International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

Nearest Neighbour based Security Scheme against Black Hole attack in MANET

Swati Saxena
Computer Science & Engineering
NIIST Bhopal
swtsaxena14@gmail.com

Assistant Prof Ms. Sini Shibu
Computer Science & Engineering
NIIST Bhopal
Sini.Shibu09@gmail.com

Abstract----- Security is one of the major issues in Mobile Ad hoc Network (MANET). Due to unique characteristics of MANETS, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a dominant security solution that achieves both extensive protection and desirable network performance. This work analyses the effect of cooperative attack which is probable attacks in ad hoc networks. In this attack, a malevolent node or malicious node impersonates a target node by sending a spoofed route reply packet to a source node which initiates a route discovery. Mobile ad hoc networks may be unprotected against attacks by the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination by that due to this attack, data loss will occur. The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets delivered through them. In this paper we proposed a simple IDS Algorithm against black hole attack and measure the network performance after applying IDS. We simulated black hole attacks in network simulator 2 (ns-2) and measured the packet loss in the presence of black hole and in presence of Intrusion Detection System against Black hole attack. Our solution improved the 80% network performance in the presence of a black hole attack.

Keywords: **- Black-hole attack, IDS, Routing, AODV, Security.**

I INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes

the node consume its battery in addition to losing packets. In our study, we simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. We made our simulations using NS-2 (Network Simulator version 2) simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though NS-2 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Black Hole attacks, we first added a new Black Hole protocol into the NS-2. We started our study by writing a new AODV protocol using C++, to simulate the Black Hole attack. Having implemented a new routing protocol which simulates the Black hole we performed tests on different topologies to compare the network performance with and without Black holes in the network. As expected, the throughput in the network was deteriorated considerably in the presence of a Black hole. Afterwards, we proposed an IDS solution to eliminate the Black Hole effects in the AODV network.

1.1. Routing In MANETs

MANETs have special limitation and properties such as limited bandwidth and power, highly dynamic topology, high error rates etc., explained in the preceding sections. Moreover, compared to infrastructure based networks, in a MANET, all nodes are mobile and can be connected dynamically in an arbitrary manner. Nodes of MANET behave as router and take part in discovery and maintenance to establish a reliable route of each other. Therefore, routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs. These routing protocols are divided into two categories [3] based on management of routing tables.

1.1.1. Table Driven Routing Protocols

- In Table Driven Routing Protocols, each node has to keep up-to-date routing tables. To maintain reliable routing tables, every node propagates the update messages to the network when the network topology changes. Because every node has information about network topology, Table Driven Routing Protocols present several problems.
- Periodically updating the network topology increases bandwidth overhead,
- Periodically updating route tables keeps the nodes awake and quickly exhaust their batteries,
- Many redundant route entries to the specific destination needlessly take place in the routing tables.
- Destination-Sequenced Distance Vector Routing Protocol (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR), Fisheye State Routing (FSR), Hierarchical State Routing (HSR), Zone-based Hierarchical Link State Routing Protocol (ZHLS) and Cluster head Gateway Switch Routing Protocol (CGSR) are Table Driven Routing Protocols.

1.1.2. On-Demand Routing Protocols

These protocols take a lazy approach to routing. [5] Compared to Table Driven Routing Protocols; On-Demand Routing Protocols are not maintained periodically, route tables are created when required. When the source node wants to connect to the destination node, it propagates the route request packet to its neighbours. Just as neighbours of the source node receive the broadcasted request packet, they forward the packet to their neighbours and this action is happen until the destination is found. Afterward, the destination node sends a replay packet the source node in the shortest path. The route remains in the route tables of the nodes through shortest path until the route is no longer needed. Cluster based Routing Protocols (CBRP), Ad-Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing Protocol (DSRP), Temporally Ordered Routing Algorithm (TORA), Associativity Based Routing (ABR), Signal Stability Routing (SSR) are On-Demand Routing protocols.

In our work, we have used Ad-Hoc On-Demand Distance Vector Routing (AODV) and implemented Black Hole attack to this protocol.

