IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-4 E-ISSN: 2347-2693

High Level Security with Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol (HiLeSec-OptiB AODV)

B.Karthikeyan[1*], S. Hari Ganesh Ph.D[2], J.G.R. Sathiaseelan, Ph.D [3th] and N.Kanimozhi[4]

[1] *Assistant Professor, Departmen of Computer Sience,Bishop Heber College, Trichy, Tamilnadu, India.*
[2] *Assistant Professor, Departmen of Computer Sience, H.H.The Raja's College, Pudukkotai , Tamilnadu, India.*
[3] *Associative Professor and Head, Departmen of Computer Sience,Bishop Heber College, Trichy, Tamilnadu, India.*
[1] *Assistant Professor, Departmen of Computer Sience, Shrimathi Indira Gadhi College, Trichy, Tamilnadu, India.*

Available online at: www.ijcseonline.org

Received: Mar/21/2016 Revised: Apr /01/2016 Accepted: Apr/16/2016 Published: Apr/30/2016

Abstract-The most wanted wireless networks is Mobile Ad hoc Network (MANET). MANET can configure easily without any infrastructure which one is used by 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 the proposed HiLeSec-OpTiB AODV is the combination of En-SIm and OpTiB AODV. This combined algorithm is tested with intruders(active and passive attackers). This proposed HiLeSec-OpTiB AODV is implemented and tested by the use of OmNet++.

Keywords: SIm AODV; En-SIM AODV; MANET; Self-Configuring; HiLeSec-OpTiB AODV; OmNet++

I. Introduction

Mobile Ad-hoc Networks (MANET's), nodes all are moving, they don't have any precise infrastructure and they are connected dynamically in a temporary arbitrary way. Nodes within each other's radio ranges they can communicate directly throw radio communication links, 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. . Mobile device in an ad-hoc network travel dynamically; consequently keeping track of the network topology is a difficult task to achieve communication. The fig.1. show the example MANET.

A. MANET Challenges

Limited bandwidth: Wireless link continue to have significantly lower capacity than existing infrastructure oriented wired or wireless networks.

In addition, the realized throughput of wireless communicationchannel after accounting for the effects (noise, multiple access, interference conditions, and fading), all other is less than a radio's maximum transmission rate.

Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. If some nodes are detected as compromised, it will disturb trust among some nodes.

Routing Overhead: In wireless ad hoc networks, nodes change their location frequently within network. So, some flat routes are generated in the routing table which leads to unnecessary routing overhead.

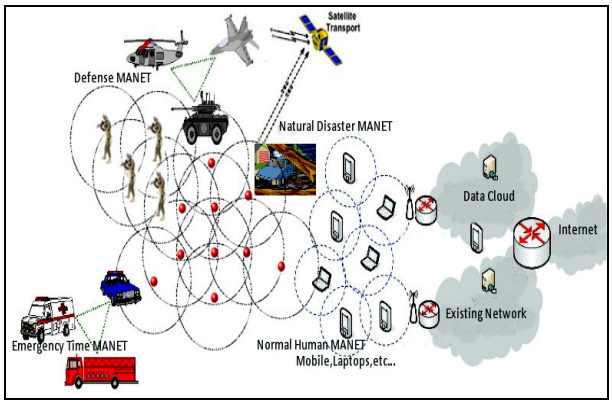


Fig.1. Mobile Ad-Hoc Network (MANET)

*Hidden terminal problem***:** The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission boundary of the originator, but are within the transmission range of the receiver.

Packet losses: The less infrastructure wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, and frequent path breaks due to mobility of nodes.

Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence the frequent path break disturbs

on-going session. So the network need frequent route changes.

Battery restrictions: Portability of the devices has restrictions on the power, size and weight of the device.

Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless communication channel is vulnerable to eavesdropping and ad hoc network functionality is established through node collaboration, mobile ad hoc networks are naturally exposed to numerous security attacks.

B. MANET Routing

MANET has the lot of challenges so that network needs some standardized way (routing protocol) to make a communication between two mobile nodes. The figure 2 shows the types which one is available in the MANET.

