Analysis of Throughput and Energy Consumption in MANET using IALERT Routing Protocol

Lohit Kumar
School of Electronics and Communication
Lovely Professional University
Phagwara, Punjab, India

Vishali Sharma
Department of Electronics and Communication
Lovely Professional University
Phagwara, Punjab, India

ABSTRACT
Mobile ad hoc Network consist of mobile nodes which do require neither a base station nor any fixed infrastructure. Nodes which are far apart from each other communicate hop by hop. An efficient routing protocol is required between the nodes to communicate. MANETs are not immune to attacks. In this paper we have implemented wormhole attack which is a type of active attack which disturbs the normal functioning of network and IALERT routing protocol. We have compared two parameters that are throughput and energy consumption of both our tcl files named wormhole and isolate. In wormhole file we have applied the attack and in the isolate file we have countered that attack. Results and simulations show that the throughput of isolate file is better than wormhole file and energy consumption of isolate file is less than wormhole file.

1. INTRODUCTION
A Mobile Ad hoc Network (MANET) consists of a collection of mobile nodes forming a dynamic autonomous network. Nodes communicate with each other without the intervention of centralized access points or base stations. In situations like battlefields or major disaster areas, ad hoc networks need to be deployed immediately without base stations or wired infrastructure. In such a network, each node acts as a host, and may act as a router. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed to exchange data between nodes in the network [1].It use radio frequency technology that allows more mobility to the user because of the absence of cable. A MANET is installed easily in such condition where requiring quick set up and modification, such as military battlefields or accident recovery areas. All MANET applications require the dissemination of packets, from node to node, on time-varying channels and time-varying topologies. Communication between non-neighbouring nodes requires a routing protocol, so a stable and efficient routing method is required for longer live transmission. Ad hoc networks consist of mobile nodes which suffer from deployment in an unorganized way. Since all nodes in MANET move randomly so topology of the network is constantly changing which lead to frequent disconnection between source and destination nodes [2]. Compared to the wired networks, mobile ad-hoc networks are much more vulnerable to security attacks. This is mainly due to its features of open medium, dynamic topology, cooperative algorithms, lack of centralized monitoring and management point. Current research work on securing mobile ad-hoc networks mainly focus on confidentiality, integrity, authentication, availability, and fairness [3]. With the ever increasing attractiveness of the Ad-Hoc networks, the issue of the security of the routing protocols of the Ad-Hoc networks has attracted many researchers in last decade [4-8][9]. Security attacks are classified into Active and Passive attacks. Active attacks are further divided into internal attacks and external attacks. External attackers can be prevented by authentication mechanisms or digital certificates in ad hoc networks. But internal attackers are very difficult to find even its presence in the group due to its valid membership in the multicast group. Internal attackers are authenticated nodes do malicious activities in order to disturb the network and routing functionalities easily since they are all authorized members to access the network services. These attacks are more severe than attacks launched by external adversaries because internal adversaries can succeed the cryptosystem of the network. The intentions of internal attack are varies into; handler for an external intruder to launch its attack, selfishness and simply disturb the network without any intention. The node that executes internal attacks called compromised nodes or malicious node. The activities of internal attacks are; packet dropping, selective packet forwarding, forwarding packets to incorrect node, message fabrication, refused to cooperate as defined by routing protocol, sending false reply and Denial of Service [10].
In this paper IALERT routing protocol has been implemented which dynamically partitions the network field horizontally and vertically and chooses a node for communication with all the other nodes. All the remaining nodes form cluster and the chosen node communicates with the clusters of nodes one by one. 49 nodes and wormhole attack has been implemented. Two tcl files name wormhole and isolate are made. In the first tcl file wormhole attack has been implemented on 7^{th} node at 110 seconds. So due to wormhole attack after 110 seconds node 7 will start to drop the packets. In second tcl file wormhole attack has been countered. So after 110 seconds node 7 will still communicate.

2. SYSTEM MODEL
In wormhole attack the malicious node receive packet at one location and tunnels them in the network from another location. This tunnelling is known as wormhole. In this source and sink nodes are placed at a distance from each others. In fig.1 source node will send route request to sink node. So there are two paths through which the packet can be sent to sink node. The first part is source-A-B-C-sink and the second part is source-M1-M2-sink. The destination will find two route request of unequal length one of 4 and other of 3. Now if M2 tunnels the route reply back to M1 source would consider M1-M2 path better for sink then A-B-C path. Thus due to tunnelling the replica of original packet is created and they will collide with the original packets in network.

