (data.size>160) then Step 7 else Step 8
Step 7 : Call split(data,160)
Step 8 : Update data packet(rdpkt,type,flags,hc, DestIP, OrginSeqNo)
Step 9 : Loop: start to listen all incoming Packet
Step 10: Check Packet is Route Request (RREQ) then
Step 11 else Step 15
Step 11 : loop Start all OHNeNT(One Hop Neighbor Node Table
Step 12 : Check (OHNeNT.NeN_IP ==R_RREQ. NeN_IP) then Step 13 else Step 14
Step 13 : Discard packet;
Step 14 : Loop end all OHNeNT
Step 15 : Check is Rout Replay(RREP) then Step 16 else Step 42
Step 16 : Route value check local(rvcl) = call replay check(RREP)
Step 17 : Check is route value check local (rvcl) then Step 18 else Step 42
Step 18 : Find Minimum number in RC entry in Link On Time Table(L2T) with Link No array (LiNo[]);
Step 19 : Loop: Start LiNo[] //list node
Step 20 : Calculate net receiving packet(nrp=trp-orp)
Step 21 : Calculate net sending packet(nsp=tsp-osp)
Step 22 : Calculate Believe node factor (B = nsp/nrp)
Step 23 : Check Believe Node Factor is 1 then Step 24 else Step 25
Step 24: Belief Node, add into the BNLT;
Step 25 : Not a Belief node
Step 26 : Loop end:LiNo[]
Step 27 : Loop: Start BNLT[]
Step 28 : Check is (BNLT.Hop_Count==0) then Step 29 else Step 30
Step 29 : Add information to OHNeNT
Step 30 : Loop end : BNLT[]
Step 31 : Update OpPNoA[n][m] array
Step 32 : Loop I= 0 to n
Step 33 : Loop j= 1 to m
Step 34 : OpPNoE[i][j]=OpNoRE[i][j] + OpNoTE[i][j] + OpNoPE[i][j];
Step 35 : OpPCPR[i]= OpNoRE[i][j].

OpNoTE[i][j] $\left(\frac{\lambda}{4\pi.rtr}\right)^2$

Step 36 : Loop end j
Step 37 : Loop end i
Step 38 : Copy OpPCPR array value to OPPCPRT
Step 39 : Loop i=0 to n
Step 40 : Loop j= 1 to m
Step 41 : Check OpPCPRT[i]>OpPCPRT[j] the Step 42 else Step 45
Step 42 : TCPR=OpPCPRT[i];
Step 43 : OpPCPRT[i]=OpPCPRT[j];
Step 44 : OpPCPRT[j]=TCPR;
Step 45 : Check ((n%2)==0) Then Step 46 else step 47
Step 46 : MVal=n/2;
Step 47 : MVal=round(n/2);
Step 48 : ESum=0;
Step 49 : Loop i=0 to MVal
Step 50 : ESum=ESum+ OpPCPRT[i];
Step 51 : Loop end i
Step 52 : AvgLow =ESum/MVal;
Step 53: ESum=0;
Step 54 : Loop i=MVal to 0
Step 55 : ESum=ESum+ OpPCPRT[i];
Step 56 : Loop End i
Step 57 : AvgHigh =ESum/MVal;
Step 58 : LAvgSSr=(SS/100) * 35;
Step 59 : HAvgSSr=(SS/100) * 85;
Step 60 : RP= OpPNoE[OpP][node] - OpNoPE[OpP][node];
Step 61 : Check ((RSS > LAvgSSr) && (RP > 15%) && (OpPCPRT[Node Optimal Path] > AvgLow)) then Step 62 else Step 63
Step 63 : Follow normal AODV Flow and Exit. (Drop if duplicate else forward RREQ and Data)
Step 63 : Drop RREQ to stop including such node in new routing path and exit
Step 64 : Check (Rpt==DATA) Then Step 65 else Step 67
Step 65 : Check (the neighbours find the alternate path) then Step 66 else Step 67
Step 66 : Routing tables will be updated to bypass the current node

