# Comparative Analysis of Routing Security in Manet

Nidhi Sehrawat
*Department of Computer Science and ApplicationEngineering*
*Ganga Institute of Technology & Management (Jhajjar)*

Puneet Garg
*Department of Electronics and Communication Engineering*
*Ganga Institute of Technology & Management (Jhajjar)*

**Abstract—Mobile Ad-Hoc Networks (MANETs) are autonomous and decentralized wireless systems. Mobile Ad hoc Network is a collection of mobile nodes in which the wireless links are frequently broken down due to mobility and dynamic infrastructure. Routing is a significant issue and challenge in ad hoc networks. Many Routing protocols have been proposed so far to improve the routing performance and reliability. This research paper describes the characteristics of ad hoc routing protocols Ad-hoc On Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), Hybrid Routing (ZRP) based on the performance metrics like Average delay, Throughput under low mobility and low traffic network as well as under high mobility and high traffic network for Black hole effect and Daniel of Service(DoS) using NS-2. Results show that AODV has maximum throughput under low traffic and DSDV has maximum throughput under high traffic. As network becomes dense DSR perform well in terms of Throughput than AODV and DSR and ZRP.**

**Keywords: Mobile Ad-Hoc Networks**

## I. INTRODUCTION

### *1.1 AODV routing protocol*

Reactive protocols seek to set up routes on-demand. If a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route.
The *Ad-Hoc On-Demand Distance Vector* routing protocol is described in RFC 3561. The philosophy in AODV, like all reactive protocols, is that topology information is only transmitted by nodes on-demand. When a node wishes to transmit traffic to a host to which it has no route, it will generate a *route request*(RREQ) message that will be flooded in a limited way to other nodes. This causes control traffic overhead to be dynamic and it will result in an initial delay when initiating such communication. A route is considered found when the RREQ message reaches either the destination itself, or an intermediate node with a valid route entry for the destination. For as long as a route exists between two endpoints, AODV remains passive. When the route becomes invalid or lost, AODV will again issue a request. AODV avoids the *``counting to infinity*'' problem from the classical distance vector algorithm by using sequence numbers for every route. The counting to infinity problem is the situation where nodes update each other in a loop. A is not updated on the fact that its route to D via C is broken. This means that A has a registered route, with a metric of 2, to D. C has registered that the link to D is down, so once node B is updated on the link breakage between C and D, it will calculate the shortest path to D to be via A using a metric of 3. C receives information that B can reach D in 3 hops and updates its metric to 4 hops. A then registers an update in hop-count for its route to D via C and updates the metric to 5. And so they continue to increment the metric in a loop.

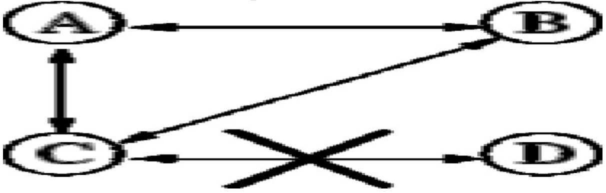


Figure 1- A scenario that can lead to the ``counting to infinity'' problem

The way this is avoided in AODV, for the example described, is by B noticing that As route to D is old based on a sequence number. B will then discard the route and C will be the node with the most recent routing information by which B will update its routing table. AODV defines three types of control messages for route maintenance: **RREQ** - A *route request* message is transmitted by a node requiring a route to a node. As an

optimization AODV uses an *expanding ring* technique when flooding these messages. Every RREQ carries a *time to live* (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted(i.e. the packets that initiated the RREQ) *should* be buffered locally and transmitted by a FIFO principal when a route is set.
**RREP** - A *route reply* message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator. **RERR** - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ``precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination. Node A wishes to initiate traffic to node J for which it has no route.A broadcasts a RREQ which is flooded to all nodes in the network.

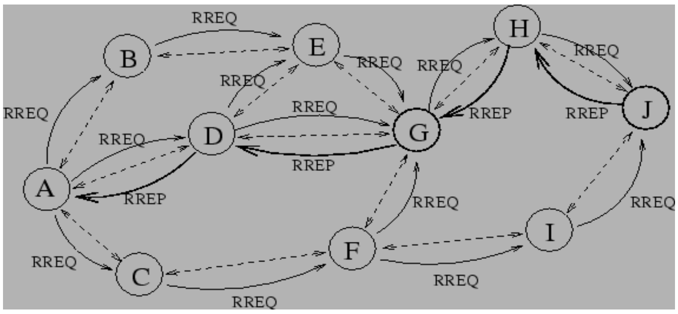


Figure 2 A possible path for a route reply if A wishes to find a route to J

When this request is forwarded to J from H, J generates a RREP. This RREP is then unicasted back to A using the cached entries in nodes H, G and D.