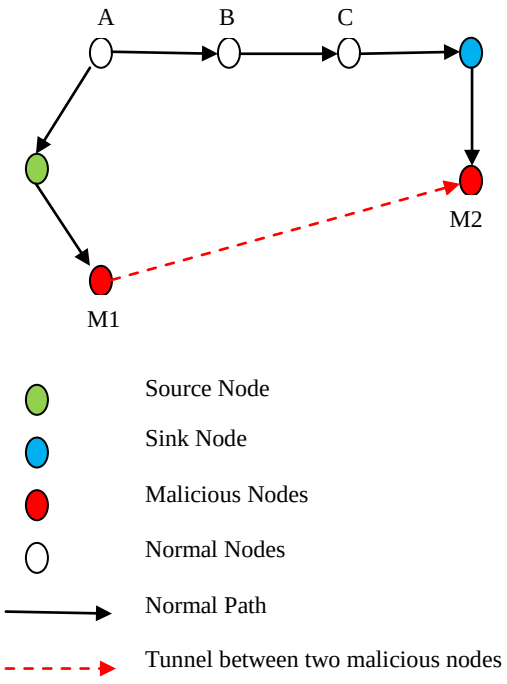

Fig 1: Wormhole Attack

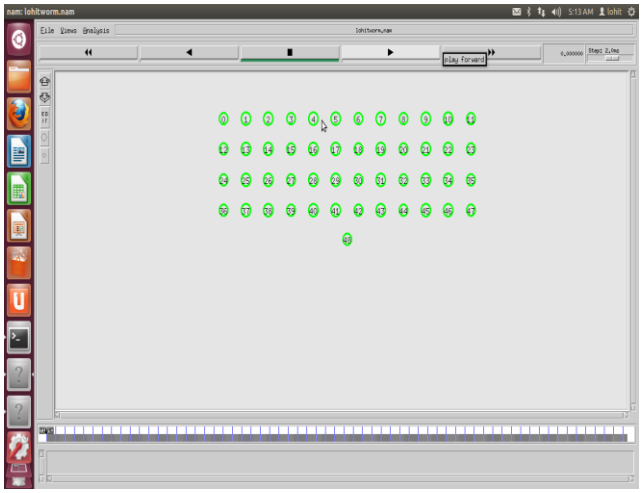

Fig 2: Initial position of nodes.

Figure 2 show the initial positioning of nodes. There are total 49 nodes from 0-48. Figure 3 show the partitioning of nodes horizontally and vertically after applying IALERT. Now node 48 will communicate with all the clusters one by one. Figure 4 show that node 48 is approaching cluster 1 for the communication. The cluster to which node 48 will approach will change its colour from red to yellow. Figure 5 show that node 48 is communicating to cluster 1 and since it is communicating to only cluster 1 the colour of cluster 1 will change from yellow to green.

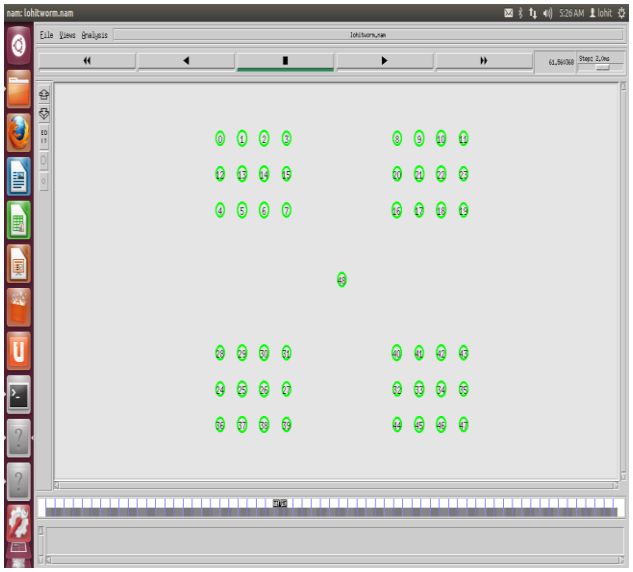

Fig 3: Partition of nodes.

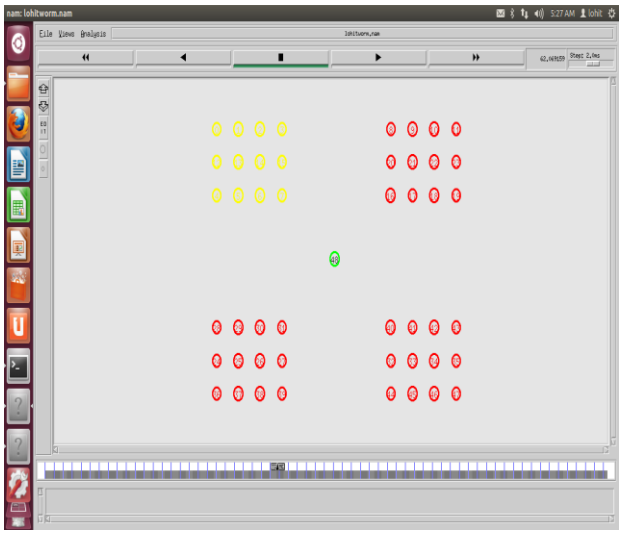

Fig 4: Node 48 approaching cluster 1.