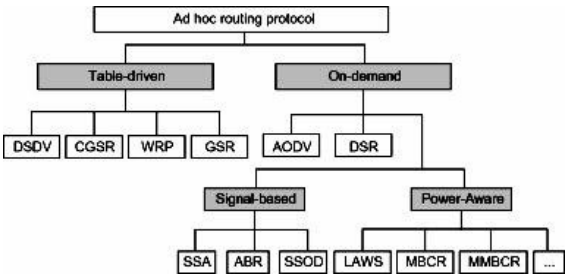


Fig. 2. Types of MANET Routing Protocols

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.

Security is the major concern in network like MANET where any node without any authentication comes in the network and leaves network. In MANET there is no central authority that can govern the authentication of nodes, which can make sure that the nodes in the network are not malicious.

C. Mobile Ad hoc Network: Attacks

These attacks are divided into two main categories as: Passive attacks and Active attacks.

Passive Attacks

Passive attacks are the attacks in which an attacker does not actively participate in bringing the network down. An attacker just secretly listen the network traffic as to determine which nodes are trying to establish routes, or which nodes are important to proper operation of the network and hence can be potential candidates for subversion and launching denial of service attacks. The attacker can then forward this information to an accomplice who in turn can use it to launch attacks to bring downward the network. The attitude of attacks varies greatly from one set of circumstances to another. Some of the generic types of attack that might be encountered in passive attacks are:

Interruption: An asset of the system is ruined, becomes unreachable. This is an attack on availability. Examples include destruction of a part of hardware, or cutting from a communication line.

Interception: An unauthorized party gains access to an resources. This is an attack on secret manner. The unauthorized party could be a individual, a program or a system. Examples include wiretapping to capture data in a network or the illicit copying of files.

Modification: An unauthorized party tampers with an resource. This is an attack on honesty. Examples include altering values in a data file or modifying the contents of a message being transmitted in a network.

Fabrication: An unauthorized party inserts malicious objects into the system. This is an attack on authentication. Examples include the insertion of fake messages in a network or the addition of records to a file.

Active Attacks

These attacks involve some alteration of the data stream or the creation of a false stream and can be subdivided into four categories.

Replacement: In this attack one object pretends to be a different object. It is done by someone familiar with your security procedures and failures. An impersonate attack usually includes one of the other forms of active attacks.

Replay: This involves capture of data units and its subsequent retransmission to produce an unauthorized effect. Safe guard are used for legitimate network management functions.

Modification of Messages: This simply means that some portion of a legitimate message is altered, delayed or reordered. Here someone between you and your connection works as an in-between, listening in on your communications and possibly modifying them.

Denial of Service: This prevents the normal use or management of communication facilities. One form of service denial is the disruption of an entire network, either by inactivating the network or by over heading it with messages

so as to degrade the performance. It is like shutting down a server that could not otherwise be compromised.

Intrusion Detection Schemes

MANETs present a number of unique problems for Intrusion Detection Systems (IDS). Differentiating between malicious network activity and fake, but typical, problems associated with a mobile ad hoc networking environment is a challenging task. In a mobile ad hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may perform maliciously only at regular intervals, further complicating their detection. The loss or capture of unattended radios and personal computing devices may allow for a malicious node to obtain legitimate credentials and launch more serious attacks.
A node that sends out fake routing information could be a compromised node, or simply a node that has a temporarily stale routing table due to volatile physical conditions. Constant changes in topology make it difficult to obtain a global view of the network and any approximation can become quickly invalid. Traffic monitoring in infrastructure wired networks is usually performed in network device (switches, routers and gateways), but an ad hoc network does not have these types of network elements where the IDS can collect audit data for the entire network. A wired network under a single administrative domain allows for discovery, repair, response, and forensics of doubtful nodes. A MANET is most likely not under a single administrative domain, making it hard to perform any kind of centralized management or control.

Mobile Ad-Hoc Network (MANET) is one of the heterogeneous, self-organizing and self-configured infrastructures less Ad-hoc mobile network. So routing in the Mobile Ad-Hoc Network is very difficult one, and it does not have any topology so security and end to end time delay is also difficult.

Here, all the nodes are mobile nodes; static optimal path is not possible in this network. Dynamic optimal path is only possible.

