ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# Analysis of Effectiveness of ALERT Protocol against Wormhole Attack in MANETs

**Devendra Kumar[*1], Deepak Kumar Xaxa[2]**

[*1] M.Tech Scholar, CSE Department, School of Engineering & IT, MATS University, Raipur (C.G.), India

[2] Assistant Professor, CSE Department, School of Engineering & IT, MATS University, Raipur (C.G.), India

devencaught@gmail.com

## Abstract

Routing in MANETs is one of the challenging issues because it dynamically changes their topology over the time and hence requires an efficient routing protocol to communicate among the mobile nodes. There are several routing protocols proposed for MANET environment categorized as non-location based protocols and location-based protocols. Among all routing protocols the location based routing protocols are preferred in MANETs as they are more efficient in routing compared with the non-location based routing protocols. On the other hand security is also the challenging issue in the MANET due to its feature like open access medium, lack of central monitoring and management etc. and therefore increased the possibility of eavesdropping, spoofing, and denial-of-service attacks. The wormhole attack is one of the stronger active attacks which are difficult to avoid/detect in any network where the two or more attacker nodes tunnel the network traffic information from one location to another in the network. In this paper we focus our study on efficient location based routing protocol ALERT and their effectiveness measure against wormhole attack based on parameters like throughput,end-2-end delay ,packet delivery ratio and normalized routing load. The performance analysis is done for 10,20,30,40 and 50 nodes using the network simulator (NS-2.35).A comparative study is represented on above parameters for all five scenarios.

**Keywords**: MANETs, Routing Protocols, ALERT protocol, Wormhole Attack, Network Simulator-2.

## Introduction

A mobile ad hoc network (MANET) is a self configurable and infrastructure-less network having collection of any number of wireless mobile devices [8]. Nodes in a MANET may be cell phone, laptop, PDA, personal computer etc. MANET's node can act as a host or as a router or both at the same time. All the nodes in a multi-hop wireless ad hoc network cooperate each other to form a network without the presence of centralized infrastructure such as access point or base station [2]. The mobile nodes in this network require to forward packets for each other on the basis of mutual trust to enable communication among nodes outside the transmission range. The nodes in the network are free to move in any direction independently, leave and join the network randomly. Thus a node experiences changes in its link states periodically with other devices. Due to the mobility in the ad hoc network, change of link states and other properties of wireless transmission such as attenuation, multipath propagation, interference etc. create a challenge for routing protocols operating in an ad hoc network.

Figure 1 shows a typical example of a mobile ad hoc network.

**Fig: 1 A Mobile Ad-hoc Network**

The application area of MANET are military battlefield, emergency or rescue situations like floods, earthquake etc, and also in classrooms or colleges as there is no need to establish a centralized infrastructure.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Security in Mobile Ad-Hoc Network is one of the most important concerns for the proper functionality of the network. MANETs often suffer from security attacks because of its features like open access medium, dynamically changing topology , lack of central monitoring and management, cooperative algorithms and no clear defence mechanism [6]. MANETs must have a secure way for transmission and communication which is a quite challenging and vital issue as there is increasing number of threats of attack on the wireless ad-hoc networks. In order to provide secure communication and transmission, the researchers must have to understand several different types of attacks and their effects on the MANETs environment. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service(DoS) , selfish node misbehaving, impersonation attack are the kind of attacks that a MANET can suffer from [4].

## Routing Protocols

For the nature and challenges found in designing an ad hoc network routing protocol, a large amount of work has been done in the research community to find a perfect routing protocol for mobile ad hoc networks. The research has resulted to a number of routing protocols which can be classified as Non-Location based routing protocols and Location-based routing protocols as shown in Figure 2 [12]. Non-Location based routing protocol uses the traditional routing concept such as maintaining a routing table or distributing link state information while the Location- based routing protocol uses the geographical physical position of the mobile nodes to route the data packets from source to destination.

***Non-Location based*** routing protocols are further divided into three groups: proactive, reactive protocols and hybrid protocols.

Proactive protocols like Destination-Sequenced Distance-Vector (DSDV) protocol try to update routing information periodically within the system so that at any time, every node knows how to route packets to the other nodes in the network. Proactive routing protocols usually require periodic exchange of messages and routing information to maintain updated information of the links among all nodes of the network. If only a few pair of nodes are communicating in a large network then most of the periodical exchanged information is useless and hence proactive protocol can waste a lot of bandwidth and other resources.