1.1.3. Gray Hole Attack (Routing Misbehaviour)

Gray-hole attacks are an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighbouring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehaviour. [2] Dropping packets is also one of the behaviours of failed or overloading nodes [6]. One should not evaluate every dropping packet action as a selective existence, Gray-hole attack. Actually most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception. [9, 10]

1.1.4. Black Hole Attack

The difference of Black Hole Attacks [11, 12, 15] compared to Gray Hole Attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighbouring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole similar to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the centre of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack. Gray hole attacks against one or two nodes in the network to isolate them, whereas black hole attack affects the whole network. Moreover, the malicious node that attempts gray-hole attacks cannot be perceived easily since it does not send false messages. Behaviour of failed or overloaded nodes may seem like selfish nodes attacks or gray-hole attacks due to dropping of messages. But, since failed nodes cannot fabricate a new control message, they cannot form a black hole attack although they will drop the message later.

II BLACK HOLE ATTACK IN AODV ROUTING PROTOCOL

Initially, we should take into account Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol and then we shall explain Black Hole Attack and Prevention through IDSAODV. Our aim to protect the Mobile ad-hoc network through Black Hole Attack, Intrusion Detection System aimed to securing the AODV protocol using our Intrusion Detection system. They conclude that AODV performs well at all mobility rates and movement speeds. However, we argue that their definition of mobility does not truly represent the dynamic topology of MANETs. In this thesis, the work of has been extended and the proposed protocol is called IDSAODV (Intrusion Detection System AODV). In our work, we make use of AODV based intrusion detection. Our Intrusion Detection and Response Protocol for MANETs

have been demonstrated to perform better than that AODV protocol and presence of Black Hole Attack, in terms of false positives and percentage of packets delivered. Since the earlier work do not report true positive i.e. the detection rate, we could not compare our results against that parameter with proposed method. The implementation of the IDSAODV protocol reported in this thesis has shown to work in real life scenarios. IDSAODV performs real time detection of attacks in MANETs running AODV routing protocol. Experimental results validate the ability of our protocol to successfully detect both local and distributed attacks against the AODV routing protocol. The algorithm also imposes a very small overhead on the nodes, which is an important factor for the resource constrained nodes.

2.1.1 AODV Protocol

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. It borrows most of the advantageous concepts from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers from DSDV make the algorithm cope up with topology and routing information. Obtaining the routes purely on-demand makes AODV a very useful and desired algorithm for MANETs

2.1.1.1 Working of AODV

Each mobile host in the network acts as a specialized router and routes are obtained as needed, thus making the network self-starting. Each node in the network maintains a routing table with the routing information entries to its neighbouring nodes, and two separate counters: a node sequence number and a broadcast-id. When a node (say, source node 'S') has to communicate with another (say, destination node 'D'), it increments its broadcast-id and initiates path discovery by broadcasting a route request packet RREQ to its neighbours. Step by step explanation of is as follows:

- Source 'S' has to send data to destination.
- S sends RREQ to its neighbours A, B, C.
- B finds the path in its routing table (with destn seq-number s1 and hop count c1) and sends RREP to S.
- C sets up reverse path.
- C forwards RREQ to its neighbours D and E.
- E sets up reverse path.
- E forwards RREQ to its neighbours F and G.
- E deletes the reverse path after a time out period as it does not receive any RREPs from F and G.
- D finds the path (with dest seq-number s2 which is greater than s1 and hop count c1) in its routing table and sends RREP to C.
- C receives RREP from D and sets up forward path and forwards RREP to S. **(change)**

2.1.1.2 Advanced uses of AODV

Maximum utilization of the bandwidth: This can be considered the major achievement of the algorithm. As the protocol does not require periodic global advertisements, the demand on the available bandwidth is less. And a monotonically increased sequence number counter is maintained by each node in order to supersede any stale cached routes. All the intermediate nodes in an active path updating their routing tables also make sure of maximum utilization of the bandwidth. Since, these routing tables will be used repeatedly if that intermediate node receives any RREQ from another source for same destination. Also, any RREPs that are received by the nodes are compared with the RREP that was propagated last using the destination sequence numbers and are discarded if they are not better than the already propagated RREPs.

Simple: It is simple with each node behaving as a router, maintaining a simple routing table, and the source node