II. LITERATURE SURVEY

Naincy Juneja, *et al* [8] - 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) [9]- 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)[10] - 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)[11] - 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* [12]- 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.
Sunil Taneja *et al* [14] : Key management is the process by which cryptographic keys are manipulated(generated, stored, protected, transferred, loaded, used, and destroyed). The data packet will be transmitted from source to destination over transmission media using efficient cryptographic algorithm to encrypt the entire packet.
Rajdeep S. Shaktawat *et al*[15]: This author's algorithm uses a fully distributed authority approach in which every node in network has its own itself certifying authority. Whenever a node enters into the network during its boot time it will generate two set of public and private key and make a communication.
A. Jegatheesan *et al* [16]: This scheme shares the key between source and destination which is more resistant against internal and external attacks. The design of our scheme offers strong privacy protection – complete unobservability, unlinkability and anonymity – for ad hoc networks.
Vishakha Singhal *et al* [17]: The sensor network is splitting into clusters with cluster head for each cluster. We assume that each sensor node has a unique ID The cluster leader or cluster head knows the IDs of its sensor node in its cluster. The nodes in its cluster transmit the information or data to the cluster leader or cluster head in place of sending data immediately to the sink or destination node.
K.S.Abitha *et al* [18]: according to this work it increases security considerations of the network using AODV algorithm for transfer of data and to increment the efficiency of AODV algorithm using ECC(Elliptic Curve Cryptography). Reliability and Efficiency will be increased in each transmission, while enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and

decrypt the data that is to be transferred and performs the active classification

S. Abila Judith Suganthi *et al* [19]: The more nodes cooperate to transfer traffic, the more powerful a MANET gets. Detecting routes and forwarding packets consumes network bandwidth, local CPU time, memory, and least energy. In this work, author found the dropping packets for optimal estimation by using path tracing algorithm in reputed AODV.

Xiaoxia Qi [20] *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 [21] *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 we can analyze the packet size of Wi-MAX based MANET.

Kewal Vora [22] et al Flooding attack in MANET results in exhaustion of battery power, degradation of throughput and wastage of bandwidth. In this paper, we have 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.

Nand Kishore [23] 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 [24] *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.

III. 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 [4] 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.

E. *Stage 5:*

The *SIm AODV* [5] 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* [6] 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[18][19] and parity bit check.

G. Stage 7:

The OpTiB AODV [7] 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 in this paper is concentrate to combine En-SIm AODV and OpTiB AODV with intruders. So this proposed HiLeSec-OpTiB AODV is evaluated

IV. 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.

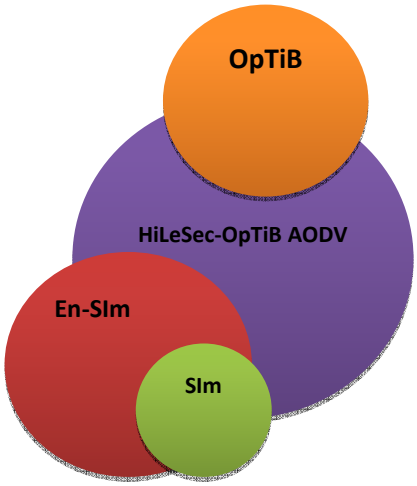


Fig 3. High Level Security – Optimal Time Bound AODV (HiLeSec–OpTiB AODV)

A. HiLeSec-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 Optimal route(OptRout) Table;
Step 32 : sort(OptRout);
Step 32 : Loop Start Optimal Path from 0 to 9
Step 33 : Packet Add (OptRout.R_No, OP, dpkt[OP]);
Step 34 : Loop End Optimal Path
Step 35 : Packet Count (pk=0)
Step 36 : Loop Optimal Path from 0 to 9
Step 37 : Packet Send (pktSend(OptRout[OP], dpkt[OP]))
Step 38 : dpkt[OP].Send_Status=true;
Step 39 : Increment Packet Count(pk++)
Step 40 : Loop End Optimal Path
Step 41 : Calculate next packet
Step 42 : Check received packet is Host Neighbor Reply(HNREP) then Step 43 else Step 44
Step 43 : Update Link Time Table (L2T)
Step 44 : Check Received Packet is Route Error (RERR) then Step 45 else Step 50
Step 45: loop Start Optimal Route
Step 46 : Check is (RERR.Dest_SeqNo== OptRout.Dest_SeqNo) then Step 47 else Step 49
Step 47 : Delete entry;
Step 48 : sort Optimal Route
Step 49 : Loop End Optimal Route
Step 50 : Check is Packet Acknoledment then Step 51 else Step 54
Step 51 : loop Start one(dpkt[pk] to dpkt[rpk])
Step 52 : update all sent packet status
Step 53 : loop End one
Step 54 : Loop: end Base
Step 55 : End

