ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

Detection and Prevention of Wormhole Attack in MANETs: A Review

Renu Sharma[1], Praveen Sharma [2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & NGF College of Engineering &Technology
Palwal, Haryana, India

Abstract: ***A Mobile Ad-Hoc Network (MANET) is a self-configured or an infrastructure less set of mobile nodes that can change their geographic positions randomly such that these networks have dynamic configurations and random mobility with restrained resources. It often works by flooding the information. Its behavior is broadcasting so there is a chance to interrupt network by intruder. The no. of attack can be performed in Mobile Ad Hoc Network. This paper examined several mechanisms to determine and prevent wormhole attack and compare them.***

Keywords: MANET, Wormhole attack, Wormhole detection techniques

I. INTRODUCTION

MANETs dynamically build a temporary infrastructure-less network of mobile nodes. In this network, intermediary nodes collaborate and behave as a router and forward messages from one node to another. It is quite significant in conditions where we have lack of static network infrastructure, i.e. medical assistance, an emergency conditions or rescue operation, mine site operations, disaster relief services and military mobile network in battlefields

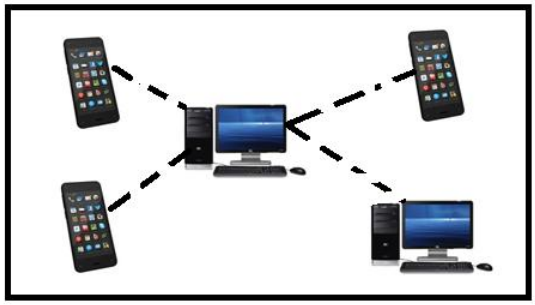

Figure 1: Mobile Ad Hoc Network

Security is offering secure interaction among mobile nodes in wireless network. There are several MANET routing protocols. It has been suggested to provide rapid and effective network restructuring and design. MANET has various challenges. They involve:

1. Multicast routing: Designing of multicast routing protocol for a constantly varying MANET atmosphere.
2. Power consumption: however the nodes in MANET network often operate on batteries and are spread in unfriendly terrains, they have unreliable power needs.
3. Dynamic Topology: The nodes move freely in network and thus the network configuration is varied.
4. Quality of service (QOS): offering constant QoS for several multimedia facilities in frequently varying atmosphere.
5. Security: The ultimate objective of the security solutions for MANET is to offer a framework dealing with confidentially, availability, authentication and integrity to assure the services to the mobile subscriber.

II. TYPES OF ATTACK

Attacks on networks come in several varieties and they can be integrated depending on different features.

a) Availability Attacks: Availability is the most general need of any network. If the networks connection ports are not reachable, or the data forwarding and routing techniques are out of order, the network would stop to present [3].

b) Packet Dropping Attack: In mobile ad hoc networks (MANETs), nodes often cooperate and send each other's packets for enabling out of range communication. Since, in hostile atmosphere, many nodes may refuse to do so, either for saving their own resources or for deliberately interrupting regular communications. This kind of misbehavior is normally known as black hole attack or packet dropping attack [4].

c) Fabricated route Attack: Fabrication attacks produce wrong routing messages. These attacks can be hard to ensure as invalid constructs, particularly in the situation of formed false messages that claim a neighbor cannot be communicated [5].

d) Resource Consumption Attack: In this attack, a harmful node deliberately attempts to consume the resources (for example bandwidth, battery power etc) of network other nodes. The attack can be of several kinds i.e. unessential route discovery, route requests, control messages, or by forwarding stale information [6].

e) Selfishness Attack: Selfishness and harmful nodes play role in route discovery phase suitably to manage their routing table, but as soon as data forwarding phase starts, they loss data packets [7].