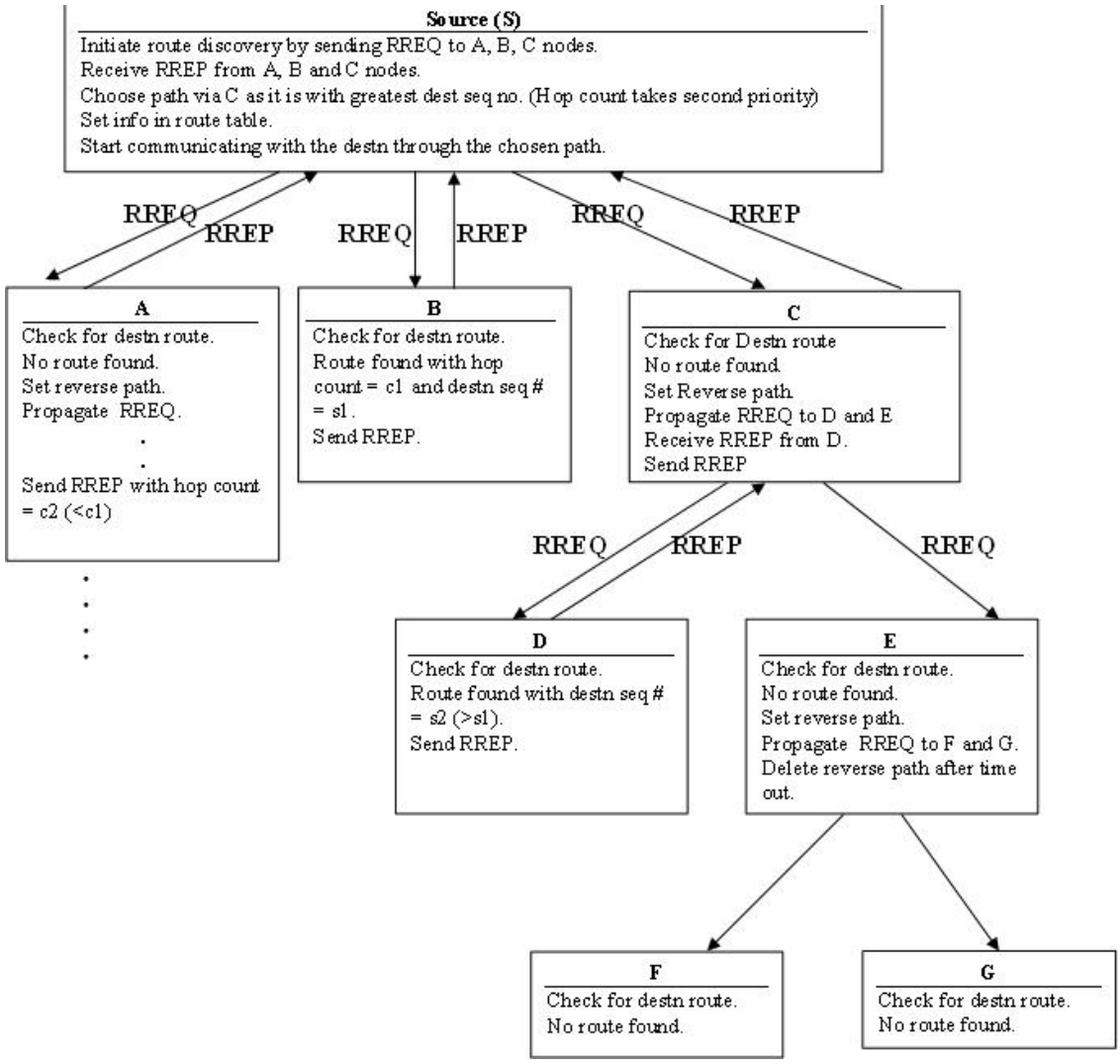
International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 01 (JAN-FEB, 2016)

initiating path discovery request, making the network self-starting.

Most effective routing info: After propagating an RREP, if a node finds receives an RREP with smaller hop-count, it updates its routing info with this better path and propagates.

Most current routing info: The route info is obtained on demand. Also, after propagating an RREP, if a node finds receives an RREP with greater destination sequence number, it updates its routing info with this latest path and propagates.

Loop-free routes: The algorithm maintains loop free routes by using the simple logic of nodes discarding non better packets for same broadcast-id.



Step by step explanation of AODV Protocol

Coping up with dynamic topology and broken links: When the nodes in the network move from their places and the topology is changed or the links in the active path are broken, the intermediate node that discovers this link breakage propagates an RERR packet. And the source node

re-initializes the path discovery if it still desires the route. This ensures quick response to broken links.

Highly Scalable: The algorithm is highly scalable because of the minimum space complexity and broadcasts avoided when it compared with DSDV [6].