Step 67 : Continue with current path
Step 68: PA_End
Step 69 : Update Optimal route(OptRout) Table;
Step 70 : sort(OptRout);
Step 71 : Loop Start Optimal Path from 0 to 9
Step 72 : Packet Add (OptRout.R_No, OP, dpkt[OP]);
Step 73 : Loop End Optimal Path
Step 74 : Packet Count (pk=0)
Step 75 : Loop Optimal Path from 0 to 9
Step 76 : Packet Send (pktSend(OptRout[OP], dpkt[OP]))
Step 77 : dpkt[OP].Send_Status=true;
Step 78 : Increment Packet Count(pk++)
Step 79 : Loop End Optimal Path
Step 80 : Calculate next packet
Step 81 : Check received packet is Host Neighbor Reply(HNREP) then Step 82 else Step 83
Step 82 : Update Link Time Table (L2T)
Step 83 : Check Received Packet is Route Error (RERR) then Step 45 else Step 50
Step 84: loop Start Optimal Route
Step 85 : Check is (RERR.Dest_SeqNo== OptRout.Dest_SeqNo) then Step 86 else Step 88
Step 86 : Delete entry;
Step 87 : sort Optimal Route
Step 88 : Loop End Optimal Route
Step 89 : Check is Packet Acknoledment then Step 90 else Step 93
Step 90 : loop Start one(dpkt[pk] to dpkt[rpk])
Step 91 : update all sent packet status
Step 92 : loop End one
Step 93 : Loop: end Base
Step 94 : End

IV. RESEARCH METHODOLOGY

In order to analyze the performance of the AODV routing protocols, with respect to the following metric:

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.

Packet Delivery Ratio (PDR) = S1 / S2

Where

S1 → The sum of data packets received by the each destination

S2 →The sum of data packets generated by the each source.

Average end-to-end delay: This implies the delay a packet suffers between leaving the sender application and arriving at the receiver application.

End to End Time Delay (EETD) = S/N

Where

S → the sum of the time spent to deliver packets for each destination

N→ the number of packets received by the all destination nodes.

Consumed Energy :The number of nodes in the network versus the total consumed energy is considered as a metric.

CnEn=NoTP * C1 + NoRP * C2

Where

CnEn → Coonsumed Energy
NoTP → Number of Transmitted Packet
NoRP → Number of Recived Packet
C1 & C2→ Constant one and two

Remaining Energy : The remaining energy available in each node after the transmission.

ReEn = InE - CnEn

Where

ReEn → Remaining Energy
InE → Initial Energy
CnEn → Consumed Energy

V. 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, 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 and the running screen shots are shown in the Fig.1. a., 1.b.

A. *Simulation Parameters*

Table .1. Simulation Parameters

Parameters	Values
Network Size	600 m x 600m
Number of Nodes	0-50

Max. Speed / Mobility	10.0ms/s
Pause Time	0-100s
Traffic model	CBR
Routing Protocols	AODV UU With PA-En-SIm—OpTiB
Simulation Time	600s

B. Simulation Outputs

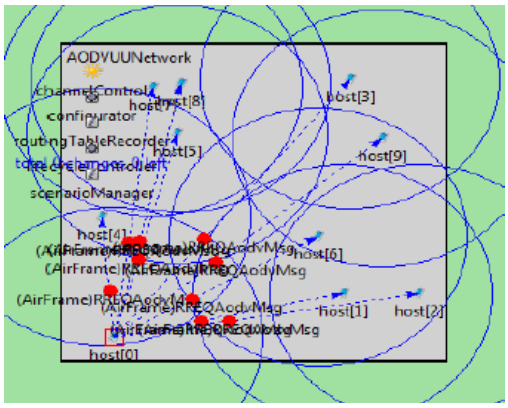
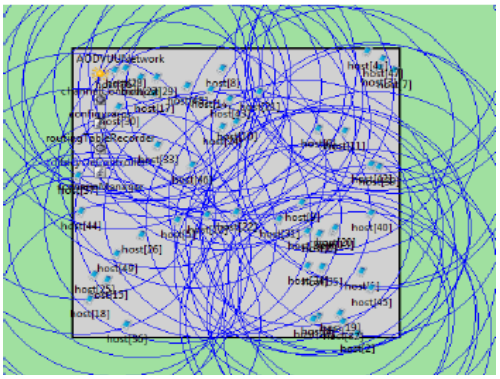


