Volume 4, No. 2, February 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

DETECTION AND PREVENTION ROUTING MISBEHAVIOUR IN OLSR ROUTING

Anita Namdev[1], Vineet Richhariya[2], Vivek Richhariya[3]
[1]M.Tech Scholar, Software Engineering, Laxmi Narayan College of Technology, Bhopal (M.P.) India
anitanamdev0103@gmail.com
[2]Professor & HOD of Computer Science & Engineering, LNCT, Bhopal (M.P.) India
vineet_rich@yahoo.com
[3]Asstt. Professor of Computer Science & Engineering, LNCT, Bhopal (M.P.) India
vivekrich@yahoo.com

Abstract- Mobile ad-hoc network are temporally network that form self controlled system with each node contain routing table but measure issue of that topology management of network because each node freely moves, in our simulation we use OLSR (optimal link state routing) that provide MANET route request flood and maintenance of routing but one is the measure challenge is security issue in mobile ad-hoc network, in this paper we proposed intrusion prevention system that protect the network through routing misbehaviour as well as congestion attack or denial of service attack, here we simulate the behaviour of normal OLSR routing , Un-trusted network and prevention system after that we conclude our prevention system provide more secure and reliable communication and increases data delivery ratio.
In this method we analyze the behaviour of network through network simulator-2 and get result of the network.

Keywords- Routing Load, Packet Delivery Ratio, attack, OLSR, congestion.

INTRODUCTION

Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ‘‘ad-hoc’’ network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g., disaster recovery environments. Ad hoc networking concept is not a new one, having been around in various forms for over 20 years. Traditionally, tactical networks have been the only communication networking application that followed the ad hoc paradigm. Recently, the introduction of new technologies such as the Bluetooth, IEEE 802.11 and Hyper LAN are helping enable eventual commercial MANET deployments outside the military domain. These recent evolutions have been generating a renewed and growing interest in the research and development of MANET [8].
An ad hoc network can be formed on-the-fly and spontaneously without the required intervention of a centralised access point or an existing infrastructure [9].

The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: firstly, the wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering; secondly, the lack of an online CA or Trusted Third Party adds the difficulty to deploy security mechanisms; thirdly, mobile devices tend to have limited power consumption and computation capabilities which makes it more vulnerable to Denial of Service attacks and incapable to execute computation-heavy algorithms like public key algorithms; fourthly, in MANETs, there are more probabilities for trusted node being compromised and then being used by adversary to launch attacks on networks, in another word, we need to consider both insider attacks and outsider attacks in mobile ad hoc networks, in which insider attacks are more difficult to deal with; finally, node mobility enforces frequent networking reconfiguration which creates more chances for attacks, for example, it is difficult to distinguish between stale routing information and faked routing information.

There are five main security services for MANETs: authentication, confidentiality, integrity, non-repudiation, availability. Authentication means that correct identity is known to communicating partner; Confidentiality means certain message information is kept secure from unauthorized party; integrity means message is unaltered during the communication; non-repudiation means the origin of a message cannot deny having sent the message; availability means the normal service provision in face of all kinds of attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system. Without knowing exactly who you are talking with, it is worthless to protect your data from being read or altered. Once authentication is achieved in MANET, confidentiality is a matter of encrypting the session using whatever key material the communicating party agrees on. Note that these security services may be provided singly or in combination [10-11].

RELATED WORK

Here we are presenting survey about existing work done in the field of MANET security.

Lalith Suresh P.1, Rajbir Kaur et al. in his work titled “Collusion Attack Resistance Through Forced MPR Switching in OLSR” [2] In this work, they propose a novel attack resistant method named Forced MPR Switching

OLSR (FMS-OLSR), in which, whenever a node observes symptoms of the attack, it temporarily blacklists potential attackers. This forces re-computation of its MPR set, thus, avoiding the attack.

Sterne et al. proposed "a dynamic intrusion detection hierarchy that is potentially scalable to large networks use clustering" [3]. This method use two levels, nodes on first level are cluster heads, while nodes on the second level are *leaf nodes*. In this model, every node has the task to monitor, log, analyze, respond, and alert or report to cluster heads.