2.1.1.3 Limitations/Disadvantages of AODV

- Requirement on broadcast medium: The algorithm expects/requires that the nodes in the broadcast medium can detect each other's broadcasts.
- Overhead on the bandwidth: Overhead on bandwidth will be occurred compared to DSR, when an RREQ travels from node to node in the process of discovering the route info on demand, it sets up the reverse path in itself with the addresses of all the nodes through which it is passing and it carries all this info all its way.
- No reuse of routing info: AODV lacks an efficient route maintenance technique. The routing info is always obtained on demand, including for common cause traffic.
- It is vulnerable to misuse: The messages can be misused for insider attacks including route disruption, route invasion, node isolation, and resource consumption.
- AODV lacks support for high throughput routing metrics: AODV is designed to support the shortest hop count metric. This metric favours long, low bandwidth links over short, high-bandwidth links
- High route discovery latency: AODV is a reactive routing protocol. This means that AODV does not discover a route until a flow is initiated. This route discovery latency result can be high in large-scale mesh networks.

2.2 Black Hole Attack

Black Hole Attack is briefly explained in the previous Chapter. In this Chapter we shall explain it in more detail as we have already explained the AODV protocol. In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behaviour in the scenario the previous section. We assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 intermediate node between Node 1 and Node 4 so initially in case of route requesting time Black Hole Node 3 immediate send false RREP, Where sender node receive route reply packet, sender node sends actual data packet through Black Hole Node 3, Black Hole Node 3 Receives data packets, if data packets are UDP then this packets Capture by the Black Hole Node and if TCP type packet then Block This type Packets By Malicious Node. So our Network has infected. In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.

2.3 Solution for Black Hole Attack and IDS its Effects

In the two previous sections, we explain how Black Hole Attack is implemented in NS2 and which the results are obtained from the simulations. When we examine the trace file of the simulations that include one Black Hole node, we saw that after a while second RREP message came to source node from the real destination node.

3.2.1 Proposed Solution in NS-2

To evaluate effects of the proposed solution, we first needed to implement it in NS-2. Therefore, we cloned the "AODV" protocol, changing it to "IDSAODV" as we did "black hole" before. To implement the black hole we changed the receive RREP function (recvRequest) of the black hole AODV.cc file but to implement the solution we had to change the receive RREP function (recvReply) and create RREP caching

mechanism to count the second RREP message. The RREP caching mechanism "rrep_insert" function is for adding RREP messages, "rrep_lookup" function is for looking any RREP message up if it is exist, "rrep_remove" function is for removing any record for RREP message that arrived from defined node and "rrep_purge" function is to delete periodically from the list if it has expired. We chose this expire time "*BCAST_ID_SAVE*" as 6 (means 3 seconds). In the "recvReply" function, we first control if the RREP message arrived for itself and if it did, function looks the RREP message up if it has already arrived. If it did not, it inserts the RREP message for its destination address and returns from the function. If the RREP message is cached before for the same destination address, normal RREP function is carried out. Afterwards, if the RREP message is not meant for itself the node forwards the message to its appropriate neighbour.

III PROPOSED IDS ALGORITHM

Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not. In Intrusion detection system (IDS) , every node needs to have two additional small-sized tables; one to keep last-packet-sequence-numbers for the last packet sent to every node and the other to keep last-packet-sequence-numbers for the last packet received from every node (from node through node). These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbours. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last- packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last-packet-sequence-numbers received from the source by this intermediate node. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol. Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not. The IDS are identified the black hole attacker.

```
{
    If ( S send RREQ_B) // S is the sender and D is the destination
    {
    rtable -> insert(rtable->rt_nexthop);
    Add extra filed to rtable (next_hop , Through)
      Identified in previous No data through that hop;
        But exist in rtable enetry ; //Check reliability
            if next hop(next_hop is unrelaible);
                    {
                      Block that Hop ;
                    }
                    else
                    {
                      Send RREQ_B till the Destination
                      Else
                          Send_RREQ_B to next other hop ;
                          Search destination D;
                    }
    }
}
```

IV SIMULATION PARAMETER

We get Simulator Parameter like Number of nodes, Dimension, Routing protocol, traffic etc. According to below table 6.1 we simulate our network. In this section we present a set of simulation experiments to evaluate this protocol by comparing with the original AODV [5].

4.1 Nam visualization of Black hole Node and IDS Node.

This simulation described in this project was tested using the ns-2 test-bed that allows users to create arbitrary network topologies [8]. By changing the logical topology of the network, ns-2 users can conduct tests in an ad hoc network without having to physically move the nodes. Ns-2 controls

the test scenarios through a wired interface, while the ad hoc nodes communicate through a wireless interface. In this section we present a set of simulation experiments to evaluate this protocol by comparing with the original AODV [5]. In this figure we represent the "nam" scenario of thirty nodes in which node 28 are the Black hole node and 29 are IDS node and rest of them are normal nodes. All the nodes are mobile nodes first they sensing the neighbour for route establishment and after that starting data transferring.

