International Journal of Research in Advent Technology, Vol.3, No.12, December 2015
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Performance Analysis of Delay and Throughput using OLSR for Security of MANET

Unnati A. Dabre[1], Juned A. Khan[2]
Student, CSE Department (ME 2nd Yr)[1], Guide CSE Department[2]
GHRCEM Amravati (MH) India[1], GHRCEM Amravati (MH) India[2]
dabre_unnati.ghrcemamecse@raisoni.net[1], juned.khan@raisoni.net[2]

Abstract - As privacy is an important aspect of mobile Ad-hoc network (MANET). Due to fundamental characteristics, routing protocols in wireless mobile Ad-hoc networks (MANETs) are particularly vulnerable to attack. We are going to discuss some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Sourced Routing, Ad-hoc On Demand Distance Vector and OLSR (Optimized link state protocol). Security is essential requirement in MANET and as compared to wired network MANETs are more vulnerable to security attacks as they are less in infrastructure and autonomous. Main objective of this is to address the different MANET routing protocols and different kinds of attacks like black-hole attack in MANET. To detect & prevent that attack, we are going to implement RSA algorithm at protocol level. As security is big issue in MANET, it would be great help for the peoples who are conducting research for security & privacy problems in MANET. The simulation results will show effectiveness of our scheme. By using OLSR protocol we are going to analyses the performance parameter like throughput & delay. The design and evaluation of this network is rigorously detailed, its performance is evaluated.

Index Terms - Protocol, MANET, Attack, Throughput, Security.

1. INTRODUCTION

The secure protocol design and development has become the most challenging task in securing mobile ad hoc network. Most of the existing protocol has been develop based on specific security scenarios. So the primary reason for this examination is to comprehend and assess the current secure protocol and actualize a safe protocol. The network layer in MANETs is helpless to different attack viz. listening in with a malignant purpose, vindictive adjustment/modification of the bundle substance and the Denial-of-service (DoS) attack viz. Wormhole attack, Sinkhole attack, and Black-hole attack. Amongst these attacks, we endeavor in breaking down and enhancing the security of the routing protocol OLSR against the Black-hole using so as to open attack RSA calculation.

In our project we focus on the Optimized Link State Routing protocol and devise a feedback reputation mechanism. This mechanism assesses the integrity of routing control traffic by correlating local routing data with feedback messages sent by the receivers of control traffic. Based on this assessment, mis-behaving nodes are reliably detected and they can be adequately punished in terms of their ability to communicate through our network. In this project, we have designed a novel method to secure attack. This isolates the malicious node from the network.

2. BRIEF LITRETURE SURVEY

A mobile adhoc network (MANET) is an arrangement of mobile nodes which impart over radio and needn't bother with any base. These sorts of networks are exceptionally adaptable and suitable for a few circumstances and applications, along these lines they

permit the building up of makeshift correspondence without pre introduced framework. Because of the restricted transmission scope of remote interfaces, the correspondence movement must be handed-off more than a few moderate nodes to empower the correspondence between two nodes. Thusly, this sort of networks is additionally called mobile multi-bounce specially appointed networks [1][8][13].

2.1. *AODV*

AODV is a reactive protocol in which the routes are made just when they are required. It utilizes protocol routing tables. In AODV, when a source node sends information movement to a destination node, firstly it starts a route revelation process. In AODV, when a source node sends information activity to a destination node, firstly it starts a route discovery process. In this procedure, the source node telecasts a Route Request (RREQ) parcel. Neighbor nodes which don't have the foggiest idea about a dynamic route for the asked for destination node forward the parcel to their neighbors until a dynamic route is discovered or the most extreme number of jumps is come to. At the point when a middle of the road node gets the dynamic route to the asked for destination node, it sends a Route Reply (RREP) parcel back to source node in unicast mode. In the end, the source node gets the RREP parcel and opens the route [15].