In contrast to this, Reactive routing protocols like Dynamic Source Routing (DSR) protocol and Ad-hoc On-Demand Distance Vector (AODV) protocol try to find a routing path between the source and the destination whenever it is required. Reactive protocols are also commonly known as on-demand routing protocols. In case of reactive protocols, the nodes waste their resources to find out the routes whenever it is necessary.

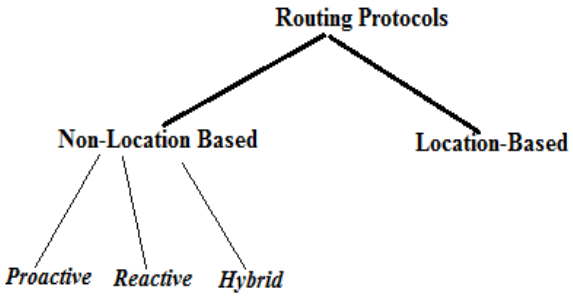


**Fig: 2 Routing protocols in MANETs**

The hybrid protocol uses a combination of reactive and proactive approach to maintain routes. In the hybrid technique proactive approach is used when the nodes are in the local neighborhood i.e. for the nodes up to a certain hops and reactive approach is used when the destinations nodes are far away.

In case of **Location-based** routing protocols, the nodes use the information about the geographical location of other nodes to route data packets to their destinations. Each node in the network is aware of their own position by means of GPS receivers and obtains the location information of other nodes via a location service that is provided by the nodes themselves [10]. When sending a data packet to a destination, the source node acquires the position of the destination node by the location service and includes this information in the header of the packet. Then, each intermediate node that receives the packet gets the location information of the destination from the packet and uses it to forward the packet comparing with its own location.

The advantage of Location-based routing protocols is that the nodes do not need to maintain routing information or to discover routes explicitly, which greatly reduces control traffic overhead over the network. This relieves the routing protocols from bearing large control overhead in the packet header. However there is still some overhead to find the location service and get location information from the location service. The disadvantage of Location-based routing protocol is

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

that the node needs to install some sort of hardware which will provide the precise geographical location information of the node itself i.e. a GPS receiver.

**Alert: Ananonymous Location Based Efficient Routing Protocol**

One of the efficient Location Base routing protocol is the ALERT protocol which provides anonymity protection to source, destination as well as routes. It assumes the entire network area to be a rectangle where the nodes are randomly disseminated. The information of the bottom-right and upper left boundary of the network area is arranged into each node whenever it tries to join in the network. This information enables a node to locate the positions of other nodes in the entire area for zone partitions in ALERT [9].

ALERT features an unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes as shown in Fig.3, for a given area, ALERT horizontally partition it into two zones say A1 and A2. Then vertically partition zone A1 to B1 and B2. After that, horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. This partition process known as hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message. Specifically, in the ALERT routing, each source node executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and destination nodes are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF).

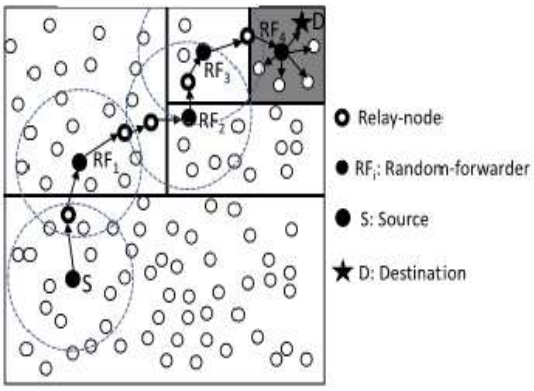


**Fig: 3 Routing Among Zones in ALERT [9]**

## Security attacks on MANETs

Currently ad hoc routing protocols are basically exposed to two different types of attacks: Active attacks and Passive attacks [6]. An attack is considered to be ***active*** when the misbehaving node has to bear some energy costs in order to perform the threat while ***passive*** attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish. Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. Recent research studies brought up also a new type of attack that goes under the name of wormhole attack.