Nora Cuppens-Boulahia et al. proposed "Property Based Intrusion Detection to Secure OLSR" [4]. In this method, they examine security issues related to proactive routing protocols for Mobile Ad-hoc Networks (MANETs). Specifically, they investigate security properties of the Optimized Link-State Routing (OLSR) Protocol, a proactive routing protocol for MANETs. They analyze the possible attacks against the integrity of the network routing infrastructure, and present techniques to counter some attacks. Researcher main approach is based on a formal model to describe normal and incorrect node behaviours.

S.Tamilarasan et al. proposed "A Quantitative Study and Comparison of Secure OLSR Routing Protocol "[5]. This work presents the comparison of the secure OLSR (Optimized Link State Routing Protocol) in mobile ad-hoc network with other approach. They compare the security from the different approach and their effect on the existing OLSR. The Main aim of this research is to study the various securities and compare the different attacks in MANET.

M. Wang, L. Lamont et al. proposed "An Effective Intrusion Detection Approach for OLSR MANET Protocol" [6]. In this method, they describe security threats to the OLSR MANET routing protocol and present an intrusion detection solution based on protocol semantics checking. That approach is based on semantic properties that are implied in the protocol definition and specify the correct OLSR routing update behaviour. Conflict checking based on semantic properties is applied in every MANET node. Any abnormal protocol semantics will trigger an intrusion alarm. While they use OLSR as an example, they argue that the presented approach can be applied to any Multi-Point Relay (MPR) proactive MANET protocol.

Thomas Clausen, Ulrich Herberg, proposed "Vulnerability Analysis of the Optimized Link State Routing Protocol version 2" [7]. researcher takes an abstract look at the algorithms that constitute the Optimized Link State Routing Protocol version 2 (OLSRv2), and identifies for each protocol element the possible vulnerabilities and attacks – in a certain way, provides a "cookbook" for how to best attack an operational OLSRv2 network, or for how to proceed with developing protective countermeasures against these attacks.

Ziming Zhao et al in his work titled "Risk-Aware Response for Mitigating MANET Routing Attacks" [12]. In this paper, they propose a risk aware response mechanism to systematically cope with the identified routing attacks. Our risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of *importance factor*.

Marjan Kuchaki Rafsanjani et al. proposed "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes" [13]. In this paper, they classify the architecture for Intrusion detection systems that have so far been introduced for MANETs, and then existing intrusion detection techniques in MANET presented and compared.

Jiejun Kong et al. in his work titled "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks" [14]. In this work researcher propose a feasible adversary model of such attacks, then present several instantiations and study the principles of designing corresponding countermeasures, they conclude that ad hoc networks deployed in hostile environments need new countermeasures to resist such passive attacks.

Amrit Suman et al. proposed "A Behavioral Study of Wormhole Attack in Routing for MANET" [15]. This paper presents an analysis of three routing protocols within wireless network where wormhole attack is occurred. By different analysis it can be observed that AODV performs better than other two protocols. AODV has better techniques to prevent data from attacks. In some conditions DYMO and FISHEYE performs better. But in all other conditions AODV perform better in different situations

PROBLEM STATEMENT

Our aim to detect malicious node and malicious activity through the novel IPS system that detect and protect the routing attack in OLSR protocol

In the field of mobile ad hoc networks routing protocols, there are lot of problems to be tackled such as Quality of service, power awareness, routing optimization and security issues. My main interest is in the security issues related to routing protocols in MANETs. Here we work on the routing misbehaviour node detection. The routing deviator or misbehaviour node, certainly get response to any sender node whose spread the routing packet and if sender node send data packet so that misbehaviour node capture all the data packet and significantly degrades the performance of the network [1].

After that we apply IPS-OLSR (intrusion prevention system in optimal link state routing) that IPS node protect from routing misbehaviour node and also detect misbehaviour node, that module provide the secure communication between sender to receiver. All above work done through network simulator to and analyze the result according to performance metrics.