The route discovery technique for AODV depends on routing tables which store the routes toward numerous destinations. Every destination is demonstrated utilizing just the following jump node to achieve this destination. The source disperses a Route REQuest (RREQ) to its neighbors which thusly sends the same parcel to their neighbors et cetera, until the last destination is come to. When the route demand achieves the destination or a middle node which knows the way toward the destination, a Route Replay (RREP) is sent back to the source node through the opposite route. AODV utilizes a grouping number to find crisp ways and to avert routing circles.

2.2. *OLSR*

OLSR is a proactive routing protocol for mobile adhoc networks. The protocol inherits the stability of the link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR minimizes the overhead brought on by using so as to flood of control activity just chose nodes, called Multi-Point Relays (MPR), to retransmit control messages. This method fundamentally diminishes the quantity of retransmissions required to surge a message to all nodes in the network. After accepting an overhaul message, the node decides the routes (grouping of bounces) toward its known nodes. Every node chooses its MPRs from the arrangement of its neighbors spared in the Neighbor list. The set spreads nodes with a separation of two bounces. The thought is that at whatever point the node shows the message, just the nodes incorporated into its MPR set are in charge of television the message. OLSR utilizes HELLO and TC messages. The Topology Control (TC) messages for nonstop keep up of the routes to all destinations in the network, the protocol is extremely productive for activity designs where an extensive subset of nodes is speaking with another substantial subset of nodes, and where the [source, destination] sets change after some time. The HELLO messages are traded intermittently among neighbor nodes, to recognize the personality of neighbors and to flag MPR determination. The protocol is especially suited for huge and thick networks, as the enhancement is finished by utilizing MPRs which function admirably as a part of this setting. The bigger and more thick a network, the more enhancement can be accomplished when compared with the fantastic connection state calculation. OLSR uses bounce by-jump routing, i.e., every node utilizes its nearby data to route bundles [14].

2.3. PSR

Zehua Wang, Yuanzhu Chen, Cheng Li propose a Proactive source routing, a lightweight proactive source routing (PSR) protocol to encourage shrewd information sending in MANETs. In PSR, every node keeps up an expansiveness first hunt spreading over tree of the network established at itself. This data is occasionally traded among neighboring nodes for upgraded network topology data. In this manner, PSR permits a node to have full-way data to every other node in the network, despite the fact that the correspondence expense is just straight to the quantity of the nodes. This permits it to bolster both source routing and ordinary IP sending. While doing this, we attempt to decrease the routing overhead of PSR as much as we can. its simulation results show that PSR has just a small amount of overhead of OLSR, DSDV, and DSR yet at the same time offers a comparative or better information transportation capacity compared and these protocols[14].

3. MOTIVATION

Security in Mobile Ad-hoc Network is the most critical sympathy toward the fundamental usefulness of network. Accessibility of network services, secrecy and respectability of the information can be accomplished by guaranteeing that security issues have been met. MANET regularly experience the ill effects of security attack as a result of its elements like open medium, changing its topology progressively, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the scenario for the Mobile Ad-hoc Networks against the security threats.

MANET is not confined up to Mobile-to-Mobile correspondence, it takes advantages of street side foundation that can likewise take an interest in correspondence between vehicles [5], however in this dessertation the primary center is on Mobile-to-Mobile correspondence. There are different sorts of conceivable attack on MANETs. It is basic that MANET security ought to be equipped for taking care of each kind of attack. MANET security is not quite the same as that of remote and wired networks in view of its special attributes of versatility limitations, foundation less structure, and brief length of time of connection between nodes. In a wired network, foundation has segments for particular capacities for instance switches choose the route to destination while network hosts send and get messages. Security execution is generally simple as networks should be physically altered for spying. Remote networks use infrared or radio recurrence signs to convey among gadgets. MANETs are mobile they make utilization of remote connections to join different networks. MANETs are a sort of Wireless specially appointed network that typically has a vigorous networks service environment on top of an association layer adhoc network. Each device continuously maintains the

information connected to larger Internet. OLSR has less average end2end delay, OLSR implementation is more user friendly and work with less headaches.

4. PROBLEM DEFINITION

There are number of security imperfections in Adhoc Network in light of their evolving topology, high power utilization, high mistake rates. The Attacker can undoubtedly attack on routing protocol by not acting like detail of protocol. Attack is one of the security dangers in Ad-hoc Network. By recovering so as to keep attack or from attack, network ought to give execution closer to unique.