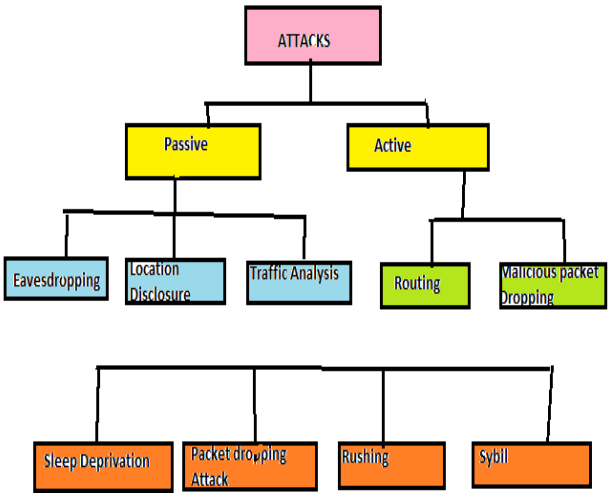

Figure 2: Classification of network layer attacks in MANETs

f. Malicious Packet Dropping

A path between a source and a destination node in a MANET is set up utilizing a route discovery mechanism. Once this has been performed, the source node begins forwarding the data packet to the adjacent node along the path; this intermediary node determines the adjacent hop node towards the destination node along the developed path and sends the data packet to it. This mechanism continues until the data packet arrives to the destination node. To obtain the required MANET operation, it is significant that intermediary nodes send data packets for all and any source nodes. Since, a dangerous node might decide to discard these packets rather than sending them; this is called a data packet dropping attack, or data sending misbehavior. In comparison of intentionally malicious nature in some situation nodes are not able to send data packets because they have low battery reserves or overloaded; instead the nodes may be selfish, for instance saving their battery for processing their own operations. Packet dropping attacks differ from grey hole and black hole attacks (look below) because there is no try to "capture" the routes in the network.

III. RELATED WORK

Geethapriya Thamilarasu et al. [1]: Here, In this paper author's Improve Reliability of Jamming Attack Detection in Ad Hoc Network using the GLoMoSim network simulator and CBR application simulation framework. For performance evaluation they used several Jammer metrics such as Jamming Rate, Malicious Node Ratio and Channel Congestion Rate. For simulation purpose authors had taken few metrics like Detection Rate, False Positive Rate. Effects of Jamming at Physical and MAC layers in a wireless ad hoc network and presented a detection algorithm to reliably detect jamming attacks are not different from collision due to hidden terminal and network congestion. For improving Detection accuracy utilized the channel utilization metric for evaluating network congestion state and performed tests to find out collision is due to jamming or network traffic conditions. After the simulation result authors conclude the effectiveness of scheme and also demonstrated that it can be used to detect attack with enhanced reliability and accuracy.

S. Raja Ratna et al. [2]: Here, In this paper author's describe various Denial of Service Attacks mitigating techniques in wireless network. To prevent the cyberspace from DOS attack this paper propose a survey on three types of DOS attack such as selective forwarding attack, pollution attack, jamming attack and its detection techniques. For Selective forwarding attack they use Channel Aware Detection (CAD) algorithm, for Pollution Attack use Digital Signature to identify pollution attack and for Jamming Attack using honey nodes for defending against jamming attack. This paper also concludes that we do not protect against jamming in all the available ways. Anti-jamming technologies should not only design and deployed but also deployed and used.

Sabbar Insaif Jasim et al. [3]: Here In this paper author's work on jamming attacks impact on the performance of mobile ad-hoc network and improvement using MANET routing protocols. For the performance evaluation author's had taken OPNET Modeler (v 14.5). In their work author's used different performance parameters for HTTP application such as Delay, Throughput, Data dropped, Traffic received and sent. The main work of this paper is studied the effect of attackers by increasing delay, data dropped traffic and decreasing throughput of the network. Four protocols were taken DSR, OLSR, TORA & GRP in order to show which of them can improve the performance of the network

in terms of parameters affected by attackers. HTTP traffic received & sent at the expense of increasing throughput and decreasing data dropped. OLSR protocol was more successful in increasing throughput and decreasing data dropped but it caused larger delay. So, some security works can be done to reduce the effect of attackers.

Ajana J. et al. [4]: Here, In this paper author's mitigate inside jammers in MANET using Localized Detection Scheme. For performance evaluation author's had taken NS2 Simulation tool for simulation purpose with taking various parameters such as 200 by 200 meters grid size, 10 nodes, simulation time 200 sec. , antenna Omni-directional with unity gain, No fading radio model with range of 376 meters, routing protocol AODV. For evaluation of performance metrics parameters such as throughput and delay. In this paper author's proposed a method that acts as a LDS for identifying inside Jammers in MANET and also compare the performance of LDS and a cluster organized network. After the simulation results authors conclude by using the algorithm delivery ratio & signal strength is less efficient in clustered algorithm and it also managing the reputation values that create a little overhead. By mitigating jamming attacks, bandwidth utilization can be improved & hence improve the overall network efficiency. It also shows that LDS is better than the clustered approach.