MANET security attacks on network layer can be classified as :

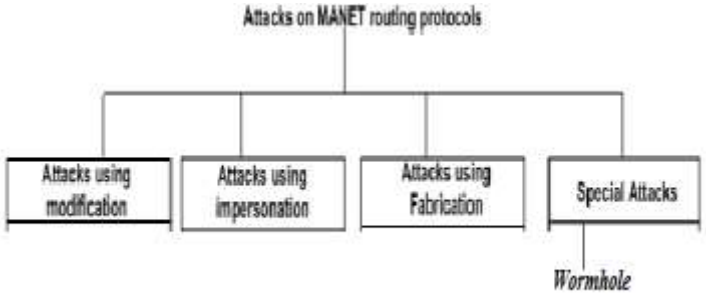


**Fig. Classification of MANET attacks**

1. *Attacks using modification*: In this type of attack, the protocol fields of the messages passed among the nodes is modified, thereby resulting in traffic subversion or Denial of

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Service (DoS) attacks. Examples of such attacks are: Redirection by modified route sequence numbers, Redirection with modified hop count and Denial of Service with modified source routes.

2. *Attacks using Impersonation*: These types of attacks violate authenticity and confidentiality in a network. A malicious node can impersonate or spoof the address of another node in order to alter the vision of the network topology as perceived by another node. . Examples of such attack is Formation of loops by spoofing.
3. *Attacks using fabrication*: In this type of attack, a malicious node tries to inject fake messages or routing packets to disrupt the routing mechanism. Such attacks are difficult to detect in a MANET since the routing packets appear to be legitimate packets to the nodes processing them. Examples of attacks by fabrication are : Falsifying route errors and Route cache poisoning.
4. *4.Special Attack* : Apart from the above attacks there are two other severe attacks which are possible against routing protocols. They are described below-(a) *Wormhole Attack:* The wormhole attack is a severe type of attack in which two colluding malicious nodes can tunnel packets through a "tunnel" in the network.It is described in detail in section 4. (b) *Black hole attack*: In this type of attack, a node advertises a zero metric for all destinations causing all nodes around it to route packets towards it. The Location Based protocols are vulnerable to such attack.

## Wormhole Attack

The wormhole attack is one of the stronger active attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". This complete scenario described in Figure 3.7 which is given below:

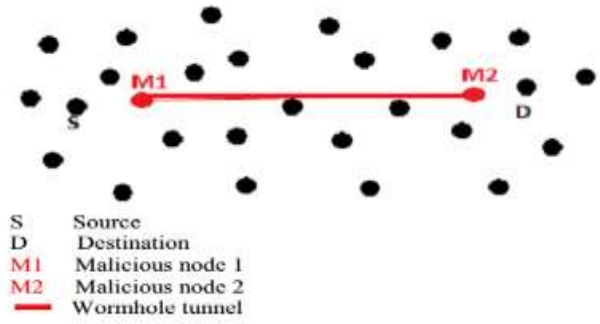


**Fig: 4 Wormhole Attack [5]**

In the above example where there are two malicious nodes M1 and M2 which are linked through a private connection called tunnel. In this type of attack every packet which an attacker receive from one network forwards to other network where another malicious node exist. The traffic between the two nodes passes through "wormhole" among each other. Due to this way it will become the cause of disrupts routing protocols and disturbing normal flow of routing packets. These types of attacks are very difficult to detect in a network, and become the cause of severe damages to the nodes [4].

## Related works

Previously the work followed the analysis of wormhole attack on Non-Location based routing protocols and very little attention has been given on location based routing protocols. As Location based protocols are better in routing comparing with Non-location based routing protocols, so there is a need of securing such protocol against severe security attacks by analyzing stronger attacks.

N. Satheesh, et al., [1] analyzed the impact of wormhole attack with AODV Routing protocol in the presence of wormhole attacks. The parameters such as throughput, end to end delay and the number of cache replies were used to evaluate the performance using the simulator NS-2. Experimental result was shown that the throughput and the number of cache replies were increased up to 50% in the presence of malicious nodes and the end to end delay was increased randomly.

VIVEK SHARMA, et al., [2] analyzed the performance of AODV and DSR routing protocols with and without wormhole attack. The result was shown that DSR performs better than AODV.

