# Identification and Removal of Malicious Nodes in Mobile Ad Hoc Networks

**Er. Satinder Kaur**
M.Tech Student
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology
engg.sonia2002@gmail.com

**Er. Tanu Preet Singh**
Associate Professor
Department of Computer Science & Engineering
Amritsar College of Engineering & Technology
Amritsar, India
tanupreet.singh@gmail.com

*Abstract* - **An ad hoc wireless network is a temporary and dynamic environment where a group of mobile nodes with radio frequency transceivers communicate with each other without the intervention of any centralized administration or established infrastructure. Due to the limited transmission range of each mobile node, communication sessions between two nodes are usually established through a number of intermediate nodes, which are supposed to be willing to cooperate while forwarding the messages they receive to their destination. Unfortunately, some of these intermediate nodes might not be trustworthy and might be malicious, thereby forming a threat to the security and/or confidentiality of the exchanged data between the mobile nodes. While data encryption can protect the content exchanged between nodes, analysis of communication patterns may reveal valuable information about end users and their relationships. Using anonymous paths for communication provides security and privacy against traffic analysis. To establish these anonymous paths, in a traditional wired network, nodes build a global view of the network by exchanging routing information, whereas in an ad hoc wireless network, building this global view is not an option. Mobile ad hoc networks are extensively used in military and civilian applications. So, security is one of the main concerns in modern network. Most of the routing protocols in MANET, such as DSR, AODV, in that node are reliable and cooperative. This routing protocol provides MANET vulnerable to various types of malicious attacks. In this paper, we propose a novel distributed routing protocol which guarantees security, anonymity and high reliability of the established route in a hostile environment, such as ad hoc wireless network, by encrypting routing packet header and abstaining from using unreliable intermediate node. The major objective of our protocol is to allow trustworthy intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of the communicating nodes. We describe our protocol, and provide its proof of correctness.**

***Keywords: Wormhole, Trust based attack, Community Key management***



## I. INTRODUCTION

A mobile ad-hoc network (MANET) is a temporary infrastructure less multi-hop wireless network in which the nodes can move arbitrarily. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, thus, well suited for the scenarios in which pre deployed infrastructure support is not available. In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Mobile ad hoc networks are finding ever increasing applications in both military and civilian scenarios due to their self-organizing, self-configuring capabilities. Ad hoc networks are dynamic collections of self-organizing mobile nodes with links that are changing in an unpredictable way. They are characterized by a dynamic topology and the lack of any fixed infrastructure. The communication medium is broadcast. The nodes can be regarded as wireless mobile hosts with limited power, range and bandwidth. The recent rise in popularity of mobile wireless devices and technological developments has made possible the deployment of such networks for several applications. Indeed, because ad hoc networks do not have any fixed infrastructure such as stations or routers, they are highly applicable to emergency deployments, disasters, search and rescue missions and military operations. So far, most of the research has focused on functionality issues and efficiency, with security given a lower priority, and in many cases, regarded as an add-on afterthought technology rather than design feature. The malicious nodes can readily function without proper security, as routers and prevent the network from delivering the

packets properly. For example, the malicious nodes can declare incorrect routing updates. Subsequently they are propagated in the network or drop all the packets passing through them. Thus security issue in ad hoc networks, specifically the protection of their network-layer operations from malicious attacks, is extremely important. On distributed computer systems, there are a number of well-known attacks. These include

• Denial of Service: A network service is not available due to overload or malfunction.

• Information theft: Information is read by an unauthorized instance.

• Intrusion: Access to some restricted service is gained by an unauthorized person.

• Tampering: Data is modified by an unauthorized person. As a solution for these kind of attacks, a network layer security solution has been provided in ad hoc networks. In this paper, developing a security framework has been proposed. This security framework involves:

1. Detection of malicious nodes by the destination node.

2. Isolation of malicious nodes by discarding the path.

3. Prevention data packets by using dispersion Techniques

Our goal in this paper is to show that tracing malicious (insider) faults of ad hoc networks is not as simple as it may appear at first.