### *1.2 DSR Routing Protocol*

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.
DSR has been implemented by numerous groups, and deployed on several testbeds. Networks using the DSR protocol have been connected to the Internet. DSR can interoperate with Mobile IP, and nodes using Mobile IP and DSR have seamlessly migrated between WLANs, cellular data services, and DSR mobile ad hoc networks.
The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use.
The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes, and is designed to work well with even very high rates of mobility.

### *1.3 Hybrid Routing Protocol*

Hybrid protocols seek to combine the proactive and reactive approaches. An example of such a protocol is the *Zone Routing Protocol*(ZRP).

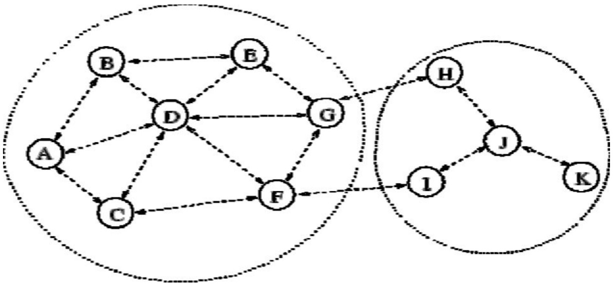


Figure 3-A ZRP scenario showing the zones of node A and node J using a r value of 2. Within the zones a pro-active routing protocol is used while a reactive protocol I used between zones

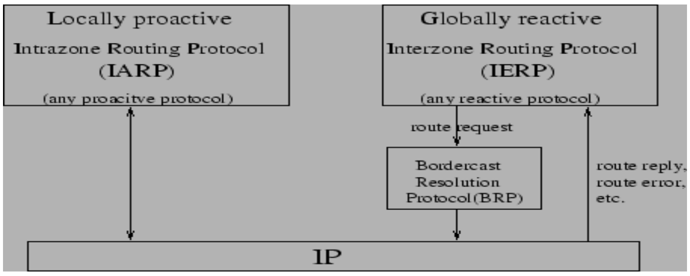


Figure 4-The different components of the Zone Routing Protocol.

ZRP divides the topology into zones and seek to utilize different routing protocols within and between the zones based on the weaknesses and strengths of these protocols. ZRP is totally modular, meaning that any routing protocol can be used within and between zones. The size of the zones is defined by a parameter *r* describing the radius in hops.Intra-zone routing is done by a proactive protocol since these protocols keep an up to date view of the zone topology, which results in no initial delay when communicating with nodes within the zone. Inter-zone routing is done by a reactive protocol. This eliminates the need for nodes to keep a proactive fresh state of the entire network.

## II. Proposed Algorithm

### *2. Black Hole Attack*

### *2.1 BLACK HOLE ATTACK IN AODV*

In Black hole attack a malicious node advertises about the shortest path to the node whose packets it wants to intercept.In following figure, imagine, M is malicious node. When node A broadcasts a RREQ packet, nodes B, D and Mreceive it. Node M, being a malicious node, this node does not check up with its routing table for the requested route to node E. Hence, it immediately sends back a RREP packet, claiming that it has a route to the destination. Node „A‟ receives the RREP from M ahead of the RREP from B and D. Node A assumes

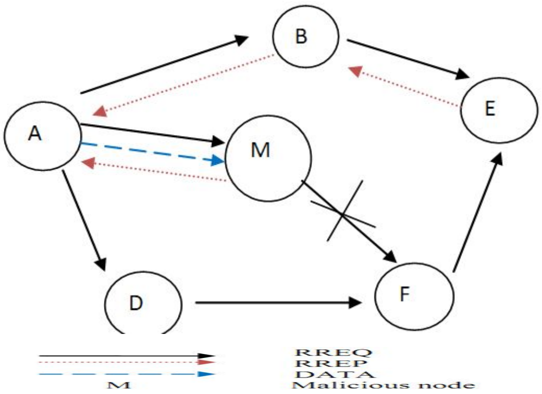


Figure 5. Black Hole Effect

that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, it absorbs all the data and thus behaves like a „Black hole". In AODV there are two type of black hole attack [4], these are following.