Gurpreet Kaur, et al., [3], in this article, the effect of wormhole attack on different routing protocols like AODV, DSR, ZRP and ANODR is analyzed on behalf of parameters like throughput, delay and energy consumption. In wormhole all drop mode, it drops all data packets so in this

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

experiment the throughput and end-to-end delay of ANODR routing protocol is considered as best as throughput is more and delay is less as compared to other routing protocols.

Devinder Pal Singh, et al. [4], in this paper the effects of Wormhole attack analyzed using OLSR and AODV routing protocols. Based on simulation result the author concluded that AODV is more vulnerable to Worm Hole attack than OLSR.

V. Karthik Raju, et al., [5], in this paper, author proposed a Round Trip Time (RTT) mechanism to detect and avoid wormhole attacks in mobile ad hoc networks using the AOMDV protocol.

Mahesh Gour, et al., [6], in this paper author analyzed wormhole attack at ALARM protocol with attack and without attack. The performance parameters considered are throughput, Packet delivery ratio, packet dropped rate and the network load.

Mehdi sookhak, et al., [7], in this paper, author reviewed the secure geographic routing protocols to protect against blackhole and wormhole attack. The metrics to evaluate the protocols performance considered are localization information (GPS), authentication, integrity and trust mode, in order to improve their level of security.

Misbah Jadoon, et al., [8], in this paper author observed that location –based protocols are better than non location based routing protocols with various mobility patterns.

## Simulation Tools and Setup

### Network simulator-2

The Network Simulator 2 (NS-2) is a popular discrete event simulator developed mainly for networking research [10]. It is open source software developed at USC/ISI. It provides an extensive simulating environment for various applications, protocols, data sources, network types, traffic models and network elements. NS-2 is designed having a dual approach as, C++ for core functionality and OTcl for scripting purposes. The core of NS is written in C++, which handle data processing and the Object TCL (OTCL) scripting language is used for writing control script to run the simulation. The fundamental reason for this is that the protocol implementation requires a powerful language (here C++) for faster per packet processing and the use of script language makes the writing and change of simulation configuration faster to adjust with desired parameters. NS-2 is also accompanied by the network animator (NAM) that gives a Graphical User Interface (GUI) and visualization of the network that is designed and simulated using NS-2. For MANET, NS-2 provides a comprehensive library for ad hoc routing and mobile IP, topology generators, propagation models, mobility models and data sources.

To run any simulation in NS-2, the scenario is defined using TCL script. The simulation generates a trace file containing data about packets sent, received, forwarded, dropped, size of packets, type of packets etc. for further analysis.

### Simulation Setup

Network Simulator tool NS-2 is used to evaluate the performance of different location based routing protocols in mobile ad-hoc networks. The wormhole attack is implemented on varying number of nodes in network and consequently isolated the wormhole attack using isolator to know the effectiveness of routing protocols .The performance of routing protocols is analyzed on behalf of metrics like throughput, end-to-end delay, packet delivery ratio and normalized routing load. The parameters used in the simulation are summarized in the table below:

| | |
|---|---|
| Mobility Model | Random Way-point |
| Simulation Area(m x m) | 1000 x 1000 |
| Simulation Time | 20 sec. |
| Number of Nodes | 10,20,30,40 and 50 |
| Routing Protocols | ALERT and GPSR |
| Traffic Type | CBR |
| Performance Parameters | Throughput,End-2-End Delay, Packet Delivery Ratio and Normalized Routing Load |

**Table: 1 Simulation Setup**

### Scenario design

The simulation topology of MANET environment with wormhole attack is shown in Fig.5 where wormhole attack drops the packets and tunnels the traffic information into another network.

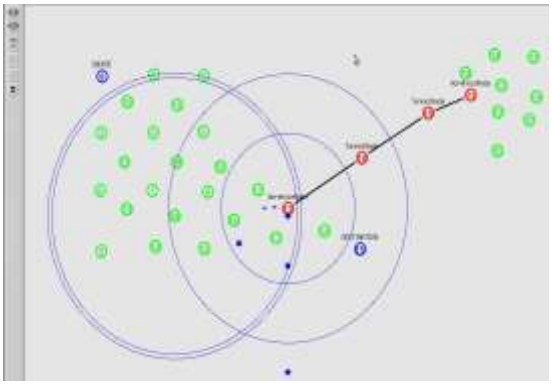

**Fig: 5 Simulation Topology**

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

## Results

Here the comparison of the ALERT protocol and GPSR protocol with Wormhole attack is represented on the basis of performance metrics of Throughput, End-2-End Delay, Packet Delivery Ratio (PDR), and Normalized Routing Load (NRL) is described.