A black hole attack is an extreme attack that can be effectively utilized against routing in mobile specially appointed networks. A black hole is a noxious node that erroneously answers for any route asks for without having dynamic route to indicated destination and drops all the getting bundles. On the off chance that these malevolent nodes cooperate as a gathering then the harm will be intense. This kind of attack is called helpful black hole attack. In this paper, we are actualizing Black hole attack considering the routing protocol: Ad-hoc On Demand Vector Routing Protocol (AODV) assesses the network execution measurements like throughput, Average end-end Delay. The Experiment demonstrate that Implementation of AODV, OLSR, PSR for MANET without Black hole attack, with, many attacks for MANET. MANET experiences Comparison of AODV OLSR, PSR without Black hole attack and with Black hole attack as far as Network Performance Metrics. After this we have to enhance execution of OLSR by decreasing e2edelay and expanding Throughput for security of MANET.

5. OBJECTIVES

The secure protocol outline and advancement has turned into the most difficult undertaking in securing mobile specially appointed network. A large portion of the current protocol has been crete taking into account particular security situations. So the fundamental motivation behind this examination is to comprehend and assess the current secure protocol and execute a secure protocol. The network layer in MANETs is helpless to different attack. spying with a vindictive plan, malignant adjustment/modification of the bundle substance and the Denial-of-service (DoS) attack. Wormhole attack, Sinkhole attack, and Black-hole attack. Amongst these attacks, we endeavor in breaking down and enhancing the security of the routing protocol OLSR against the Black using so as to open attack RSA calculation.

6. WORKING

Reproduction can characterized as "Evaluating how occasions may happen in a genuine circumstance". It can include complex scientific demonstrating, pretending without the guide of innovation. The significance of recreation lies in the thought of reasonable conditions that change as consequence of conduct of others included diverse test networks, for example, NS2, GloMoSim, OPNET and so on. I have utilized NS2 for the assessment of proposed routing protocol as the same is an open source, uninhibitedly accessible and the programming dialect utilized is tcl.

(1) Implementation of OLSR:
In this module we will actualize the olsr protocol and compute throughput, and e2edelay for 10 nodes to 50 nodes.

(2) Implementation of AODV*:*
In this module we will actualize the AODV protocol and compute throughput, and e2edelay for 10 nodes to 50 nodes.

(3) Implementation of PSR:
In this module we will actualize PSR protocol and compute throughput, and e2edelay for 10 nodes to 50 nodes.

(4) Performance Comparisons:
In this module we are going to contrast throughput of OLSR and AODV and PSR graphically, end 2 end postponement of OLSR with AODV and PSR graphically.

(5) Attack*:*
In this module we will execute black hole attack to protocol and think about the execution before and after attack. and build the security by applying RSA Algorithm.