Bo Sun et al suggested a detection technique known as Neighborhood-based technique to find the black hole attack and a recovery routing protocol to create a proper route to destination node [2]. In neighborhood-based technique we can detect harmful nodes in network and the source node forwards a changed route entry control packet to destination in route recovery protocol so that source node will forward packets to destination node by re-routing. In this technique, we obtained lower detection time and higher throughput but this technique is not good when the attackers forward the fraud response packets. In Multiple Route Replies (MRR) technique [2], source node expects for multiple RREP (Route reply) packets form network nodes. After getting more than two RREP packets, the source checks whether there is a common hop in the route or not. If there is any common hop then source node assures as the path is secure and it begins forwarding packets along this route. But limitation of this technique is time delay because source code requires expecting for many RREPs. In Watchdog process e node each will listen to the adjacent node for identifying the miss conducting node in network. If any node in active route is losing packets greater than threshold value then source node is advised. But this process fails in detecting misbehaving node in some situations [3]. Let us take one example, consider 1-2-3 is route in network. The node 1 may not be able in detecting misbehaving node in the following situations.

1. When node 1 is hearing to node 2, if a collision happens in node 1then node 1 cannot detect whether this collision is because of sending packets by node 2(well behaving) or any another node in the network forwarding packets to node 1 while node 2(misbehaving node) is not transmitting the packets.
2. If node 2 propagation is not strong so that node 3 does not obtained the packets from node 2, but node 1 finds that mobile node 2 sent the packets.
3. If node 3 does not obtained packets due to collision at mobile node 3, but node 2 is not re-sending the packets.
4. If both nodes 2 and 3 are not well behaving nodes, node 2 propagate the packets to node 3 but node 3 losing the packets and node 2 not communicating to node 1.
5. If node 2 is losing packets but lower than the threshold value then node 1 can detect that node is not well behaving.

In Pathrater technique, it holds a rate for each node in network such as a node is decreased when a node is detected as misbehaving node [4]. These node rates are utilized to find the most authentic path to destination. But this technique also has the same limitations as watchdog process i.e. limited transmission power, receiver collisions.

IV. ROUTING PROTOCOLS

Routing protocol in MANET can be categorized as

A. Proactive Routing Protocol

In proactive routing [1], mobile nodes periodically flood their routing information to the adjacent node. Every node requires to manage the records of the next and reachable nodes with a no. of hops. Nodes have to measure their neighborhood as per the network configuration change. It is also known as table-driven routing protocol. These kinds of protocols are Optimized Link State Routing (OLSR) protocol and Destination Sequenced Distance Vector (DSDV) routing protocol. Global State Routing (GSR), Wireless Routing Protocol (WRP), Zone Based Hierarchical Link State Routing Protocol (ZHLS) and Clustered Gateway Switch Routing Protocol (CGSR) are also proactive routing protocols.

B. Reactive Routing Protocol

Reactive routing [1] protocol is known as on-demand routing protocol. If there is no interaction then it is not managing routing information. If a node wishes to forward packet to another node then the protocol has to look for the path in on demand. It has to set up

the link for transmitting and obtain the packet. It is simply began when nodes want to transmit data packets. Reactive routing protocols and On-demand routing protocols are Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV). Temporally Ordered Routing Algorithm (TORA), Clustered Based Routing Protocols (CBRP), Signal Stability Routing (SSR) and Associatively Based Routing (ABR) are also reactive routing protocols.

C. Hybrid Routing Protocol

Hybrid routing [1] protocol is integration of reactive and proactive routing protocol's benefits. It overcomes on the drawbacks of these protocols. This protocol depends on layered or hierarchical network framework. There are two Hybrid routing protocol i.e. temporally-ordered routing algorithm (TORA) and zone routing protocol (ZRP) and.