**Internal Black hole attack**

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination, when it gets the chance this malicious node makes itself an active data route element. Now this node is capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route.

**External black hole attack**

External attack physically stays outside of the network and denies access to network. External attack can become a kind of internal attack when it take a control of internal malicious node and control it to attack other nodes in MANET.

External black hole attack can be summarized as following points:

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

### *2.2. DoS Attack*

Based on the composition of nodes that form a network, ad hoc networks can be classified into two main categories, cooperative and non-cooperative. In the first category, cooperative, nodes form networks based on common goals to achieve certain objectives. Examples are networks that can be formed in emergency relief operations, collaborative data processing, military applications, entertainment, and conference sessions. In this scenario all members of the group have common objectives, and therefore they cooperate. In the second category, a network is formed to establish communication in civilian environments. There is no reason for mutual cooperation. While the nodes in a network used by the soldiers in a battlefield or disaster recovery area can be assumed to cooperate, there is no good reason to assume that networks formed by civilians with diverging goals and interests will cooperate. Such a network can be formed by a group of people who want to communicate by establishing a temporary networking environment. Each user's objective is usually to maximize his own benefit, and hence the network may suffer from misbehaving nodes that may want to save theirown resources while using other nodes for packet forwarding. It seems appropriate to use a mechanism that encourages cooperation in non-cooperating networks to improve network performance.

Non-cooperation in MANETs occurs due to misbehaving nodes and lack of resources in non-misbehaving nodes. In the non-cooperation due to misbehaving nodes scenario, nodes fail to cooperate due either to malicious behavior or selfishness to maximize their own benefits. In non-cooperating scenarios, a node may promise to forward a packet but fail to do so, or may not be willing to forward packets to save its resources. In both scenarios, network services can be degraded due to lack of cooperation among the nodes. We consider this type of non-cooperation in our study.

In the non-cooperation due to lack of resources scenario, nodes fail to cooperate due to lack of sufficient resources. This resource shortage may occur as a result of wireless network characteristics (limited memory, bandwidth, or energy) or environmental conditions (unreliable connectivity or network load). This category of non-cooperative behaviour is called reasonable non-cooperation. The main issue that requires attention here is load balancing, which is required to distribute the network load equally among the nodes.

### *2.2.1 DoS Attack Scenarios*

The DoS attacks that target resources can be grouped into three broad scenarios. The first attack scenario targets Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider.

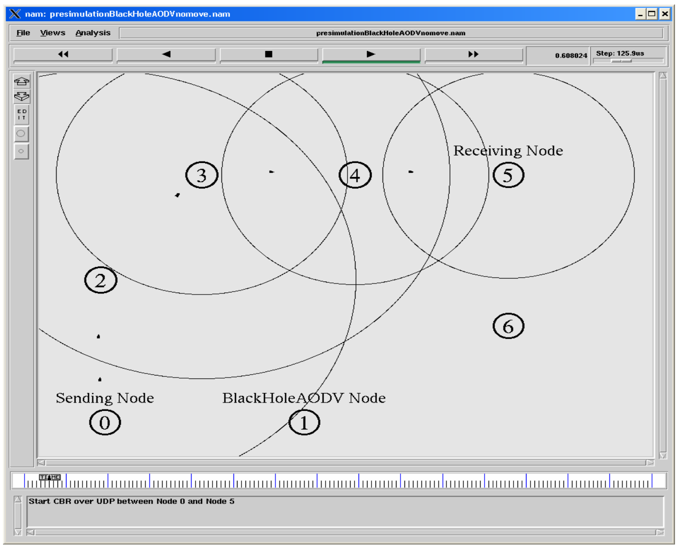
Consider the case where a node continuously sends an executable flooding packet to its neighbourhoods and to overload the storage space and deplete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes. Neighbourhood watch and monitoring can prevent the occurrence of such events by gradually excluding such malicious nodes. The second attack scenario targets energy resources, specifically the battery power of the service provider. Since mobile devices operate by battery power, energy is an important resource in MANETs. A malicious node may continuously send a bogus packet to a node with the intention of consuming the victim’s battery energy and preventing other nodes from communicating with the node. The use of localized monitoring can help in detecting such nodes and preventing their consequences. The third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send packets with bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all neighbours that communicate, overloads the network, and results in performance degradations. Such attacks can be prevented based on the reputation information exchanged among the involved nodes or the cluster head.