6.1. *OLSR implementation*

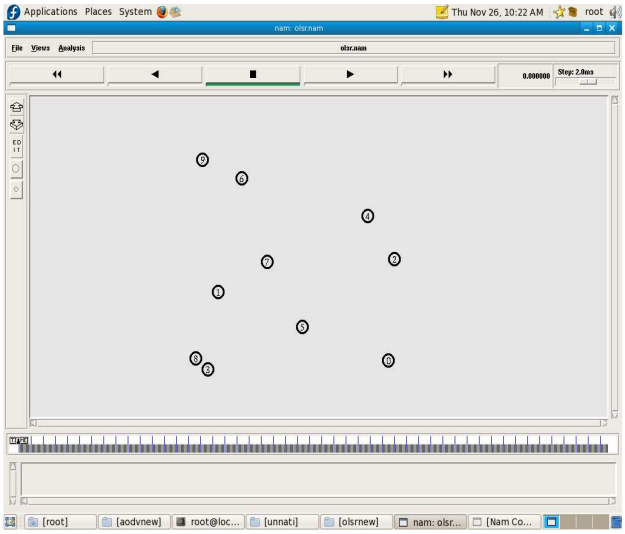

Fig 6.1 Normal OLSR Implementation

6.2. *BLACK HOLE attack implementation on OLSR*

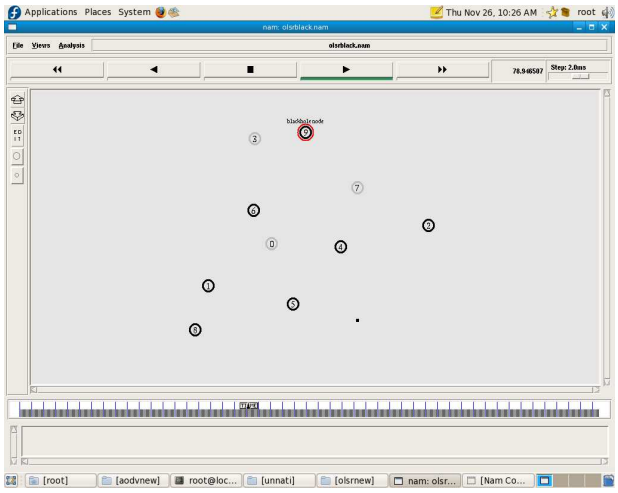

Fig 6.2 Black Hole Attack on OLSR

6.3. *Secure OLSR implementation*

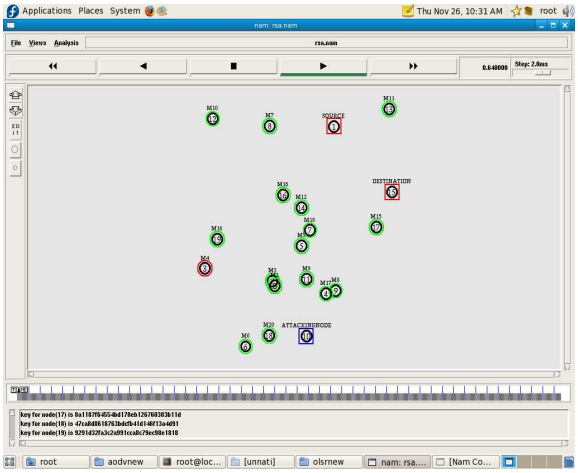

Fig 6.3 Secure OLSR Implementation

7. ANALYSIS & RESULT

7.1. *Throughput*

Throughput refers to the performance of tasks by a computing service or device over a specific period. It measures the amount of completed work against time consumed and may be used to measure the performance of a processor, memory and network communications. It can be represents Bits per Second. Throughput is the number of successfully received packets in a unit time and it is represented in bps. Throughput is calculated using awk script which processes the trace file and produce result.

Throughput Formula: Throughput = File Size / Transmission Time (bps)

Table 7.1 Throughput for OLSR

No. Of Nodes	Throughput (in kbps)		
	OLSR	With Black hole Attack	After RSA (secure)
10	35.78	33.38	45.89
20	39.01	33.34	48.70
30	43.69	35.53	48.78
40	54.32	37.40	55.45
50	50.42	33.17	53.78

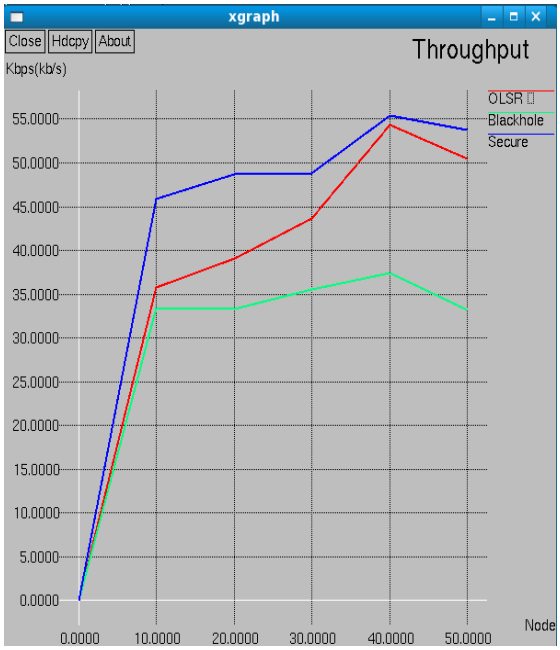

Fig 7.1 Throughput comparison graph for OLSR

Table 7.2 Throughput for AODV

No. Of Nodes	Throughput (in kbps)		
	AODV	With Black hole Attack	After RSA (secure)
10	39.41	2.20	41.34
20	39.35	5.09	40.04
30	39.47	4.00	39.88
40	39.60	10.79	40.09
50	39.02	4.36	40.04