D. AODV Routing Protocol

Ad hoc on-demand distance vector (AODV) routing protocol is an on demand routing protocol for discovering routes and a route is set up only when it is needed by source node for transferring of data packets [5]. AODV utilizes a sequence no. It employs a destination sequence nos. to determine the fresher path. AODV has three types of message RREQ, RREP, RERR. In an AODV, the source node floods the Route Request (RREQ) packet in the network when the route is not existed for the preferred destination node. A node manages its path information only if the DesSeqNum (destination sequence no.) of the current packet obtained is more than the last DesSeqNum (destination sequence no.) saved at the node. A Route Request (RREQ) [4] has six parameter, (1)The source identifier (SrcID), (2)The destination identifier (DesID), (3)The source sequence number (SrcSeqNum), (4)The destination sequence number (DesSeqNum), (5)The broadcast identifier (BcastID), and (6)The time to live (TTL) field. When an intermediary node obtains a Route Request (RREQ), it either sends it or offers a Route Reply (RREP) if it has a valid route to the destination node. The route is proper or not at the middle node is found by comparing the sequence no. (Seq) at the intermediary node with the destination sequence no. (DesSeqNum) in the route request (RREQ) packet. All middle nodes having valid routes to the destination node or the destination node itself, only those nodes are allowed to forward Route Reply (RREP) packets to the source node. When a node obtains a Route Reply (RREP) packet, data or information about the previous node from which the packet is obtained is also reserved for forwarding the data packet to this adjacent node as the adjacent hop against the destination node. AODV does not re-establish a not working path temporary but at the same time of connection breaks. It is detected by observing the periodical beacons or via link-level acknowledgements, the end nodes are announced. Thus, source node came to aware about the route break and it reestablish a route to the destination node if needed by higher layers. If route break is determined at an intermediary node, the node warns the end nodes by forwarding a voluntary Route Response with the hop count adjusted as infinity.

3. Security Attacks

A. Flooding Attack

In a flooding attack, a dangerous node takes a benefit of the route discovery mechanism of the AODV routing protocol. The dangerous node targets to broadcast the network with a huge no. of RREQs to missing destinations in the network which considers a lot of the resources of network. However the destination does not available in the network, a RREP packet cannot be created by any network node and all the nodes continue flooding the RREQ packet. When large no. of fraud RREQ packets is flooded into the network, new routes can no longer be appended to the network. And the network is not able to transfer data packets, which causes to network congestion and flood the route table in the intermediary nodes so that the nodes are not able to obtain new RREQ packet, which leads to a DoS attack.

B. Black hole Attack In a black hole attack, a dangerous node observes the network traffic and discards all packets. To carry out with a black hole attack, a dangerous node waits for coming RREQ packets from other nodes. When RREQ message obtained at the dangerous node, without examining its routing table, the harmful node instantly forwards a wrong RREP with a large sequence no. with zero hop count to spoof its neighboring nodes that it has the best route to the destination node. The harmful node response will be obtained by the source before any response is obtained from other nodes. When source node obtains numerous RREP, it chooses the RREP with the highest destination sequence no. and the least hop count. Then the source node neglects other RREP packets and begins forwarding data packets over the dangerous node. When the data packets transferred by the source node and it is arrived to the black hole node, at that interval it discards the packets before transmit them to the destination.

C. Gray hole Attack A gray hole [3] may send all the packets to specific nodes but may discard those packets incoming from or targeted to some particular nodes. In another variation of this attack, a node may act harmfully for some time but after that it acts normally. Sometimes, a node may integrate the behavior of attacks explained above. Because of this doubt in behavior of gray hole, this kind of attacks

are more complex to detect/prevent in comparison of black hole attack. Same as black holes, cooperative gray hole attacks may be possible against AODV.

D. Worm hole Attack A security attack, known as the wormhole attack [9], has been proposed in the ad hoc networks background. In this kind of attack, a dangerous node picks packets from one location in the network. Dangerous node tunnels this packet to another harmful node at a distant point which replays this packet temporary. The tunnel can be identified in several ways such as out-of-band and In-band channel. This builds the tunneled packet get there either rapidly or with a slighter no. of hops in comparison of the packets transferred over normal multi hop routes. This generates a wrong impression that the two end points of the tunnel are very nearest to each other implies that that one is a shorter route. But it is utilized by harmful nodes to disrupt the right operation of ad hoc routing protocols. They can then establish several attacks against the data traffic flow i.e. replay attack, selective dropping, eavesdropping etc. Wormhole can be made utilizing, first, in-band channel where dangerous node m1 tunnels the obtained RREQ packet to another dangerous node m2 utilizing encapsulation even though there is one or more nodes between two dangerous nodes, the nodes adopting m2 nodes trust that there is no node between m1 and m2. Second, out-of-band channel where two dangerous nodes m1 and m2 use a physical channel between them by either dedicated wired connection or long range wireless connection depicted in Figure.