Fig 1.a. OMNet++ Simulation Output with 10 nodes



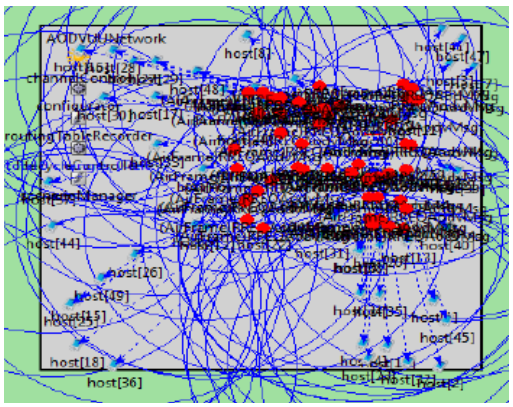


Fig 1.b. OMNet++ Simulation Output with 50 nodes

VI. RESULTS AND DISCUSSION

The proposed PA-En-SIm-OpTiB AODV is evaluated in two ways. First it is evaluated by the use of Packet Delivery Ration (PDR) and End to End Time Delay (EETD) metrics. These two metrics is used in two forms to evaluate the security, optimal time, and encryption. They are with intruders and without intruders.

The following table shows comparition of Packet Delivery ratio with Normal AODV, SIm AODV, En-SIm AODV, OpTiB AODV, En-SIm-OpTiB AODV, and PA-En-SIm-OpTiB AODV. As per the results SIm AODV provide higher PDR, next to SIm AODV En-SIm AODV provides higher PDR, after that En-SIm-OpTiB AODV, and PA-En-SIm-OpTiB AODV provides higher PDR.

Table.2 Packet Delivery Ratio without Malicious Nodes

No. of Nodes	Total Packets	AODV (PPs)	SIm AODV (PPs)	En-SIm AODV (PPs)	OpTiB AODV (PPs)	En-Sim-OpTiB AODV (PPs)	PA-En-Sim-OpTiB AODV (PPs)
10	30	18	25	24	19	23	22

20	60	40	42	40	41	42	41
30	90	60	83	78	58	81	53
40	120	96	109	102	95	107	105
50	150	121	145	130	120	141	142