WHY WE ANALYZE ATTACK ANALYSIS UNDER OLSR ROUTING

OLSR is a flat routing protocol, it does not need central controller system to handle its routing process. The table driven characteristic of the protocol provides that the

protocol has all the routing information to all participated hosts in the network.
The reactiveness to the topological changes can be adjusted by changing the time interval for broadcasting the routing messages. It increases the protocols suitability for ad hoc network with the rapid changes of the source and destinations pairs. Also the OLSR protocol does not require that the link is reliable for the control messages, since the messages are sent periodically and the delivery does not have to be sequential. [17, 18]

Due to the OLSR routing protocol simplicity in using interfaces, it is easy to integrate the routing protocol in the existing operating systems, without changing the format of the header of the IP messages. The protocol only interacts with the host's Routing Table. [17, 18] OLSR protocol is well suited for the application which does not allow the long delays in the transmission of the data packets. The best working environment for OLSR protocol is a dense network, where the most communication is concentrated between a large number of nodes.

OLSR has also extensions to allow for hosts to have multiple OLSR interface addresses and provide the external routing information giving the possibility for routing to the external addresses [16]. Based on this information there is possibility to have hosts in the ad hoc network which can act as gateways to another possible network. That's why we use OLSR routing and protect from mis-activity in the network.

ALGORITHM FOR OLSR-IPS

Here we describe algorithm of route misbehaviour prevention through IPS (intrusion prevention system), very first we create internal module of IPS that call through TCL script and create mobile node, here we create node s as IPS node that watch to all neighbour or radio range node for their activity and store there activity on the s node after that s node analyze each routing packet, if packet updated via any node so s node block the misbehaviour node and send misbehaviour node information to the actual sender node so sender node change self route compute method, and sender search secure path that time eliminate misbehaviour node and find destination node after that sender sends actual data packet through secure path.

a. Create mobile node M;
b. Set Sender node = I //I □ M
c. Set Destination Node = D // D □ M
d. Set Routing Protocol =OLSR // routing protocol
e. Start simulation time = t_0
f. Set radio range = rr; //initialize radio range
g. Set node s; // s ϵ M, s is intrusion prevention node;
h. s sense all neighbor node and capture behavior of each node

If (node n updated routing packet || node n not forward data to destination)
{s create table all misroute node n;
Send reply packet to source node about misbehavior node n;
node s block the misbehavior node n;
recompute_path ();
}
Else {establish path are secure ;}

i. recompute_path (sender, destination, route-pkt)
{if (node m in radio range || neighbor == true || node n = false)
{create route table ();
Receives route packet destination;
}
Else {node out of range or destination unreachable ;}

j. Send acknowledgment to sender node
k. Sender send data packet through secure path;
l. Terminate session;

SIMULATION STUCTURE

The simulator which is used to simulate the ad-hoc routing protocols, is the Network Simulator 2 (ns-2) [19] from Berkeley to simulate the mobile wireless radio environment. A mobility extension to ns is used which is developed by the CMU Monarch project at Carnegie Mellon University.

Simulation Environment:

Network simulator 2 is the result of an on-going effort of research and development that is administrated by researchers at Berkeley. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols [19].

The simulator is written in C++ and a script language called OTcl2. Ns uses an Otcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called Network Animator.

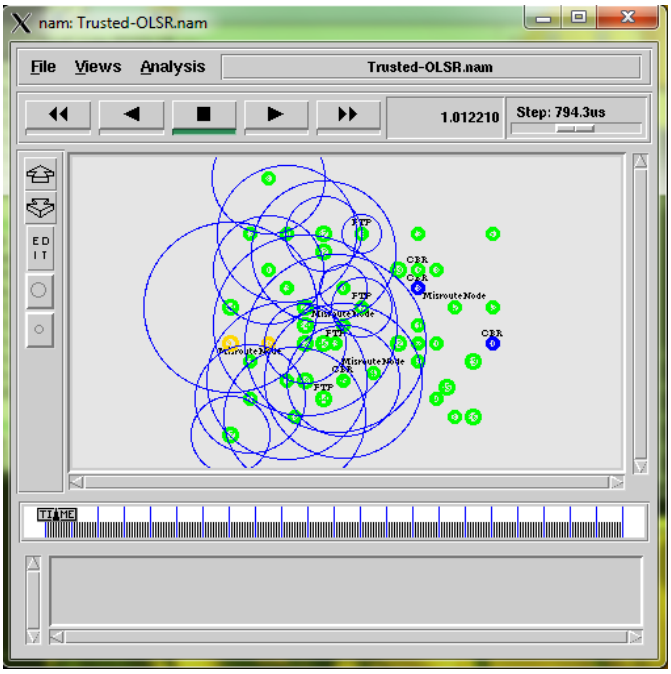

Figure 1: Network Animator scenario

Simulation Parameter:

We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc.