**Throughput**

Throughput is the average rate of successful packet delivery over a network in per unit time. Throughput is decreased in presence of wormhole attack for ALERT because wormhole receives packet from one location and tunnel it to into another network. Throughput of network is improved without wormhole node for ALERT as shown in the figure 6.

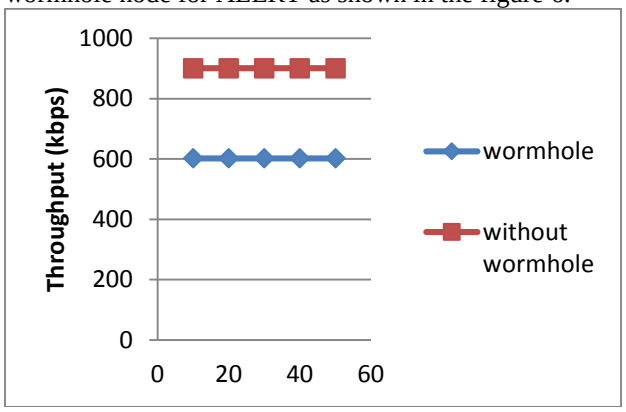


**Fig: 6 Throughput over ALERT**

**Packet Delivery Ratio (PDR)**

Packet Delivery Ratio is defined as the ratio between no. of packet received to no. of packet sent in the network and it should be minimal for any routing protocol. Fig. 7 shows a comparative graph of PDR of ALERT with Wormhole and without wormhole attack for all five scenarios.

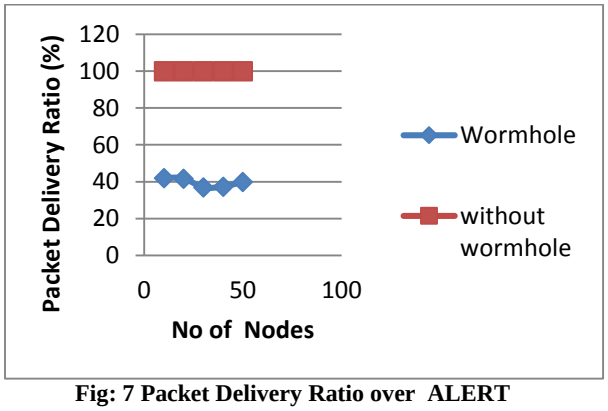


**Fig: 7 Packet Delivery Ratio over ALERT**

**End-2-End Delay**

End-2-End Delay refers to the time taken for a packet to be transmitted across a network from source to destination. End-2-End Delay graph of ALERT is shown in figure 8. The delay in case of ALERT protocol without wormhole is less as compared to with wormhole attack.

**Normalized Routing Load**

Normalized Routing Load refers to amount of data or traffic overhead being carried by the network. Normalized Routing Load graph of ALERT is shown in figure 9. The network load in case of ALERT protocol without wormhole is less as compared to with wormhole attack.