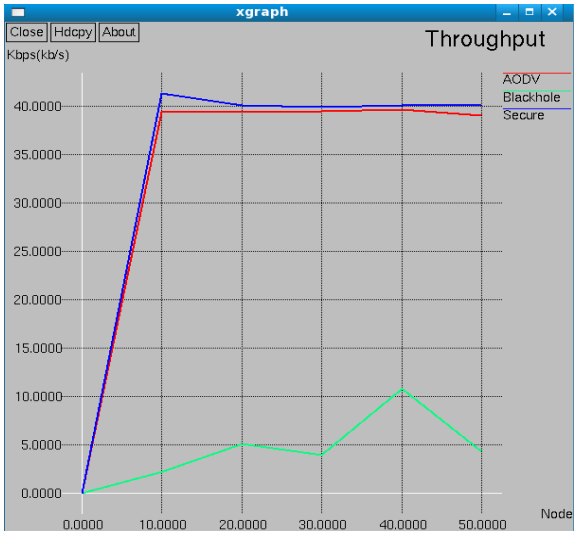

Fig 7.2 Throughput comparison graph for AODV

Table 7.3 Throughput for PSR

No. Of Nodes	Throughput (in kbps)		
	PSR	With Blackhole Attack	After RSA (secure)
10	35.78	14.82	36.71
20	25.80	14.66	34.53
30	26.66	17.98	34.78
40	28.45	16.08	35.25
50	21.45	14.08	36.71

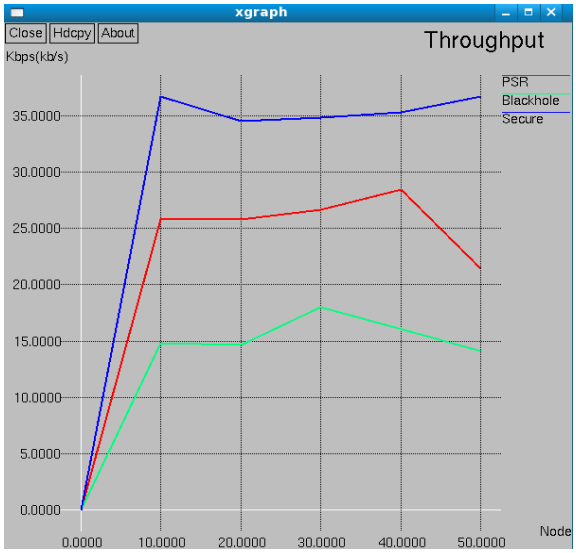

Fig 7.3 Throughput comparison graph for PSR

7.2. *End-to-End Delay*

Delay is the difference between the time at which the sender generated the packet and the time at which the receiver received the packet. Delay is calculated using awk script which processes the trace file and produces the result.

End-to-end Delay: The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$\sum$ (arrive time – send time) / $\sum$ Number of connections

Table 7.4 e2edelay for OLSR

No. Of Nodes	e2eDelay		
	OLSR	With Black hole Attack	After RSA (secure)
10	0.00454489	0.0144057	0.0160893
20	0.00354863	0.00453519	0.00767512
30	0.00588701	0.0145554	0.00742778
40	0.019225	0.0404557	0.00757782
50	0.0316397	0.0776673	0.00743378