Table 1 Simulation parameter

Simulation Parameter	Value
Number of nodes	50
Dimension of simulated area	800×600
Routing Protocol	OLSR, IPS-OLSR
Simulation time (seconds)	100
Transport Layer	TCP ,FTP
Traffic type	CBR
Packet size (bytes)	1000
Number of traffic connections	15
Maximum Speed (m/s)	Random

According to above table 1 we simulate our network.

Performance Evaluation:

There are following different performance metrics have showed the results on the basis of following:

Packet delivery ratio: ratio of the data packets received at the destination nodes to the packets that were sent by the sources.

Routing load: number of routing packets (and supporting protocol control packets) transmitted per data packet delivered at the destination.

Loop Freedom: Network protocols can resolve the issue of infinite looping by using time-to-live (TTL) features that are traditionally done in IP networks. It would be greatly beneficial for the network as a whole if loop freedom can be *avoided* rather than resolved. Loop-free routing protocols generally will allow for better performance ad hoc networks.

SIMULATION RESULT

Packet Delivery Ratio Analysis:

Packet delivery fraction (PDF) or packet delivery ratio is a ratio of receives packets from packets sends at time unit. PDF calculated as

$$PDF = \left(\frac{Rx}{Send}\right) * 100$$

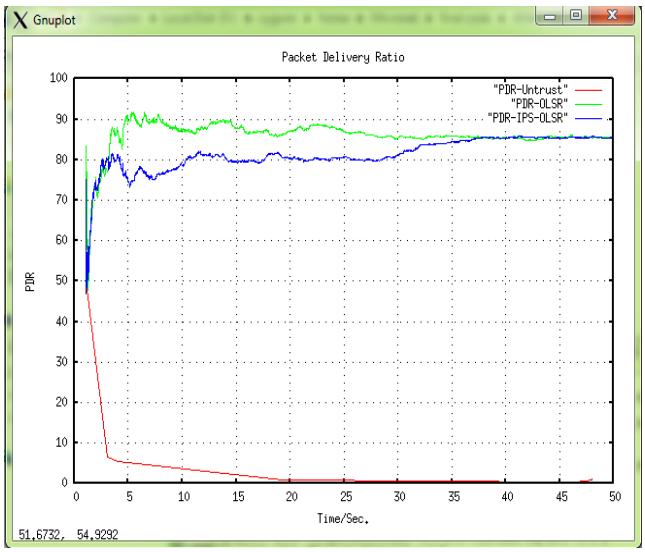

Figure 2: Packet Delivery Ratio Analysis

According to formula if our PDF is best that means this performance is very good. In this graph we analyze PDF in three cases= normal OLSR routing protocol case, Untruth time and intrusion prevention time and get result that if un-trust network form so packet delivery ration nearly zero that means data communication is stop, but the case of network prevention and normal OLSR routing case nearly 87%

Attack Percentage Analysis:

In this graph we analyze attack percentage, here maximum 15% percentage node are misroute information gives to neighbour and flood the routing mis behaviour that work spread attack in the network. In our fifty second simulation case at the time of 25th second maximum mis-routing packet spread on the network.

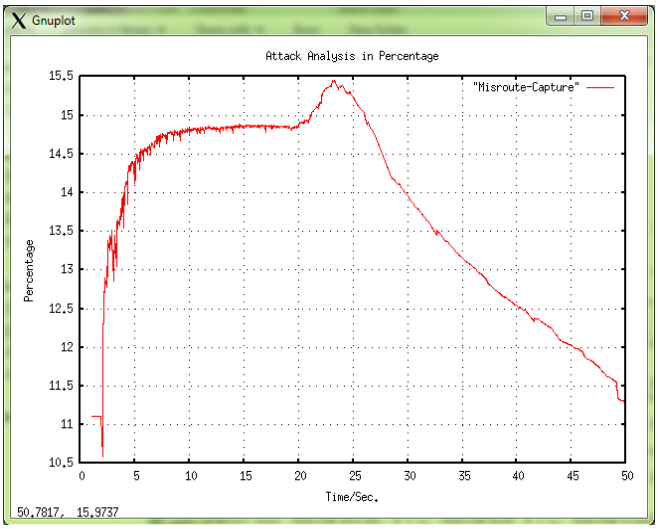

Figure 3: Attack Percentage Analysis

Routing Load Analysis:

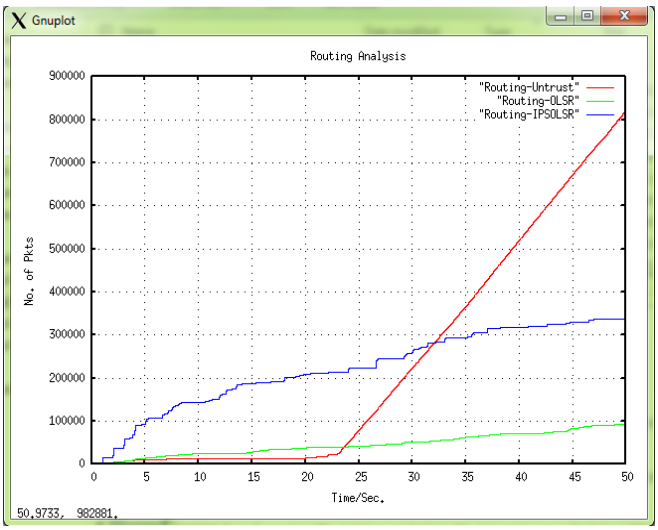

Figure 4: Routing Load Analysis

Routing load is calculated as the total number routing packets are transmitted over the successful data transmission. The increase in the routing load reduces the performance of the ad-hoc network as it consumes portions from the bandwidth available to transfer data between the nodes.

As per graph shown it is observed that till 20 seconds of simulation routing load is slightly increases in case of Un-trust time that means if mis-activity node present in the network so routing packet maximum flood, here IPS and normal OLSR routing time routing packet less as compare to Un-trust case.

Congestion Attack analysis:

In this graph we analyze congestion attack on to the network, result shows nearly 3000 useless packet spread in the network that minimize the performance of network, that congestion packet spread denial of service attack and that case actual source node can't efficiently send's data packet to actual receiver node.

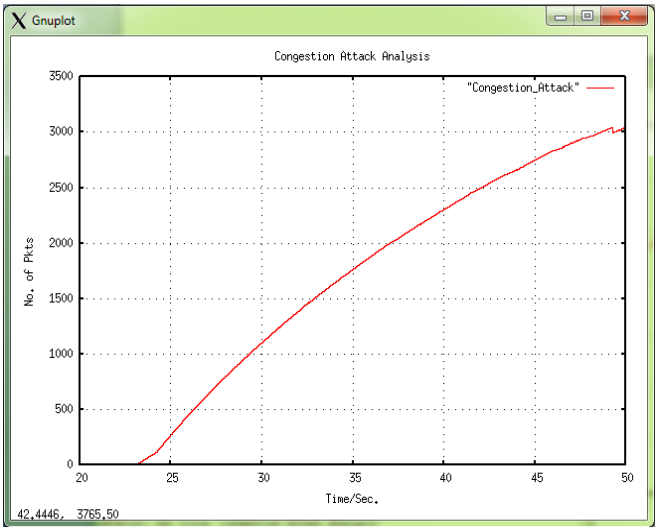

Figure 5: Congestion Attack Analysis

ABOUT THE DEMONSTRATION

In this demo, we analyze network performance on the basis of network parameter like attack percentage, routing load, packet delivery ratio and congestion attack analysis etc. In our simulation we check network performance in normal OLSR time, Un-trust and IPSOLSR time.