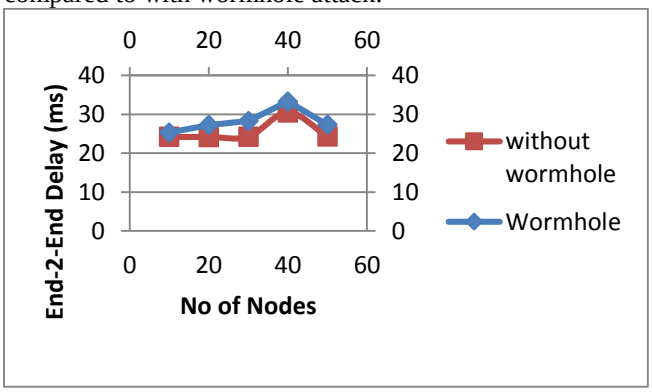


**Fig: 8 End-2-End Delay ALERT**

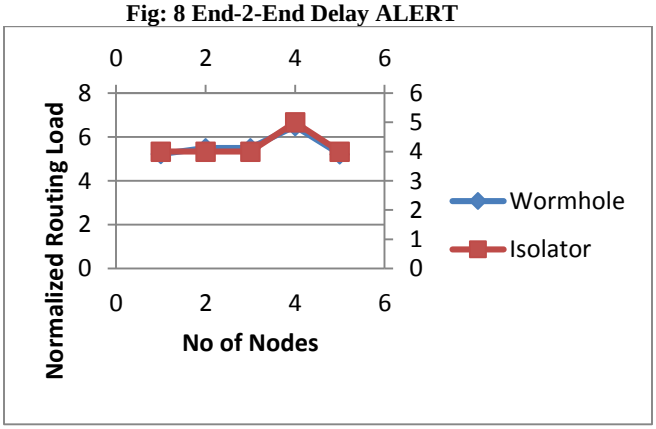


**Fig: 9 Normalized Routing Load over ALERT**

## Conclusion

Mobile Ad-Hoc Networks could be deployed anywhere as it does not require any centralized infrastructure. With the importance of MANET and its large application areas it has still many challenges to overcome. There are number of threats of MANET security from which it can suffer, one of them is wormhole attack. Wormhole attacks are stronger attacks that can easily be launched in any network whether networks having stronger congeniality and authenticity mechanism. In this paper, we performed and analyzed the wormhole attack at location based protocol ALERT. The simulative results shows that ALERT protocol

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

slightly effected in case of wormhole attack for all parameters like network throughput, end-2-end delay, packet delivery ratio and the normalized network load.

## References


**[1]** *Satheesh et al.,'Analysis and Parameterized Evaluation of Impact of Wormhole Attack Using AODV Protocol in MANET', International Journal of Advanced Research in Computer Science and Software Engineering 3(9), pp. 708-713, September - 2013.*

**[2]** *Vivek Sharma et al.,' Analysis of AODV and DSR in Presence of Wormhole Attack in Mobile Ad-hoc Network', International Journal of Engineering Science and Technology Vol. 2(11), 2010, 6657-6662.*

**[3]** *Gurpreet Kaur and Er. Sandeep Kaur Dhanda,' Analysing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network', International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.*

**[4]** *Devinder Pal Singh et al.,' INVESTIGATING THE EFFECT OF WORMHOLE ATTACK ON AODV& OLSR ROUTING PROTOCOLS IN MANET', International Journal of Future Engineering & Technology, Volume (1): Issue (1).*

**[5]** *V. Karthik Raju and K. Vinay Kumar,' A Simple and Efficient Mechanism to Detect and Avoid Wormhole Attacks In Mobile Ad Hoc Networks', 2012 International Conference on Computing Sciences.*

**[6]** *Mahesh Gour, Amrit Suman and Ankur Kulhar,' Detection and Prevention of Wormhole Attack in ALARM Protocol (MANETs)', HCTL Open Int. J. of Technology Innovations and Research HCTL Open IJTIR, Volume 4, e-ISSN: 2321-1814 ,ISBN (Print): 978-1-62776-132-1,July 2013.*

**[7]** *Mehdi sookhak et al.,' Secure Geographic Routing Protocols: Issues and Approaches', IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4,ISSN (Online): 1694-0814,July 2011.*

**[8]** *Misbah Jadoon et al.,' Location and Non-Location Based Ad-hoc Routing Protocols under various Mobility Models :A Comparative Study', The International Arab journals of Information Technology,Vol.9, No.5,September 2012 .*

**[9]** *Haiying Shen and Lianyu Zhao,' ALERT: An Anonymous Location-Based Efficient Routing Protocol in Mantes', IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013.*

**[10]** *Karim El Defrawy and Gene Tsudik' ALARM: Anonymous Location-Aided Routing in Suspicious MANETs ', IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9, SEPTEMBER 2011.*

**[11]** *Brad Karp and H.T. kung,"GPSR: Greedy Perimeter Stateless Routing for Wireless Networks",research supported by AFOSR MURI Grant F49620-91-1-0382 and NSF Grant CDA-94-0124 and in part by Microsoft Research,Nortel,Sprint,ISI and ACIRI.*