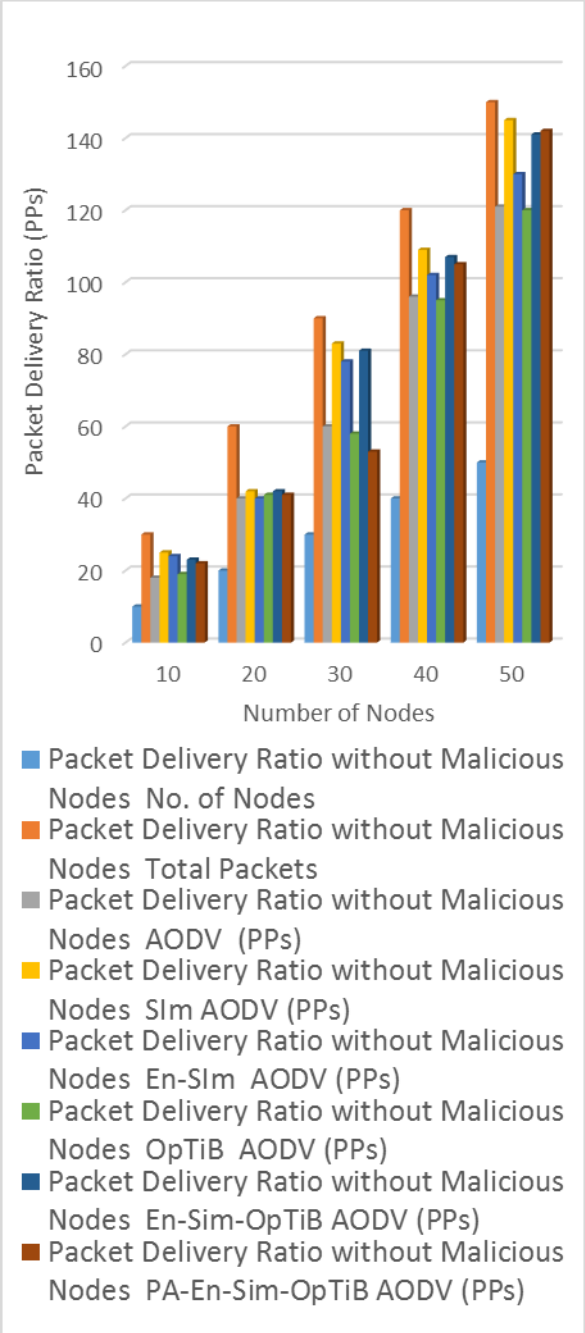


Figure 2. Packet Delivery Ratio between AODV, SIm AODV, En-SIm AODV, OpTiB AODV, En-SIm-OpTiB AODV, and PA-En-SIm AODV without Malicious.

The following table 3. Shows EETD between AODV, SIm AODV, En-SIm AODV,

OpTiB AODV, En-SIm-OpTiB AODV, and PA-En-SIm AODV without Malicious. En-SIm-OpTiB AODV provides excellent EETD compare to all other implementation.

If implement Power Aware algorithm with En-SIm-OpTiB AODV it consumes more EETD compare to the En-SIm-OpTiB AODV. But it consumes less EETD compare to all others.

Power Aware (PA) algorithm provides less power consumption, due to this algorithm it tooks little bit higher time to reach destination.

Table 3. End to End Time Delay without Malicious Nodes

No. of Nodes	AODV (ms)	SIm AODV (ms)	En-SIm AODV (ms)	OpTiB AODV (ms)	En-Sim-OpTiB AODV (ms)	PA-En-Sim-OpTiB AODV (ms)
10	3.11	4.88	3.72	0.92	1.02	1.001
20	4	5	4.26	0.9	0.98	0.99
30	4.55	7.4	6.12	0.83	0.9	0.92
40	6.63	8.82	7.26	0.71	0.81	0.8
50	5.9	11	9.5	0.6	0.64	0.7

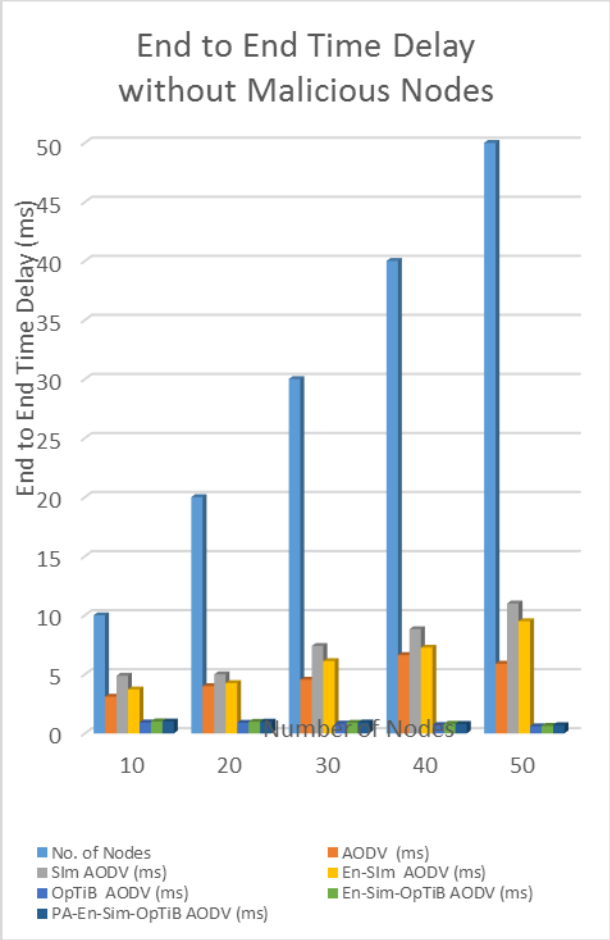


Figure 3.End to End Time Delay between AODV, SIm AODV, En-SIm AODV, OpTiB AODV, En-SIm-OpTiB AODV, and PA-En-SIm AODV without Malicious.