CONCLUSION

In this simulation we use network simulator -2 (ns-2). Here number of simulation were taken and finally conclude through various result. Very first we create normal network that time no any attacker node in the network and second scenario routing and congestion attack spreader node present that spread misbehaviour on the network and third scenario we use prevention system in presence of attacker node, finally we conclude that congestion and routing misbehaviour case network performance is very degraded and we also detect infection percentage that is nearly 15% but we apply prevention system so performance is increases and eliminate the path of misrouted node. Finally we conclude that our prevention system gives better result and protect against routing misbehaviour as well as congestion attack, further we apply distributed IPS system for more security provision of the network.

REFERENCES

[1]. K.Urmila Vidhya , M. Mohana Priya "A Novel Technique For Defending Routing Attacks In OLSR MANET" 2010 IEEE International Conference on Computational Intelligence and Computing Research, ISBN: 97881 8371 362 7

[2]. Lalith Suresh P., Rajbir Kaur, M.S.Gaur, V.Laxmi "Collusion Attack Resistance through Forced MPR Switching in OLSR" 978-1-4244-9228-2/10/ ©2010 IEEE

[3]. D. Sterne, P. Balasubramanyam, et al. "A General Cooperative Intrusion Detection Architecture for MANETs". In Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, 2005

[4]. Frederic Cuppens, Nora Cuppens-Boulahia, Tony Ramard "Property Based Intrusion Detection to Secure OLSR" GET/ENST Bretagne, 2 rue de la Chˆataigneraie, 35512 Cesson S´evign´e Cedex, France

[5]. S.Tamilarasan, M.Sathyam Reddy "A Quantitative Study and Comparison of Secure OLSR Routing Protocol" S Tamilarasan et al,Int.J.Computer Technology & Applications,Vol 3 (2), 632-638

[6]. M. Wang, L. Lamont, P. Mason, M. Gorlatova "An Effective Intrusion Detection Approach for OLSR MANET Protocol" 2005 IEEE

[7]. Thomas Clausen, Ulrich Herberg "Vulnerability Analysis of the Optimized Link State Routing Protocol version 2 (OLSRv2)" Thomas Clausen and Ulrich Herberg are with the "Laboratoire d'Informatique de l'X" (LIX) at Ecole Polytechnique, UMR CNRS, 7161 Paris, France

[8]. Imrich Chlamtac a, Marco Conti b,*, Jennifer J.-N. Liu "Mobile ad hoc networking: imperatives and challenges" www.elsevier.com/locate/adhoc, 1570-8705/$ - see front matter @ 2003 Elsevier B.V. doi:10.1016/S1570-8705(03)00013-1

[9]. Ash Mohammad Abbas and Øivind Kure "Quality of Service in mobile ad hoc networks: a survey" 2008 Inderscience Enterprises Ltd

[10]. H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, February 2006, pp. 261-273.

[11]. P. Karn, "MACA – a new channel access method for packet radio," in proceedings. ARRL/CRRL Amateur Radio Computer Networking Conference, September 1990.

[12]. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu "Risk-Aware Response for Mitigating MANET Routing Attacks" 978-1-4244-5638-3/10, publication in the IEEE Globecom 2010 proceedings.

[13]. Marjan Kuchaki Rafsanjani , Ali Movaghar , Faroukh Koroupi "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes" in Proceedings of World Academy of Science, Engineering and Technology 2008

[14]. Jiejun Kong, Xiaoyan Hong, Mario Gerla "A New Set Of Passive Routing Attacks In Mobile Ad Hoc Networks" This Work Is Funded By Minuteman Project And Related STTR Project Of Office Of Naval Research

[15]. Amrit Suman, Praneet Saurabh, Bhupendra Verma "A Behavioral Study of Wormhole Attack in Routing for MANET" International Journal of Computer Applications (0975 – 8887) Volume 26– No.10, July 2011

[16]. T. Clausen and P. Jacquet "Optimized Link State Routing Protocol (OLSR)." RFC 3626, IETF Network Working Group, October 2003.

[17]. Ying Ge, Thomas Kunz and Louise Lamont "Quality of Service Routing in Ad-Hoc Networks Using OLSR." Proceeding of the 36th Hawaii International Conference on System Science(HICSS'03)

[18]. Koey Huishan, Chua Huimin and Koh Yeow Nam "Routing Protocols in Ad hocWireless Networks." National University of Singapore.

[19]. The Network Simulator – ns-2 http://www.isi.edu/nsnam/ns/