V. 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.

VI. 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.4. a., 4. b.

A. 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 HiLeSec-OpTiB AODV
Simulation Time	600s

B. *Simulation Outputs*

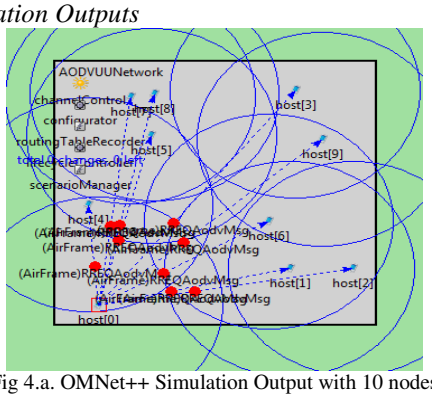
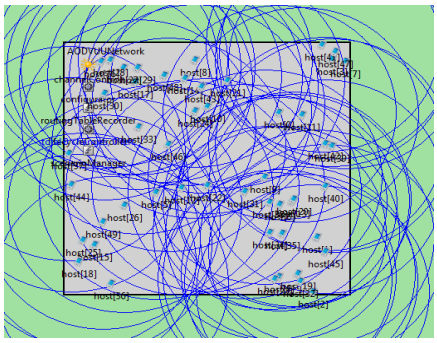


Fig 4.a. OMNet++ Simulation Output with 10 nodes



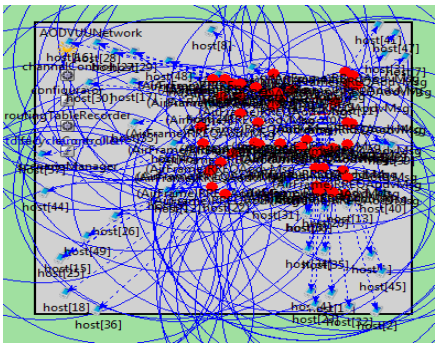


Fig 4.b. OMNet++ Simulation Output with 50 nodes

Above two figures 4.a and b show the simulation output initial stage to packet communication. In this simulation after the *Path Discover* each and every node has to send three packets of data.

VII. RESULTS AND DISCUSSION

A. *Packet Delivery Ratio (PDR) without Malicious Nodes*

The following two tables show the result without malicious nodes. So the PDR is more in HiLeSec-OpTiB compare to AODV. Like the End to end time delay also is low.

Table 2. Packet Delivery Ratio

No. of Nodes	Total Packets	AODV (PPs)	SIm AODV (PPs)	En-SIm AODV (PPs)	OpTiB AODV (PPs)	HiLeSec-OpTiB AODV (PPs)
10	30	18	25	24	19	23
20	60	40	42	40	41	42
30	90	60	83	78	58	81
40	120	96	109	102	95	107
50	150	121	145	130	120	141