## II. SECURITY ISSUES IN MANETs

The threats on a MANET can be from the unauthorized nodes those are outside the network or from the nodes inside the network. Threats from the nodes outside of the network are likely to be more easily detected than the internal nodes of the network. The threats from the internal nodes are difficult to detect as they are from trusted sources. Threats on the MANET can be broadly divided into 2 categories such as (i) external threats and (ii) internal threats [14]. In the presence of an authentication protocol to protect the upper layers, external threats are detected at the physical and data link layers. The threats posed by internal nodes are very serious; as internal nodes have the necessary information to participate in distributed operations. Malicious nodes exploit the routing protocol to their own advantage, e.g. to enhance performance or save resources. The main attack by malicious nodes is the packet dropping where most routing protocols have no mechanism to detect whether data packets have been forwarded.

*Types of Attacks*

The attacks can be divided into 2 categories [1].

A. Active attacks are lunched intended to disrupt the service of a network. Such attacks produce threats to confidentiality, integrity and availability of data and services in MANET. Here the term active attack has been used to mean that if any of the node's intention in the network to disrupt any of the security goals intended, such types of attack can be termed as active attack. In contrast the passive attack is an attack which is performed by the nodes to benefice itself only. The node has no other intention to disrupt the service of the network [26].

B. Passive attacks are done by some of the malicious nodes selfishly to conserve power by not forwarding the packets to the destination. One type of such attacks is known as the black hole attack or the wormhole attack which causes data packet dropping. These nodes are very difficult to detect.

*Black hole Attack*

A node which is a black hole has two properties – it participates in the route discovery process and the second property is that, it sometimes does not forward the data packet towards the destination. These nodes create problems in data transmission if they come in the route to destination. The nodes in the MANET are resource constrained; resource may be bandwidth, energy etc. Most of the nodes in MANET rely on batteries as their source of power; so, some of the nodes behave maliciously to conserve their limited battery power [28]. So, when the data packets are forwarded to the destination these selfish nodes simply do not forward the data packets towards the destination [27][28]. So all the packets move up to that node and disappear. Hence, these nodes act as a black hole which causes data packet dropping.

Attack Classification [24] classifies attacks on network coordinate systems into four classes:

(1) Isolation: Malicious nodes select several nodes as their targets and then inveigle themselves into a remote area. These targets seem to be isolated from other nodes so that they would probably choose malicious nodes as their neighbors because the malicious ones are their closest nodes in the remote zone. Thus, malicious nodes can play tricks on these targets.

(2) Repulsion: In order to reduce the consumption of its resources, e.g. bandwidth, a malicious node provides other nodes with false information either by

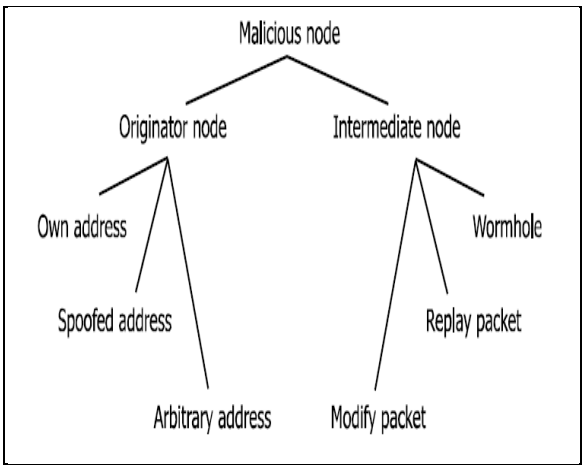
forging coordinates or delaying the probes to pretend its position is rather far away.

(3) Disorder: The aim of this attack is to cause high error or even non-convergence in coordinate systems. In order to realize the attack, malicious nodes provide fake information to others.

(4) System control: In this attack, malicious nodes try to be in higher hierarchy to influence as many nodes as possible.