Table 4. Packet Delivery Ratio with Malicious Nodes

No. of Nodes	Total Packets	AODV (PPs)	SIm AODV (PPs)	En-SIm AODV (PPs)	OpTiB AODV (PPs)	En-Sim-OpTiB AODV (PPs)	PA-En-Sim-OpTiB AODV (PPs)
10	30	2	14	23	23	16	19
20	60	4	32	38	38	35	38
30	90	6	48	75	74	49	58
40	120	8	77	98	97	81	79
50	150	10	97	131	124	102	97

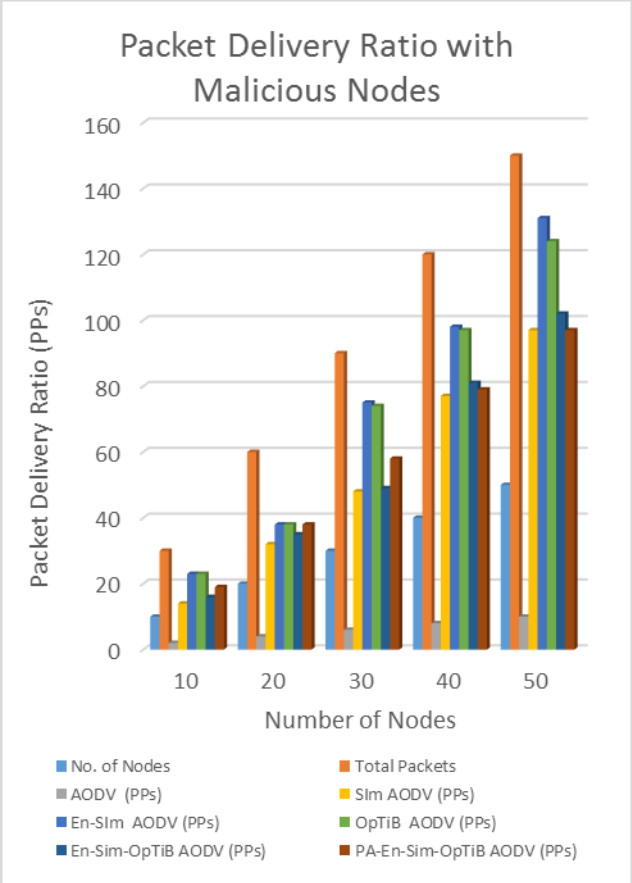


Figure 4. Packet Delivery Ratio between AODV, SIm AODV, En-SIm AODV, OpTiB AODV, En-SIm-OpTiB AODV, and PA-En-SIm AODV with Malicious.

Table 5. End to End Time Delay with Malicious Nodes

No. of Nodes	AODV (PPs)	SIm AODV (PPs)	En-SIm AODV (PPs)	OpTiB AODV (PPs)	En-Sim-OpTiB AODV (PPs)	PA-En-Sim-OpTiB AODV (PPs)
10	3.11	4.88	3.72	0.92	1.02	0.99
20	4	5	4.26	0.9	0.98	1
30	4.55	7.4	6.12	0.83	0.9	0.95
40	6.63	8.82	7.26	0.71	0.81	0.8
50	5.9	11	9.5	0.6	0.64	0.63

When network introduce malicious nodes, compare to all other algorithms PA-En-SIm-OpTiB AODV provides good PDR and less EETD. The results shows, PA-En-SIm-OpTiB AODV gives excellent job against QoS problems.