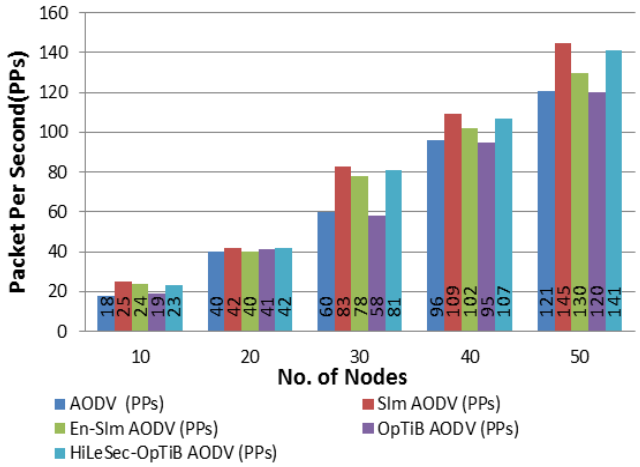


Fig5.. Packet Delivery Ratio

B. *End to End Time Delay without Malicious Nodes*

Table 3. End to End Time Delay

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

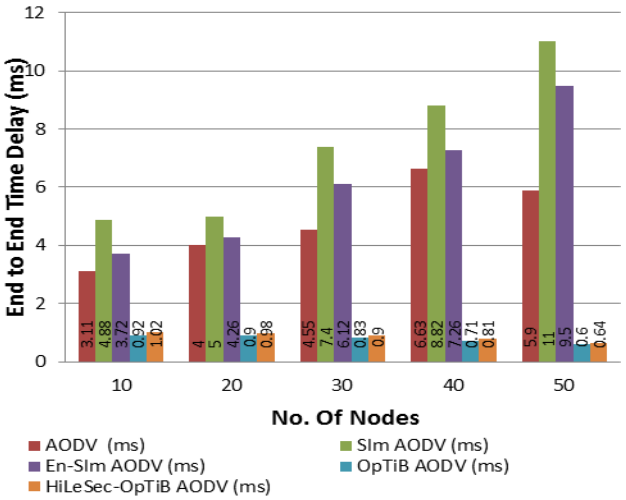


Fig 6. End to End Time Delay

The following two result show with 20% of malicious nodes. The result shows some percentage of packet delivery is low as well as the time taken is little bit more compare to the without malicious node result.

C. Packet Delivery Ratio (PDR) with Malicious Nodes

Table 4. Packet Delivery Ratio

No. of Nodes	Total Packets	No. Of Malicious Nodes	AODV (PPs)	SIm AODV (PPs)	En-SIm AODV (PPs)	OpTiB AODV (PPs)	HiLeSec-OpTiB (PPs)
10	30	2	14	23	23	16	22
20	60	4	32	38	38	35	41
30	90	6	48	75	74	49	79
40	120	8	77	98	97	81	104
50	150	10	97	131	124	102	137

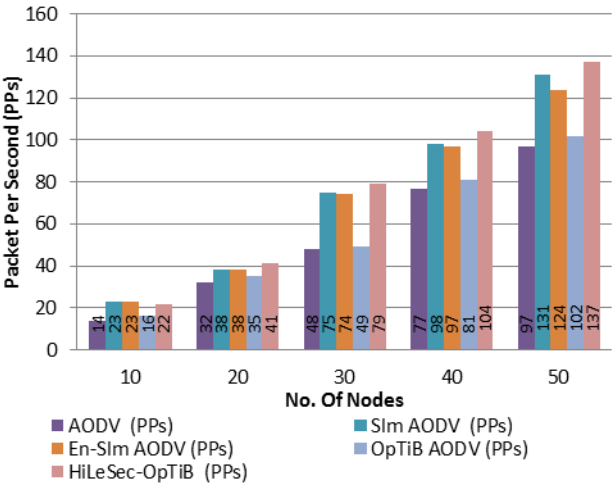


Fig 7. Packet Delivery Ratio

D. End to End Time Delay with Malicious Nodes

Table 5. End to End Time Delay

No. of Nodes	No. of Malicious Nodes	AODV (ms)	SIm AODV (ms)	En-SIm AODV(ms)	OpTiB AODV (ms)	HiLeSec-OpTiB AODV (ms)
10	**2**	3.732	5.124	3.98	1.104	1.061
20	**4**	4.8	5.25	4.558	1.08	1.019
30	**6**	5.46	7.77	6.548	0.996	0.936
40	**8**	7.956	9.261	7.768	0.852	0.842
50	**10**	7.08	11.55	10.165	0.72	0.666