*Attacking the routing protocol*

Two possible threats from malicious nodes are misdirection of traffic, one of the consequences of which may be denial of service, or denial of service as a means to an end itself. These threats can be further subdivided, as in the attack model shown in Figure. Attacks arising from malicious behaviour can be divided into those where packets are originated by the malicious node, and those where a malicious node is an intermediate node and receives control packets for for-warding. When a malicious node is originating packets, it can send control packets using its own source address, an address which belongs to an existing node in the ad hoc network, or an arbitrary address which does not belong to any node. Malicious intermediate nodes can either modify or replay received packets.




This section concentrates on possible attacks on the various mechanisms used to discover and maintain routes in both proactive and reactive protocols. In particular, we investigate if the type of routing protocol used has a bearing on the effort needed to successfully perform such attacks. First, we discuss issues which are common for both types of protocol: the scope of malicious attacks and the use of sequence numbers. We then look at potential attacks that exploit the two main threats from malicious nodes: misdirection of packets and denial of service.

The scope of attacks arising from malicious behavior

Even though an ad hoc network is vulnerable to attacks from an internal node, the scope of such an attack is limited. In general, the scope of an attack will be affected by two factors — distance and node density. A malicious node can divertise network topology information which contradicts information provided by a well behaved node, creating a case of the well known 'Byzantine generals problem'. For example, if a malicious node falsely advertises a direct route to a node which is connected elsewhere in the network, then the probability of other nodes accepting the false route depends on their relative distances to the malicious node and the well-behaved node. Nodes closer to the malicious node than the well-behaved node are more likely to accept the false information. The resources required to mount an attack, together with the number of nodes that are affected, can be used as a measure of the efficiency of that attack, i.e. the effort that a malicious node has to make to achieve a specific amount of damage. In general, the more densely populated is the area in which a malicious node is located, the more nodes will be affected, and hence the greater the efficiency of the attack. A malicious node could find itself as part of the only route between two or more groups of nodes. In this case, the malicious node can partition the network; the node can now attack one or both of the resulting partitions independently. Such a malicious node is able to control the scope of its attack by focusing on one partition, which may help it avoid detection. Other than finding some means of preventing malicious behaviour, one method of tackling this threat is to ensure that there are always multiple routes between any two nodes. An attack will potentially have a much greater impact if it is performed by a group of malicious nodes, possibly colluding to perform a coordinated attack. It is difficult to make any assumptions about how many malicious nodes there will be in an ad hoc network, and if they have prior relationships which can be used to launch a distributed attack. Therefore, the effectiveness of any security solution should be assessed for various percentages of malicious nodes in the network.

## III. RELATED WORK

The following list of papers shows the relative work carried out for different types of attacks in MANETS and possible solutions given.

1) Detecting Network Intrusions via Sampling: A Game Theoretic Approach: In this paper, the problem

of detecting an intruding packet in a communication network is considered [2].

2) A Distributed Security Scheme for Ad Hoc Networks discuss the DoS attack like flooding using AODV protocol and concludes with an immediate enhancement to make the limit-parameters adaptive in nature. This can be done by making calculations based on parameters like memory, processing capability, battery power, and average number of requests per second in the network and so on [3].

3) Wormhole attacks detection in wireless ad hoc networks using a statistical analysis approach [4].

4) Wormhole Attack Detection in Wireless Sensor Networks: This paper analyzes the nature of wormhole attack and existing methods of defending mechanism and then proposes round trip time (RTT) and neighbor numbers based wormhole detection mechanism [5].

*Misbehavior on Data*

Different types of misbehavior out of different purposes have been created by the misbehaving nodes in an ad hoc network. The types of misbehavior on data related to the work are discussed here.

*Data Dropping*

This is the denial of service (DoS) attack. In this attack, the selfish or malicious intermediate nodes decline to forward data packets for other nodes in the network. In this paper two adverse environments are inspected. They represent the types of data dropping misbehavior formed by individual and cooperating misbehaving nodes respectively.