We attempt to prevent both selfish and malicious nodes from degrading network performance by providing incentives to encourage cooperation and punishing nodes that do not cooperate.

## III. EXPERIMENT AND RESULT

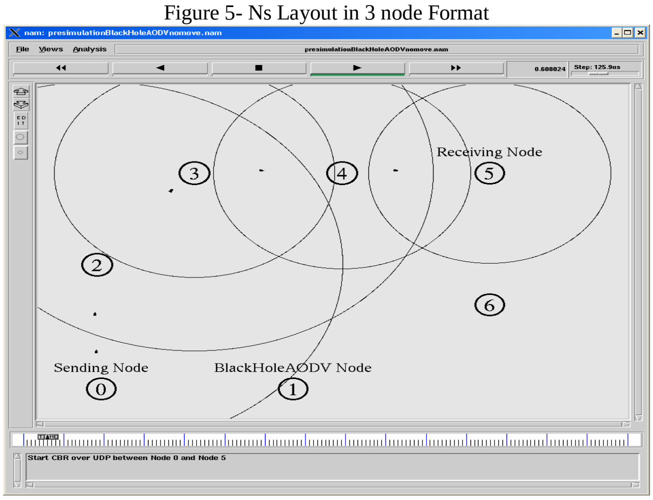
We have employed 5 different scenario to analyses the work, viz. with 3, 5, 8, 10 and 15 node MANET network for AODV, DSR, and Hybrid, and the black hole and DoS attack is employed to the last scenario i.e. of 15 node structure.

These figures are to



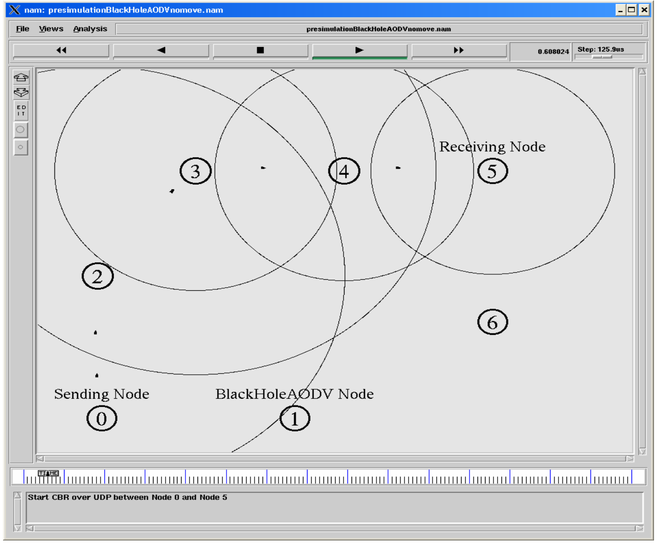
Start CBR over UDP between Node 0 and Node 5

Figure 5- Ns Layout in 3 node Format



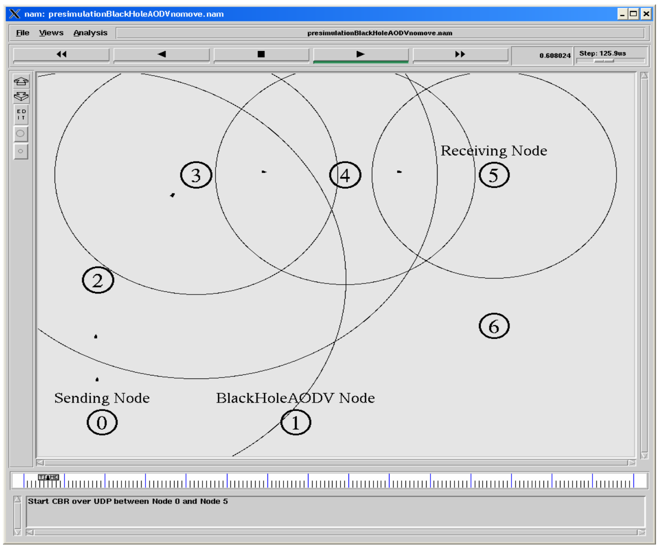
Start CBR over UDP between Node 0 and Node 5