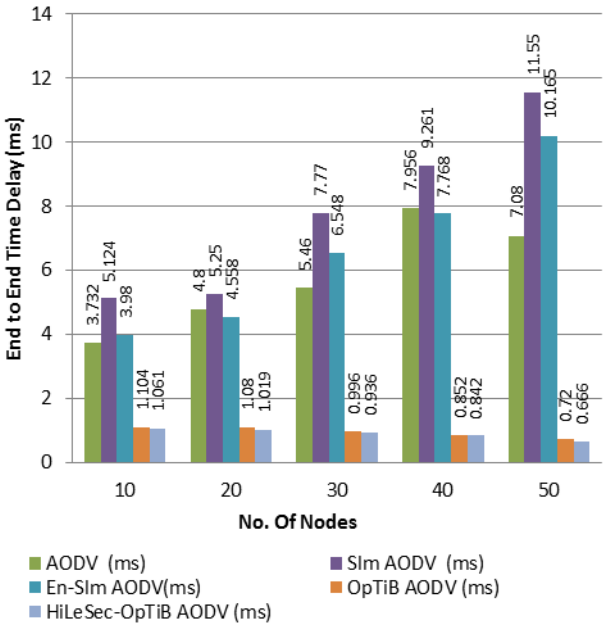


Fig 8. End to End Time Delay

VIII. CONCLUSION

The HileSec-OpTiB is the combination of En-SIm AODV and OpTiB AODV with intruders. This algorithm provides averagely 1.4 times higher packet delivery ratio and 6.8 times lesser end to end time delay under author's simulation scenario.

IX. FUTURE ENHANCEMENT

HiLiSec-OpTib algorithm 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]. Singh, Umesh Kumar, et al. "An Overview and Study of Security Issues & Challenges in Mobile Ad-hoc Networks (MANET)." International Journal of Computer Science and Information Security, Volume-9, No-4 (2011), pp 106-110.

[2]. Nagendra, M., and B. Kondaiah. "A Comparison and Performance Evaluation of On-Demand Routing Protocols for Mobile Ad-hoc Networks." International Journal of Computer Sciences and Engineering, Volume-2, Issue-5 (2014) pp 15-19.

[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.

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

[6]. B..Karthikeyan, N.Kanimozhi 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, VOL. 11, NO. 2, JANUARY 2016

[7]. 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 (0975 – 8887) Volume 140 – No.6, April 2016

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

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

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

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

[12]. 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.

[13]. Dr.Mahmood K. Ibrahem , Ameer M. Aboud, "A Secure Routing Protocol for MANET", IJCSET, July 2014.

[14]. Sunil Taneja, Sima Singh, Ashwani Kush, "Encryption Scheme for Secure Routing in Ad Hoc Networks",IJICT, Vol 1, No 1, ISSN 0976- 4860,2011,PP 22-29.

[15]. Rajdeep S. Shaktawat, Dharm Singh, Naveen Choudhary, "An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE- AODV)",IJCA (0975 – 8887), PP 34-41. Volume 97– No.8, July 2014,

[16]. A. Jegatheesan, D. Manimegalai, "Secure Key Sharing in Mobile Ad hoc Network using Content Invisibility Scheme", WSEAS TRANSACTIONS on COMPUTERS, E-ISSN: 2224-2872, Volume 14, 2015,PP 124-133.

[17]. Vishakha Singhal and Shrutika Suri, "Comparative Study of Hierarchical Routing Protocols in Wireless Sensor Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-05, Page No (142-147), May -2014

[18]. K.S.Abitha, Anjalipandey, DR.K.P.Kaliyamurthie, "Secured Data Transmission Using Elliptic Curve Cryptography", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015,PP 1419-1425

[19]. S. Abila Judith Suganthi, P. Rajesh, "ENCRYPTION BASED INTRUSION DETECTION IN MANET USING AODV ROUTING PROTOCOL", Elysium Journal, P-ISSN: 2347-4408, Volume - 2, Issue – 2, April 2015.

[20].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

[21].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.

[22].Kewal Vora, Jugal Shah, Shreyas Parmar and Shivani Bhattacharjee, "MANETs: Overview of Vulnerabilities, Security Threats and Prevention and Detection Techniques", International Journal of Computer Sciences and Engineering, Volume-03, Issue-10, Page No (26-31), Oct -2015, E-ISSN: 2347-2693

[23]. Nand Kishore, SukhvirSingh and Renu Dhir, "Energy Related Issues for MANETs: A Study", International Journal of Computer Sciences and Engineering, Volume-02, Issue-03, Page No (98-100), Mar -2014

[24]. 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.

AUTHORS PROFILE

Mr B.Karthikeyan Bachelor of Science in Computer Science and Master of Science in information Technology from Bharathidasan University, india in year 2000 and 2002.Master of Philosophy in Computer Science form Bharadhidasan University,Trichy, India in the year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science, Bishop Heber College,Trichy,Tamilnadu, India since 2009. He has published more than 6 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Infrastructure Oriented and Infrastructure Less network, Mobile Ad Hoc Network routing protocols. He has 10 pulse years of teaching experience and 3 pulse years of Research Experience.