*A. Individual dropping*: This is a relatively simple type of misbehavior. The misbehaving nodes drop all or a certain percent of the received data packets because of unlike intentions. Most schemes detecting misbehavior on data have expected to deal with this kind of misbehavior.

*B. Colluded dropping*: This is an advanced type of misbehavior formed by two cooperating malicious nodes. It is difficult to detect and defend this attack. It is assumed that two malicious intermediate nodes N1 and N2 are connected on a data transmission path. N1 forwards received data packets to N2, and N2 drops all or part of them. N1 tries to cover the data droppings at N2 by ignoring it and/or generating / forwarding faked acknowledgements in the system. As N1 would not report the misbehavior of N2 to the system, the overhearing schemes fail to detect such colluded misbehavior. Since N1 could forward faked 2ACK generated by N2 or generate faked 2ACK for N2, neither of the protocols proposed in [20] could detect such fabricated packets and this colluded dropping. The schemes discussed in tackle such colluded misbehavior

*Data Modifying*

During their transmission, the malicious nodes alter the received data packets. One malicious node is assumed to form the data modifying misbehavior independently along the data transmission path. Whereas the schemes in [21], [22] can successfully detect such misbehavior, the schemes in cannot detect such kind of misbehavior

## IV. DESIGN

Identification of Malicious node in an Adhoc Network - An Adhoc network can be attacked from any direction at any node which is different from the fixed hardwired networks with physical protection at firewall and gateways. Altogether it denotes that every node should be equipped to meet an attacker directly or indirectly. Malicious attack can be initiated from both inside and outside of the network. Tracking a specific node is difficult in large Adhoc networks and hence, it is more dangerous and much difficult to detect the attacks from an affected node. Altogether it denotes that every node should be prepared to work in a way that it should not trust on any node immediately. Distributed architecture should be applied in order to achieve high availability. This is because if the central entity is used in the security solution, it causes serious attack on the entire network when the centralized entity gets affected. The following are the types of active attacks and its relevant solutions:

*A. Black hole attack*

Let H be a malicious node. When H receives a Route

Request, it sends back a Route Reply immediately, which constructs the data and can be transmitted by itself with the shortest path. So S receives Route Reply and it is replaced by H -> S. Then H receives all the data from S.

*B. Neighbor attack*

The neighbor attack and the black hole attack prevent the data from being delivered to the destination. But the neighbor attacker does not catch and capture the data packets from the source node. It leaves the settings as soon as sending the false messages.

*C. Wormhole attack*

Two malicious nodes share a private communication link between them. One node captures the traffic information of the network and sends them directly to other node. Warm hole can eavesdrop the traffic, maliciously drop the packets, and perform man-in- the-middle attacks against the network protocols. [6].

*D. DoS (Denial of Service) attack*

When the network bandwidth is hacked by a malicious node [5], then it results to the DoS attack. In order to utilize precious network resources like bandwidth, or to utilize node resources like memory or computation power, the attacker inserts packets into the network. The specific instances of the DoS attack are the routing table overflow attack and energy consumption attack.

### *E. Information Disclosure attack*

The information disclosure attack aims at the privacy requirements of network. The confidential information's like routing location, node status or secret keys and password are leaked out by the malicious node to the unauthorized nodes

### *F. Rushing attack*

The rushing attack aims against on-demand routing protocols which uses identical suppression at each node. In order to find routed to the destinations, the source nodes sends out the RREQ. Each intermediate node processes only the first non-duplicate packet and discards any duplicate packet which arrives at a later time. Rushing attackers can forward these packets quickly by skipping some of the routing processes. They are also able gain access to the forwarding group [7].

### *G. Jellyfish attack*

A malicious node receives and sends RREQ and RREP normally. But before forwarding it delays the data packets without any reason for some time[7]. Since the node has to intrude the forwarding group first, it is difficult to implement this type of attack. If the number of malicious node is few, then the influence to the network is also less.