The screenshots of Network Animator which shows how the nodes are partitioned and how they communicate. Proposed routing protocol IALERT partitions the nodes horizontally and vertically as shown in the NAM screen shots. Then it selects node which communicates with the other clusters. Here that communicating node is node 48.

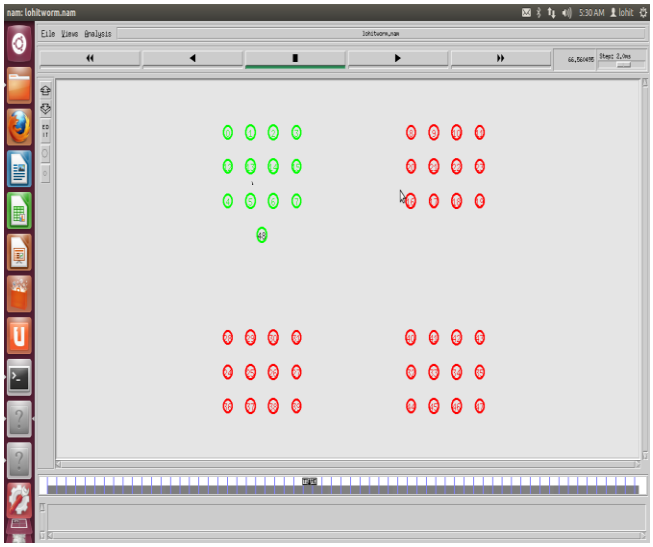

Fig 5: Node 48 communicating to cluster 1.

The same process will be repeated for cluster2, 3 and cluster 4. After communicating from cluster 1 node 48 will approach cluster 2 and will communicate with it. After completing the communication with cluster 2 node 48 will approach cluster 3 and will communicate with it. After completing the communication with cluster 3 node 48 will approach cluster 4 and will communicate with it. After completing the communication with all four clusters node 48 will come back to its initial position.

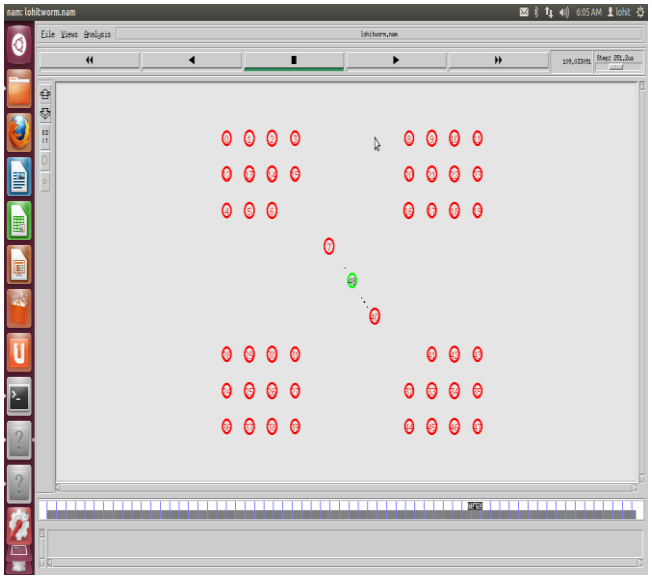

Fig 6: Node 48 communicating to cluster heads of cluster 1 and 3.

In this figure node 7 and node 40 will act as cluster heads of cluster 1 and cluster 3 respectively and will come out from their respective clusters and will communicate with node 48 till 110seconds.