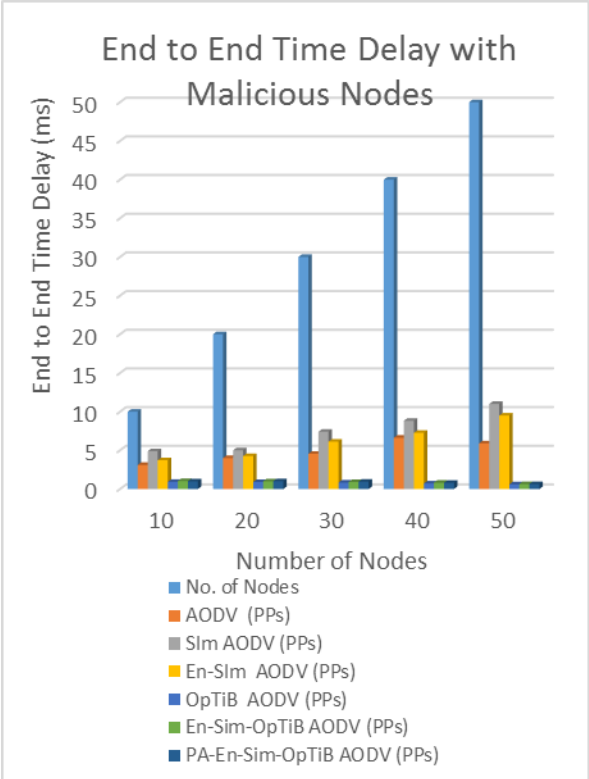


Figure 5.End to End Time Delay between AODV, SIm AODV, En-SIm AODV, OpTiB AODV, En-SIm-OpTiB AODV, and PA-En-SIm AODV with Malicious.

Next, this work is going to evaluate how far the power consumption is provided by the three different algorithms. For this comparison Normal AODV, En-SIm-OpTiB AODV, and PA-En-SIm-OptiB AODV was taken.

Power Aware algorithm provides excellent remaining power. The following three comparisons shows how PA-En-SIm-OpTiB, AODV provides excellent power saving technique.

Power Aware-Encrypted-Security Improved – Optimal Time Bound AODV

Table 6. Power Consumption and Remaining power

s of N	AODV	En-Sim-OpTiB-	Po-En-Sim-

			AODV		OpTiB-AODV	
	Remaining Energy (Joules)	Consumed Energy (Joules)	Remaining Energy (Joules)	Consumed Energy (Joules)	Remaining Energy (Joules)	Consumed Energy (Joules)
10	208.1324	2791.8676	302.62438	2463.56165	397.11636	2135.2557
20	964.7701	5035.2298	1402.77565	4304.02115	1840.7812	3572.8125
30	1396.2204	7603.7795	2030.10445	6513.8936	2663.9885	5424.0077
40	584.8544	11415.146	850.37825	10135.60565	1115.9021	8856.0653
50	2266.4013	12733.599	3295.3474	10925.3683	4324.2935	9117.1376

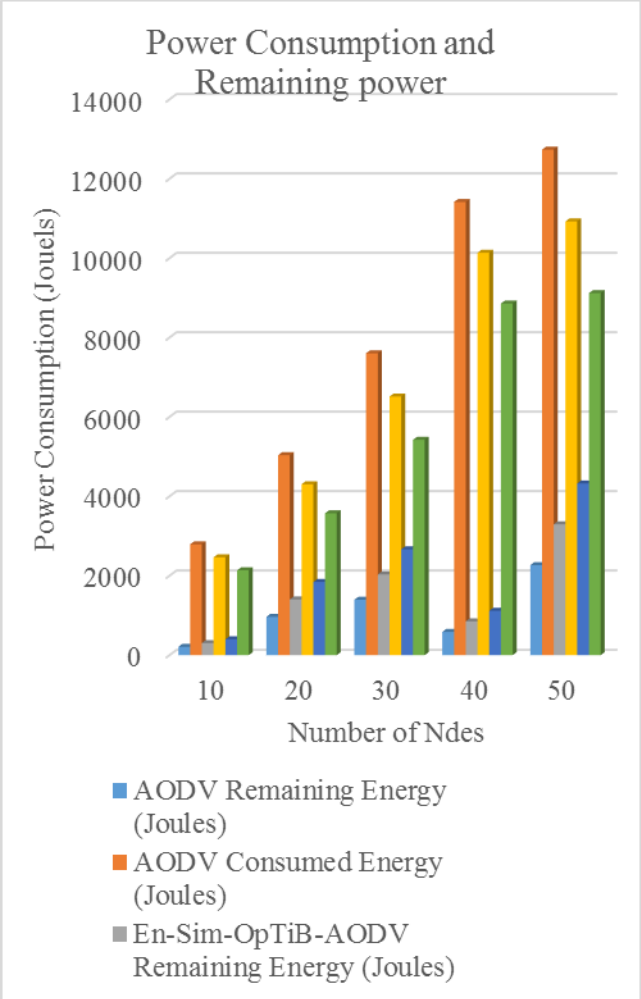


Figure 6. Power consumption comparison between AODV, En-SIm-OpTiB , and PA- En-SIm-OpTiB