Figure 6-Ns Layout in 5 node Format



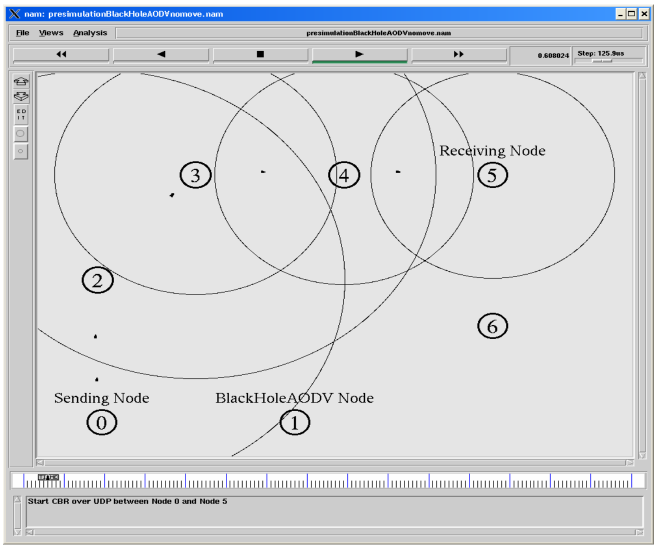
Start CBR over UDP between Node 0 and Node 5

Figure 7- Ns Layout in 8 node Format



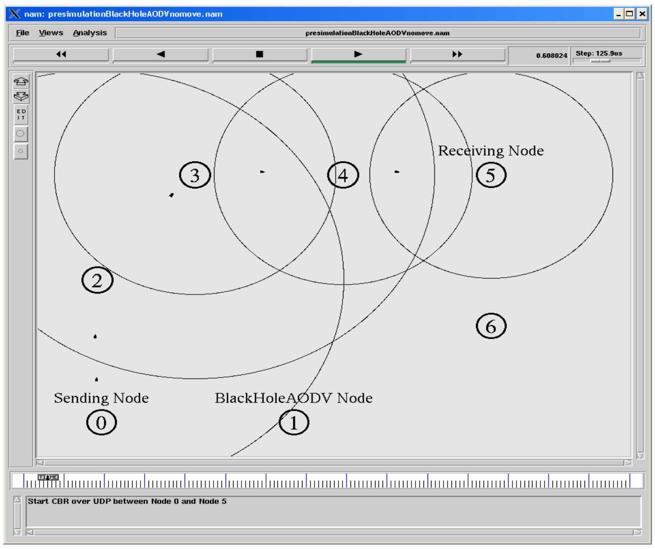
Start CBR over UDP between Node 0 and Node 5

Figure 8- Ns Layout in 10 node Format



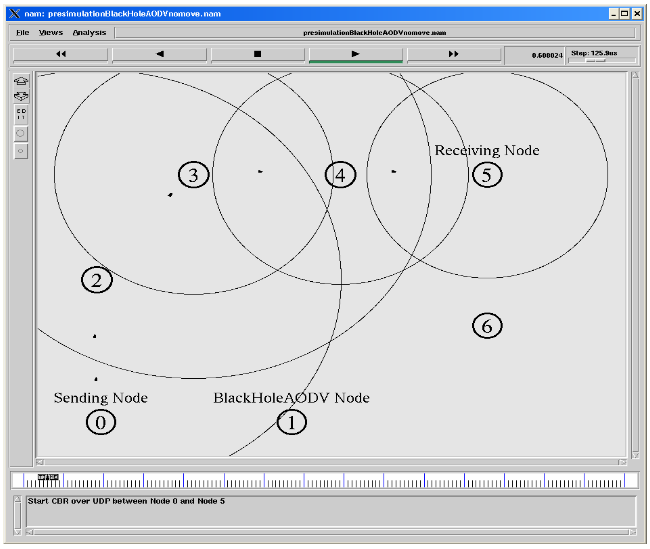
Start CBR over UDP between Node 0 and Node 5

Figure 91- Ns Layout in 15 node Format



Start CBR over UDP between Node 0 and Node 5

Figure 102- Ns Layout in 3 node Format with black hole



Start CBR over UDP between Node 0 and Node 5

Figure 11- Ns Layout in 15 node Format with DoS

## IV .CONCLUSION

In this study, we analyzed effect of the Black Hole and DoS in an AODV, DSR and Hybrid Network. We simulated five normal scenarios where each has 3, 5, 8,10 and 15 node that use AODV, DSR and Hybrid protocol and also simulated the last scenarios after introducing one Black Hole Node and DoS into the network. Our simulation results are analyzed below: Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. In tables of simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase.