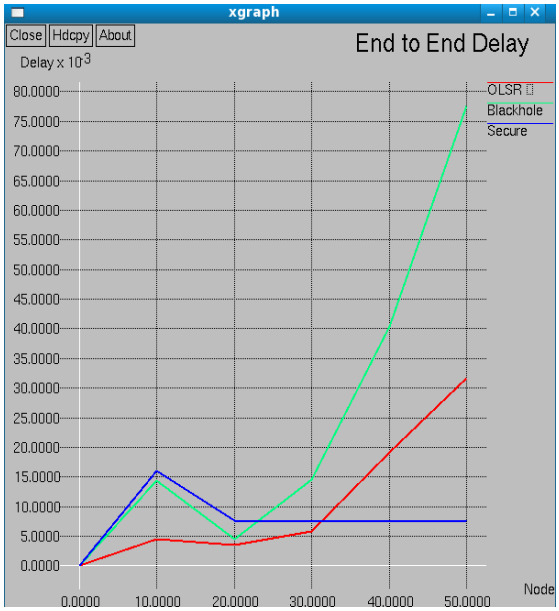

Fig 7.4 e2edelay comparison graph for OLSR

No. Of Nodes	e2eDelay		
	AODV	With Black hole Attack	After RSA (secure)
10	0.00395289	0.115249	0.00365289
20	0.0204162	0.260438	0.0393875
30	0.0250854	0.214167	0.036629
40	0.0301106	0.215386	0.00410549
50	0.0205409	0.153847	0.292965

Table 7.5 e2edelay for AODV

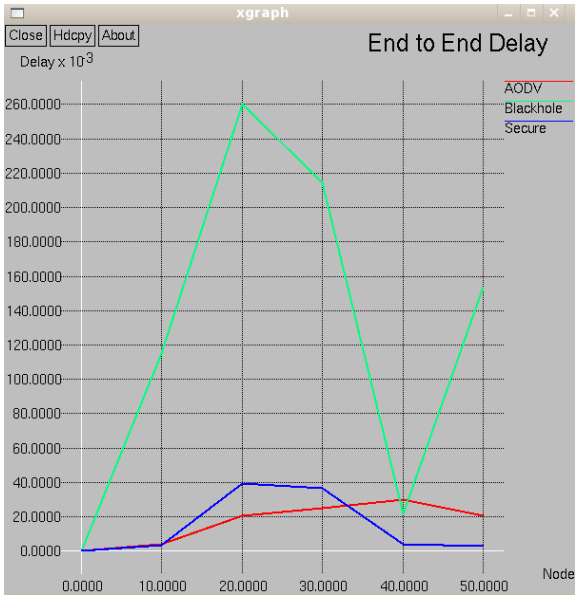

Fig 7.5 e2edelay comparison graph for AODV

No. Of Nodes	e2eDelay		
	PSR	With Black hole Attack	After RSA (secure)
10	0.0185978	0.0285978	0.00791615
20	0.0187938	0.00725447	0.00891615
30	0.00883213	0.0266979	0.00791615
40	0.0084623	0.03647205	0.00691615
50	0.0078153	0.02741481	0.00747815

Table 7.6 e2edelay for PSR

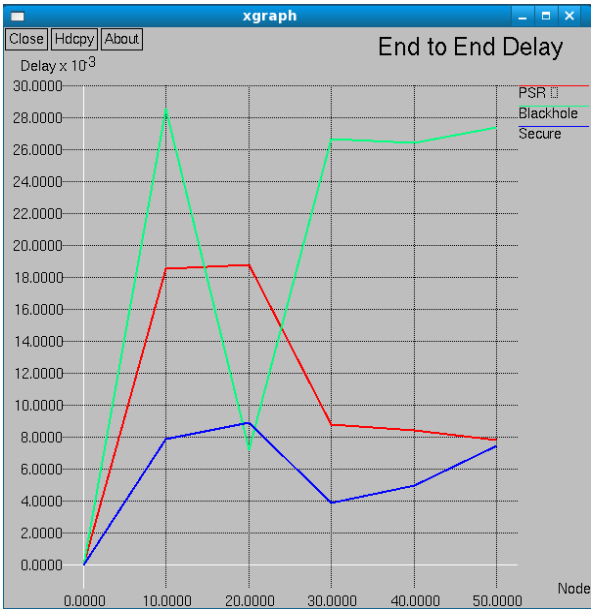

Fig 7.6 e2edelay comparison graph for PSR

8. CONCLUSION

From above we are trying to detect the attack in and prevent them by applying the algorithm on MANET protocol. The performance of above can be measured by implementing this protocol and after applying algorithm it will provide security.