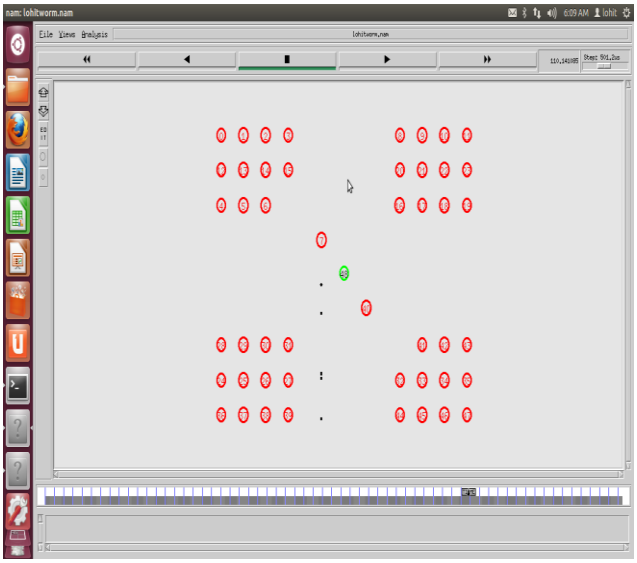

Fig 7: Node 7 dropping packets due to wormhole attack.

After 110 seconds wormhole attack will become active on node 7 and it will start to drop packets because of wormhole attack. After 110 seconds till the end of simulation packets will continue to drop

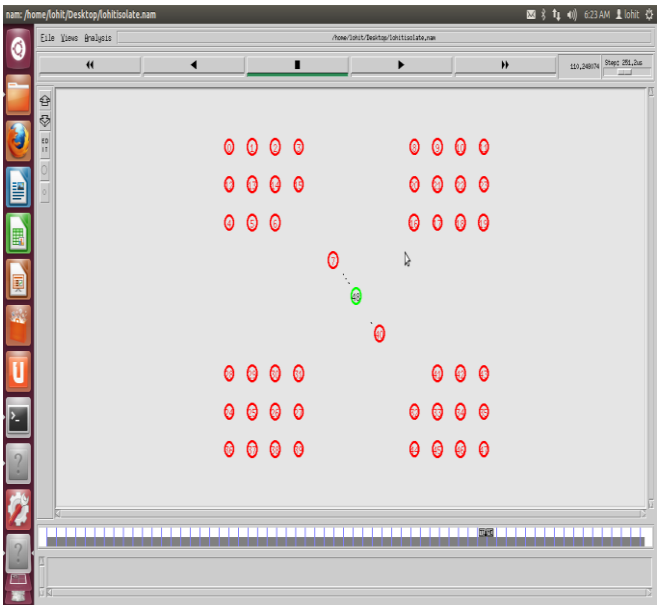

Fig 8: Node 7 communicating despite wormhole attack.

This figure is from 2nd tcl where we have counter the wormhole attack and even after 110 seconds the communication is possible between node 7 and node 48.

3. RESULTS AND SIMULATION

Simulations have been conducted to compare the throughput and energy consumption of two tcl files.

Table I System Parameters

Chanel	Wireless
Propagation	Two ray Ground
MAC	802.11
Antenna	Omni Antenna
No. of Mobile nodes	49
Simulation time	150 seconds

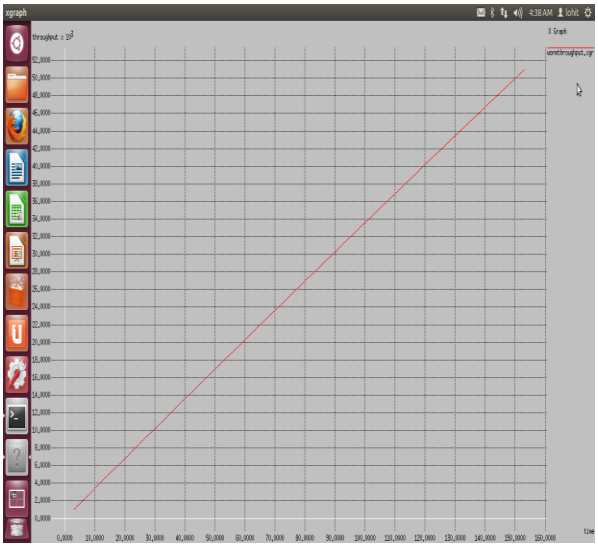

Fig 9: Throughput of Wormhole file.

Figure 9 shows the throughput of wormhole tcl file. In this graph y-axis shows the throughput and x-axis shows the time. The throughput of wormhole tcl file is increasing linearly with time. The maximum value of throughput at 150 sec. is around 49975.