We can understand from our research work that AODV network has normally 3.21% data loss and if a Black Hole Node is introducing in this network data loss is increased to 92.59%. As 3.21% data loss already exists in this data traffic, Black Hole Node increases this data loss by 89.38%. When we used IDS AODV protocol in the same network, the data loss decreased to 65%. The results show that our solution reduces the Black Hole effects by 24.38 % as packet loss in a network using IDS AODV and where there is no black holes increases to75.62%.

### *4.1 FUTURE WORK*

We simulated the Black Hole Attack and DoS in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV, DSR and Hybrid routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol may be determined. In our thesis, we try to analyses the Black Hole and DoS effect in the network, and to determine which is best in different cases. But detection of the Black Hole Node is another future work. The reare many Intrusion Detection Systems (IDS) for ad-hoc networks. These IDS scould be tested to determine which one is the best to detect the Black Hole. Our solution tries to eliminate the Black Hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start the packets. Additionally, we used UDP connection to be able to count the packets at sending and receiving nodes. If we had used the TCP connection between nodes, the sending node would be the end of the connection, since ACK packets do not reach the sending node. This would be another solution for finding the Black Hole Node. This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period. Our solution finds the path in the AODV level. Finding the black hole node with connection oriented protocols could be another work as a future study.

## REFERENCES

[1] C.E. Perkins and P. Bhagwat,et. al, "*Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers,*" in Proc. ACM SIGCOMM 94, London, UK, pp.234-244, Oct. 1994.

[2] T. Liu & K. Liu,et. al, *"Improvement on DSDV in Mobile Ad Hoc Networks"*, IEEE, China, pp.1637-1640, 2007.

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y-Ch Hu, and J. Jetcheva,et. al *"A Performance Comparison of Multi-Hop Wireless Ad Hoc Network for mobile ad hoc networks,"* in Proc. 4th annual IEEE/ACM international conference on Mobile Computing and Networking, Dallas, Texas, pp. 85-97, U.S.Oct. 1998.

[4] Ahmed Al-Maashri and Mohamed Ould-Khaoua.et. al *"Performance Analysis of MANET Routing Protocols in the Presence of Self-Similar Traffic"*. IEEE, ISSN- 0742-1303, First published in Proc. of the 31st IEEE Conference on Local Computer Networks, 2006.

[5] Elizabeth M. Royer and C-K Toh.et al *"A Review of current Routing Protocols for Ad-hoc Mobile Wireless Networks"*, IEEE Personal Communications, Vol. 6, No.2, pp. 46-55, April 1999.

[6] N Vetrivelan, Dr. A V Reddy et al,"*Performance Analysis of Three Routing Protocols for Varying MANET Size*" Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol II IMECS 2008, 19-21, Hong Kong, March, 2008.

[7] S.Basagni, I. Chlamtac, V. R. Syrotiuk, and B. A. Woodward, et. al *"A distance routing effect algorithm for mobility (dream),"* in Proceedings of the IEEE/ACM international Conference on Mobile Computing and Networking (MOBICOM'98), pp. 76–84, 1998.

[8] C. E. Perkins, E. M. Royer, and S. R. Das,et. al *"Ad Hoc On- Demand Distance Vector (AODV) Routing"*, Internet Draft, draft-ietf-manet aodv-10.txt, work in progress, 2002.

[9] Azizol Abdullah, Norlida Ramly, Abdullah Muhammed, Mohd Noor Derahman, et. al " *Performance Comparison Study of Routing Protocols for Mobile Grid Environment*", pp 82-88, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008

[10] Altman E, and Jimenez T. Et al " NS Simulator for Beginners". Lecture notes. Univ.de Los Andes, Merida, Venezuela and ESSI.Sophia-Antipolis, France, (2003).

[11] http://en.wikipedia.org/wiki/DestinationSequenced_ Distance_Vector_routing

[12] Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme, Mieso K. Denko, Department of Computing and Information Science, University of Guelph, Guelph, Ontario, Canada, N1G 2W1

[13] T.Franklin,"WirelessLocalAreaNetworks",Technical Report http://www.jisc.ac.uk/uploaded_documents/WirelessLANTechRep.pdf. 25July2005