### *H. Byzantine attack*

It is also called as impersonation attack because the malicious node might imitate another normal node. It also sends false routing information for creating an anomaly update in the routing table. In addition to this, an attacker may get unauthorized admission to resource and sensitive information.

### *I. Blackmail attack*

This attack is applicable against routing protocols which uses mechanisms for the recognition of malicious nodes and broadcast the messages which try to blacklist the offender [8]. By adding other legitimate nodes to their blacklists, an attacker might blackmail a legitimate node. Thus the nodes can be avoided in those routes.

### *Community Key Management*

In each community, the central node classifies its neighboring nodes into three classes, based on their trust level. The first and lowest trust level is for nodes whose trust value is between 0 and d1, while the second trust level, i.e. the medium level, contains the nodes whose trust level is between d1 and d2. The trust level, corresponding to the high level, contains the nodes whose trust value is between d2 and F. Each node selects independently the values for d1, d2, and F. The central node generates two different keys for the medium and high trust level, and shares them with its neighbors. All neighbors in the same trust level share the same key. The neighbors in high trust level will have both High Trust Level Community Key (referred to as HTLCK) and Medium Trust Level Community Key (referred to as MTLCK), whereas, the neighbors in medium trust level have only MTLCK. As for the neighbors in low trust level, they do not share any community key at all. When the central node detects a new neighbor, it will assign an initial trust value to it and updates this trust level later on, based on their interaction. We will assume that the node assigns a medium trust level to a new neighbor and shares with it the MTLCK. The central node updates the corresponding community key when a node's trust level goes up or down, and also when a node leaves the community. To protect a community key during distribution, the central node encrypts the key with the public key of the intended neighboring node before sending it.

### *Identification of nodes' malicious behavior*

In this section, we will describe how each node can compute and constantly update the node's trust in its neighboring nodes. Our approach is based on the ability of the node to identify neighboring nodes good or malicious behavior, and hence updating the trust level accordingly. A behavior is good if it confirms to the specification of the routing protocol and malicious otherwise. For our protocol, a malicious behavior happens when a node drops silently the packet without forwarding it or maliciously updating the packet before forwarding it. We call these two malicious behaviors as Malicious Dropping and Malicious Modification. A node can identify these behaviors simply by overhearing whether its neighboring node modified maliciously the message before sending it (Malicious Modification) or simply did not forward the message (Malicious Dropping). Note that for the destination node to protect its anonymity without jeopardizing its trust, it must also forward a copy of the message it receives.

## Trust-based distributed route selection mechanism

Our routing protocol requires each intermediate node that receives a route request message, to forward this message to its neighboring nodes. But in order to achieve the security and reliability of the route, our protocol uses a selection algorithm that is based on the level of trust each intermediate node has with its neighboring nodes. When a source node initiates the route discovery protocol, it specifies the trust level requirement in the initial message. Each intermediate node will propagate the message only to selected neighboring nodes, depending on the source node requested trust level. If the requested trust level is high, the node will use the community key for the neighbors with high trust level to encrypt the message; this will ensure that only highly trusted nodes will participate in the routing protocol. If the required trust level is medium, the node will use the community key for the neighbors with medium or high trust level to encrypt the message. Using this approach restricts the participation of intermediate nodes only to the ones that have a certain trust level.

## V. FUTURE WORK

Security and Privacy are one of the most challenging issues in wireless and mobile ad hoc networks (MANET). In this paper, we have developed a trust based security protocol which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we have designed a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious Our approach has several advantages when compared to previous schemes that can be summarized as follow:

(1) non-source-based routing—source node does not need to know global topology and link a availability; route computation shared among many nodes; easy adaptability to changes in network topology

(2) flexible and reliable route selection—route selection is based on the source node's trust requirement to the route and done in a distributed way in the path discovery phase according to intermediate nodes' own direct experience with its neighbor; and

(3) Resilience against path hijacking—resilience against malicious nodes compromising the communication through collusion.