Table 7. Routing Overload

No. of Nodes	AODV (%)	En-SIm-OpTiB-AODV (%)	PA-En-SIm-OpTiB-AODV (%)
10	31.4	23.25	15.1
20	67.8	53.25	38.7
30	71.8	54.7	37.6
40	79.1	60.15	41.2
50	87.2	67.7	48.2

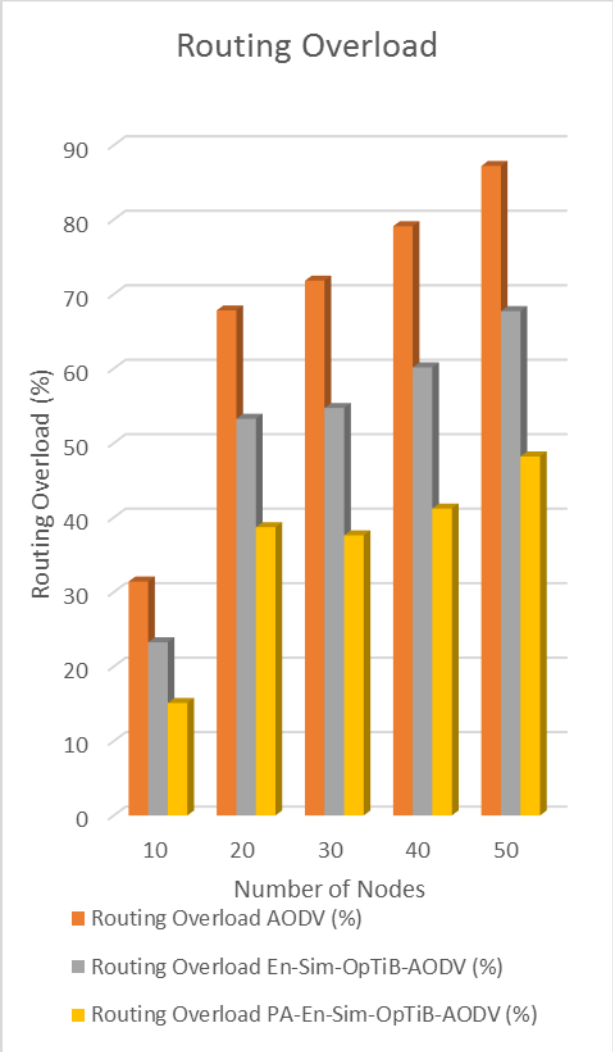


Figure 7. Routing overload comparison between AODV, En-SIm-OpTiB , and PA- En-SIm-OpTiB

Table 8. Normalized Routing Load

No. of Nodes	AODV (%)	En-SIm-OpTiB-AODV (%)	Po-En-SIm-OpTiB-AODV (%)
10	0.7863	0.71265	0.639
20	0.0073	0.00705	0.0068
30	0.0553	0.05585	0.0564
40	0.1346	0.1223	0.11
50	0.0352	0.0276	0.02