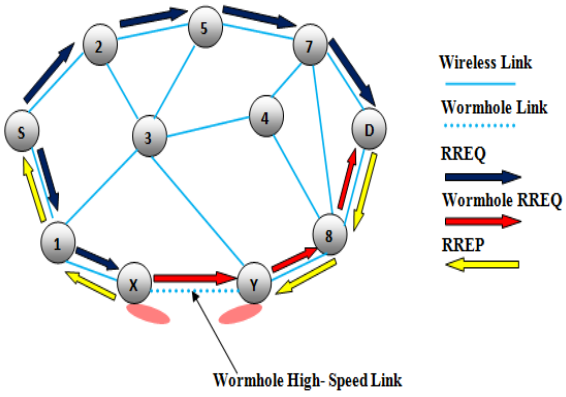

Figure 2: Wormhole attack

4. Literature Survey

The several methods utilized for the detection and prevention of wormhole attack in MANET is explained below:

A. Packet Leashes In this paper [6], the approach is utilized to determine wormhole attack. Two kinds of Leashes: Temporal Leashes and Geographical Leashes. Temporal Leashes depends on time of forwarding and obtaining packets from 1 node to another node. Geographical Leashes depends on nodes location.

1. *Temporal Leashes:* All nodes must require strongly synchronized clock. It depend on off- the - shelf hardware.
2. *Geographical Leashes:* There is no need of clock synchronization. It needs GPS hardware. In this approach when one node forward a packet to another node then it append its own location ps and time on which it forwards a packet ts. The recipient compare the value of forwarding packet with its own location pr and time at which it obtains packet tr.

B. Directional Antennas It is a hardware based technique [7] in which every node is fitted with directional antennas that interact with each other, nodes utilize particular sectors of antennas and realize the direction of obtained signal. If the directions of both the pairs match then relation is set. This technique fails if an intruder deliberately places the wormhole between the interacting nodes.

C. Digital Signature This paper [8] introduces a technique which is helpful to prevent a wormhole attack in ad hoc network is analyze a digital signature of a forwarding nodes by obtaining node. All nodes consists digital signature of each other legitimate nodes of current network. Generate an authorized path between receiver and sender with the support of verifying of digital signature. If dangerous node available it is detected because that node does not have valid digital signature.

D. Neighbour Node Analysis

In this paper [10] neighboring node mechanism examine the whole neighboring nodes for the objective of authentication, so that protected transmission can be happen throughout the wireless network. This mechanism utilizes request and response technique. Node will forward a request to its all neighboring nodes. The node will manage a table which buffer a response time. If response time is not accurate there is a malicious node in the current network. The reply time of RREP message is compared to the reply time of original message forwarded. If reply time of original message is more as compared to the reply time of RREP + threshold value then we can say that wormhole connection is available in the route. Comparison of this phenomenon is repeated till the destination arrived.

E. DelPHI technique Delay Per Hop Indication [9] depend on the calculation of (delay per hop) value of disjoint paths. It depends on the fact that under general situation, the delay a packet observes in propagates one hop should be comparable along every hop path. While in wormhole attack, the delay

for traversing across fraud neighboring nodes are high as there are several hops between them. It doesn't require any additional hardware or tight time synchronization and has high power efficiency [9]. It runs for both Out-of-Band and In–Band mode.

F. WHOP technique This paper [12] introduces a routing protocol WHOP (Wormhole Attack Detection Protocol employing Hound Packet), which depends on AODV protocol. In WHOP, a hound packet will be forward after the route has been disclosed utilizing AODV routing protocol, the hound packet will be processed by each node except nodes who were included in route from source node to destination node during path establishment. WHOP consist other three column address of node processing bit (PB) and count to reach next hop (CRNH). CRNH shows the hop difference between neighboring nodes of one hop separated node; its value will be increased by every node for the first node entry whose bit of processing is zero in the packet.

6. Conclusions

MANET is a WAN in which security is major issue. In this paper, we have examined the various kinds of protocols and attacks which decrease the network performance. Also several mechanisms are compared to determine and prevent wormhole attack. WHOP doesn't need important change in AODV. It only appends additional packet known as hound packet. Detection is performed without help of any hardware.

REFERENCES

[1] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[2] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[3] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[4] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole

[5] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[6] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference,

[7] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[8] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

[9] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[10] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[11] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.

[12] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[13] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[14] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[15] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[16] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.

[17] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[18] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[19] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.