From these we conclude that, the performance of our network can improve and it helps the researcher for their future research. Because of this algorithm we can send the data securely. Beyond providing a natural solution for these security problems, our practical scheme is resistant to general problems of reputation networks. Specifically, we are able to eliminate the dissemination of reputation information throughout the network, and make it impossible for nodes to accuse or praise other nodes falsely. This would require them either to generate false feedback messages or to repeat old feedback messages. Due to it Manet protocol gives better result by preventing them by applying security

REFERENCES

[1] Ismail Butun, Salvatore D. Morgera and Ravi Sankar:A Survey of Intrusion Detection Networks in Wireless Sensor Networks, IEEE Communications Surveys & Tutorials, Vol. 16, No.1, First Quarter 2014.

[2] Luoyi Fu,Yi Qin, Xinbing Wang, and Xue Liu, :Throughput and Delay Analysis for Convergecast with MIMO in Wireless Networks,IEEE Transaction on Parallel and Disrtibuted Networks, Vol. 23, No.4, April 2012.

[3] Zehua Wang, Yuanzhu Chen, and Cheng Li:PSR: A Lightweight Proactive Source Routing Protocol

For Mobile Ad Hoc Networks,IEEE Transaction on Vehicular Technology, Vol. 63, No.2, February 2014.

[4] Dorus R. and Vinoth P.: Mitigation of Jamming Attack in Wireless Networks,IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, Vol. 32, No.22, March 2013.

[5] Sreedhar S.:An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks,InternationalConferenceonMicroelectronics, Communication and Renewable Energy, Vol. No.10, June 2013.

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, :Routing Security in Wireless Ad Hoc Networks," IEEE Communications Magazine, October 2002, pages 70-75.

[7] Douglas S. J. De Couto, Daniel Aguayo, John Bicket and Robert Morris:A High-Throughput Path MetricforMulti-HopWireless Routing, AICERA/ICMiCR, Sept 2003.

[8] J. Raymond:Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.

[9] Y.-C. Hu, A. Perrig, and D.B. Johnson, Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks, Wireless Networks, vol. 11, pp. 21-38, 2005.

[10] Yongguang Zhang and Wenke Lee:Intrusion Detection in Wireless Ad-Hoc Networks,International Conference on Mobile Computing and (MOBICOM'00), pp275-283, June 2000.

[11] Elizabeth M. Royer and Chai Keong Toh,:A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks, IEEE Personal Communications, Volume 6, pp46-55, April 1999.

[12] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker:Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, In Proceedings of Mobicom, August 2000.

[13] Sonali Bhargava and Dharma P. Agrawal, :Security Enhancements in AODV protocol for Wireless Ad Hoc Networks, In Proceedings of Vehicular Technology Conference, 2001.

[14] Zhan Haawei, Zhou Yun:Comparison and analysis AODV and OLSR Routing Protocols in Ad Hoc Network, Wireless Communications, Networking, and Mobile Computing International Conference, WiCOM 08, Oct 2008.

[15] P. Gowrisankar, N. Srinivasulu, dr.ch. Balaswamy, :Design and Implementation of Black hole attack in AODV Routing protocol for Mobile Adhoc Network, International Journal of Advance Research in Computer and Communication Engineering. Vol.2,Issue12, Dec2013.

[16] X. Hong, M. Gerla, G. Pei, and C.C. Chiang:A Group Mobility Model for Ad Hoc Wireless Networks,Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Networks (MSWiM), 1999.

[17] K.C. Lee, J. Haerri, L. Uichin, and M. Gerla, :Enhanced Perimeter Routing for Geographic Forwarding Protocols in Urban Vehicular Scenarios, Proc. IEEE GlobeCom Workshops, 2007.

[18] X. Wu:DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles, Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.