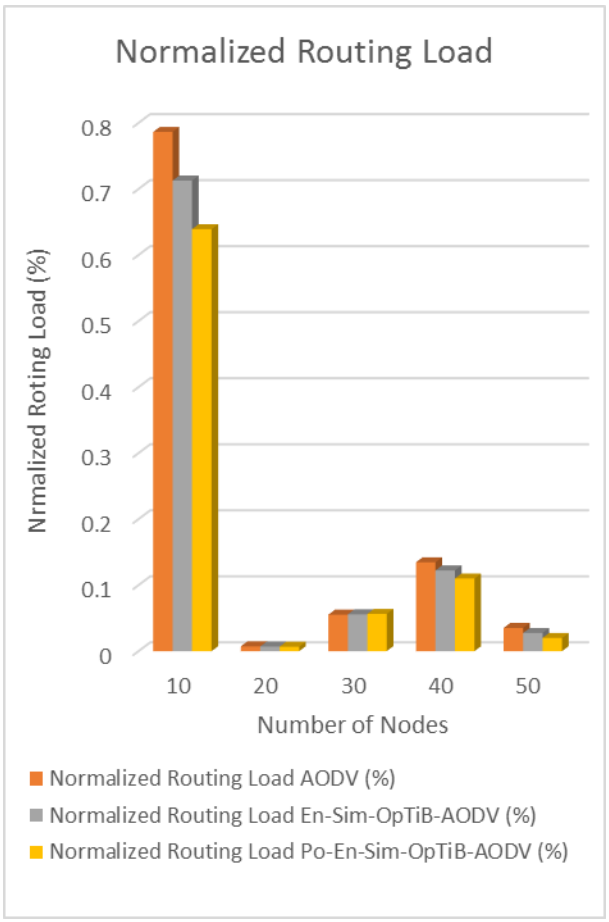


Figure 8. Normalized Routing Overload comparison between AODV, En-SIm-OpTiB , and PA- En-SIm-OpTiB

The three metrics is used to find the power effectiveness of algorithm. They are power consumption, routing load, and normalized routing load. From this above results the PA-En-SIm-OpTiB AODV gives good and moderate power saving.

VII. CONCLUSION

The above result is obtained by six different metrics. The proposed PA-En-SIm-OpTiB AODV gives good power efficiency. But it give less packet delivery ratio compare to En-SIm-OpTiB AODV. So as per the simulation result PA-En-SIm-OpTiB AODV is provides moderate packet delevery ratio, reduced end to end time delay, and good power efficiency with this simulation scenario.

VIII. FUTURE ENHANCEMENT

PA-En-SIm-OpTiB AODV algorithm is tested only in the simulation with defined scenario. In future it should be test in the test bed emulator after that real time test bed.

REFERENCES

[1]. B.Karthikeyan and Dr.S.Hari Ganesh, "Performance and Analysis of Ad-Hoc Network Routing Protocols in MANET", NACA, Mar 2013, pp. 65-71.

[2]. B.Karthikeyan, Dr.S.Hari Ganesh, and N.Kanimozhi "*Analysis of Reactive AODV Routing Protocol for MANET*", IEEE Xplore, Digital Library,ISBN:978-1-4799-2876-7, Oct 2014, pp. 264-267, Scopus Index, Impact Factor :5.629.

[3]. B.Karthikeyan, Dr.S.Hari Ganesh, and N.Kanimozhi "*Security and Time Complexity in AODV Routing Protocol*", International Journal of Applied Engineering Research (ISSN:0973-4562), Vol. 10, No.20, June 2015, pp.15542- 155546. – Scopus Indexed, Impact Factor: 1.35.

[4]. B. Karthikeyan and Dr.S.Hari Ganesh, "*Encrypt - Security Improved Ad Hoc On Demand Distance Vector Routing Protocol (En-SIm AODV)*", ARPN Journal of Engineering and Applied Sciences (ISSN: 1819-6608), Vol. 11, No. 2, January 2016,pp. 1092-1096,Scopus Indexed, Impact Factor: 2.5682.

[5]. B. Karthikeyan,Dr.S.Hari Ganesh and Dr. JG.R. Sathiaseelan, " *Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol (OpTiB-AODV)*", International Journal of Computer Applications (ISSN:0975 – 8887), Vol. 140, No.6, April 2016,pp 7-11, Impact Factor:0.11.

[6]. B. Karthikeyan, Dr.S.Hari Ganesh and Dr. JG.R. Sathiaseelan , "*High Level Security with Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol (HiLeSec-OpTiB AODV)*",International Journal of Computer Science Engineering(E-ISSN: 2347-2693),Vol. 4, No. 4, April 2016, pp.156-164, Impact Factor: 2.162.