In the future, we plan to implement our scheme for both proactive and reactive ad hoc routing protocols, removal of that identified malicious nodes using trust based method and evaluate its performance using an extensive simulation set of experiments.

## REFERENCES

[1] Kamanashis Biswas and Md. Ali, "Security threats in Mobile ad hoc networks", University essay from Blekinge Tek nisha Hogskola/Sektionen for Teknik (TEK), 2007.

[2] Murali Kodialam T. V. Lakshman, "Detecting Network Intrusions via Sampling: A Game Theoretic Approach", IEEE INFOCOM, 2003.

[3] Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody Sugata Sanyal, Ajith Abraham, "A Distributed Security Scheme for Ad Hoc Networks", ACM Publications, Vol-11, Issue 1, 2004, pp. 5 – 5.

[4] N. Song, L.Qian, X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach", Parallel and Distributed Processing Symposium, Proceedings, 19th IEEE International, 2005.

[5] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks", Proc. IFIP CMS, 2002.

[6] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks," Proc. 2nd Workshop Economics of Peer-to- Peer Systems, 2004.

[7] P.F. Syverson, D.M. Goldschlag, M.G. Reed, Anonymous connections and onion routing, in: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, May 1997, pp. 44–54.

[8] L. Korba, R. Song, G. Yee, Anonymous communications for mobile agents, MATA 2002; 171–181.

[9] http://www.sendfakemail.com/wraph/remailer-list.html.

[10] http://www2.pro-ns.net/wcrypto/chapter8.html.

[11] S.Madhavi and Dr. Tai Hoon Kim "AN INTRUSION DETECTION SYSTEM IN MOBILE ADHOC networks" International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.

[12] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks" in Proc. SCS CNDS, San Antonio, TX, Jan. 27–31, 2002, pp. 193–204.

[13] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in Proc. IEEE CS Workshop on Security and Assurance in ad hoc Network, Orlando, FL, Jan. 2003, pp. 379–383.

[14] P. Papadimitratos and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks," ACM MobiCom Workshop on Wireless Security (WiSe), San Diego, CA, September 2003

[15] Mahesh K.Marina and Samir R.Das, "Ad hoc On-demand Multipath Distance Vector Routing", IEEE 2001.

[16] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, no. 2,pp. 335–348, Apr.1989.

[17] P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile ad hoc networks," *Elsevier Ad Hoc Netw. J.*, vol. 1, no. 1, pp. 193–209, Jul. 2003.

[18] S. Marti, T.J.Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proc.MobiCom 2000.

[19] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks," Proc. GlobeCom 2002.

[20] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: preventing selfish in mobile ad hoc networks," Proc. WCNC'05, 2005.

[21] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," IEEE INFOCOM 2004, pp. 2404 – 2413.

[22] K. Stewart, T. Haniotakis, and S. Tragoudas, "A security protocol for sensor networks," Proc. IEEE GlobeCom 2005.

[23] A. Boukerche, Performance evaluation of on-demand routing protocols, ACM/Kluwer Mobile Networks and Applications, 2004.

[24] A. Boukerche, S. Rogers, GPS query optimization in mobile and wireless ad hoc networks, Proceedings of the Sixth IEEE Symposium on Computers and Communications, 2003 pp. 198–203.

[25] M. A. Kaafar, L. Mathy, T. Turletti and W. Dabbous. Real attacks on virtual networks: Vivaldi out of tune. In Proceedings of the SIGCOMM workshop on Large Scale Attack Defense (LSAD), September 2006.

[26] Po-Wah Yau; Mitchell, C.J., "Reputation methods for routing security for mobile ad hoc networks", Mobile Future and Symposium on Trends in Communications, 2003.

[27] Payal N Raj, Prashant B. Swadas, "DPRAODV: A Dynamic Larning System Against Blackhole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[28] Akanksha Saini, Harish Kumar," Comparision between Various Blackhole Detection Techniques in MANET", NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.