Number of nodes	**30**
Black hole node	1
Dimension of simulated area	800×600
Routing Protocol	AODV
Simulation time (seconds)	100
Transmission Range	250m
Traffic type	CBR
Packet size (bytes)	512
Number of traffic connections	20, 8
Maximum Speed (m/s)	30

Table 6.1 Simulation parameter

V CONCLUSION & FUTURE SCOPE

We simulated attack in the ad-hoc networks and find its affects. In our study, we used the AODV routing protocol. But the other various routing protocols could be simulated also. In this synopsis, we try to resolve cooperative effect in the network. But the detection of the black hole attack is possible through proposed IDS security scheme. Our solution looks the path in the AODV level. As malicious node is the main security threat that effect the performance of the AODV routing protocol. Effect on packet loss is clearly visualized in throughput and other metrics. As malicious node is the main security threat that effect the performance of the AODV routing protocol. Its detection is the main matter of concern. Therefore the proposed IDS algorithm work will be excellent to detect and defence the network from Black Hole attack. Improvement for overcoming the effect of Black hole should orient towards controlling the delay. In future some techniques should be proposed for reducing end to end delay. Also Black hole for AODV routing algorithm can be implemented in real life scenario and its analysis can be compared with the analysis results.

REFERENCES

[1] T. Franklin, "Wireless Local Area Networks", Technical Report http://www.jisc.ac.uk/uploaded_documents/WirelessLANTechRep.pdf. 25 July 2010.

[2] www.cs.cmu.se/education/examina/Rapporter/ClaesGahlin.pdf.

[3] P. Misra, "Routing Protocols for Ad Hoc Mobile Wireless Networks", http://www.cse.wustl.edu/~jain/cis788-99/ adhoc_routing/index.html, 14 May 2006.

[4] P. Yau and C. J. Mitchell, "Security Vulnerabilities in Adhoc Network".

[5] SCOTT CORSON AND JOSEPH MACKER, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations". Internet-Draft, draft-ietf-manet-issues-01.txt, March 2008.

[6] Hao Yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications, February 2010.

[7] Charles E. Perkins and Elizabeth M. Royer. "Ad-Hoc on- Demand Distance Vector Routing". In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pages 90–100, February 1999.

[8] C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[9] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June2002, pp. 3-13.

[10] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc.8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[11] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks In Proceedings of the 10thIEEE International Conference on Network Protocols (ICNP' 02), 2002.

[12] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks," Proc. 2nd ACM Symposium Mobile Ad hoc Networking and Computing (Mobihoc'01), Long Beach, CA, October 2001, pp. 299-302.

[13] Y. Zhang and W. Lee, "Intrusion detection in wireless ad – hoc networks," 6th annual international Mobile computing and networking Conference Proceedings, 2000.

[14] T. Anantvalee and J. Wu. "A Survey on Intrusion Detection in Mobile Ad Hoc Networks", Book Series Wireless Network Security, Springer, pp. 170 – 196, 2007.

[15] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in ICPP Workshops, pp. 73, 2002.

[16] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.

[17] E. A .Mary Anita, V. Vasudevan ," Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining", International Journal of Computer Applications, Volume 1 – No. 12, 2010.

[18] Bhargava, Monika Roopak and Dr. B Reddy, "Performance Analysis of AODV Protocol under Black Hole Attack", International Journal of Scientific & Engineering Research, Volume 2, Issue 8, 2011.

[19] Akanksha Saini, Harish Kumar "COMPARISON BETWEEN VARIOUS BLACK HOLE DETECTION TECHNIQUES IN MANET" NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010.

[20] Nishant Sitapara, Prof. Sandeep B. Vanjale "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks" International Conference" ICETE-2010" on Emerging trends in engineering on 21st Feb 2010.

[21] Mohammad Al-Shurman, Seong and Seungjin Park "Black Hole Attack in Mobile Ad Hoc Networks Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, April 2004.

[22] Satria Mandala, Md. Asri Ngadi, A .Hanan Abdullah "A Survey on MANET Intrusion Detection" International Journal of Computer Science and Security, Volume 2 No.1, 2009.

[23] G.S. Mamatha and Dr. S.C. Sharma "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey" International Journal of Computer Applications, Volume 9 No.9, November 2010

[24] www.cs.cmu.se/education/examina/Rapporter/ClaesGahlin.pdf.