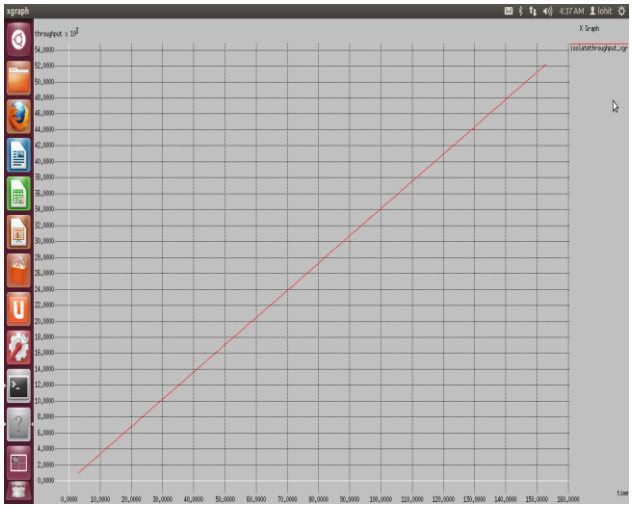

Fig 10: Throughput of Isolate file.

Figure 10 shows the throughput of isolate tcl file. In this graph y-axis shows the throughput and x-axis shows the time. The throughput of isolate file is increasing linearly with time. The maximum value of throughput at 150 sec. is 51200.

Table II Throughput Comparison

Time	Wormhole file throughput	Isolate file throughputs
3	1024	1024
6	2047	2048
9	3069	3072
12	4090	4096
30	10195	10240
60	20290	20480
90	30285	30720
120	40180	40960
150	49975	51200

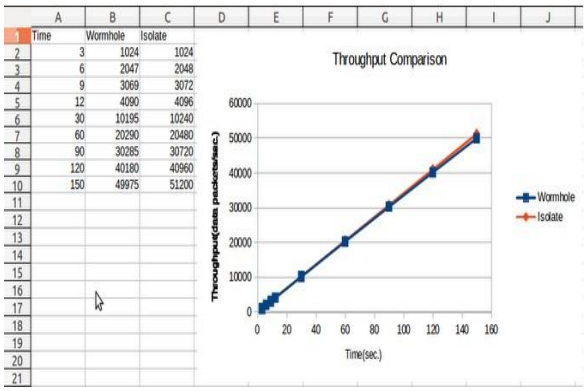

Fig 11: Throughput comparison of both the tcl files.

Figure 11 shows the throughput comparison of both the files at different time intervals. In this graph y-axis shows the throughput and x-axis shows the time. Blue line represents the wormhole file throughput while orange line represents isolate file throughput. It can be clearly seen from the table and graph that the throughput of isolate file is greater than throughput of wormhole file.

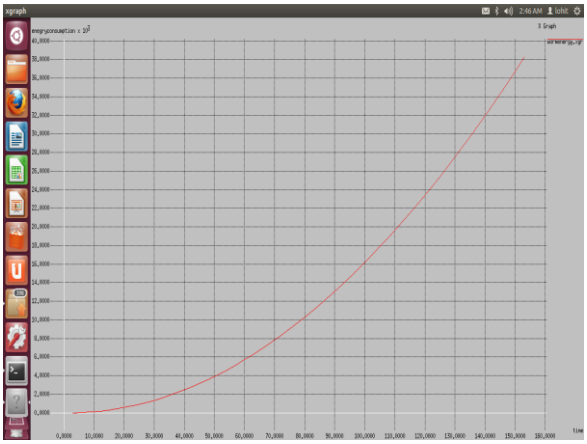

Fig 12: Energy consumption of wormhole file.

Figure 12 shows the energy consumption of wormhole tcl file. In this graph y-axis shows the energy consumed by the nodes and x-axis shows the time. The value of energy consumption at 147 sec. is 35280.

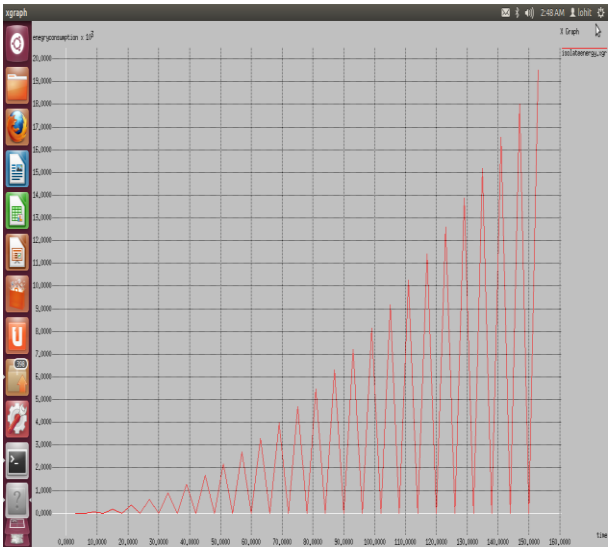

Fig 13: Energy consumption of isolate file.

Figure 13 shows the energy consumption of isolate tcl file. In this graph y-axis shows the energy consumed by the nodes and x-axis shows the time. The value of energy consumption at 147 sec. is 18000.

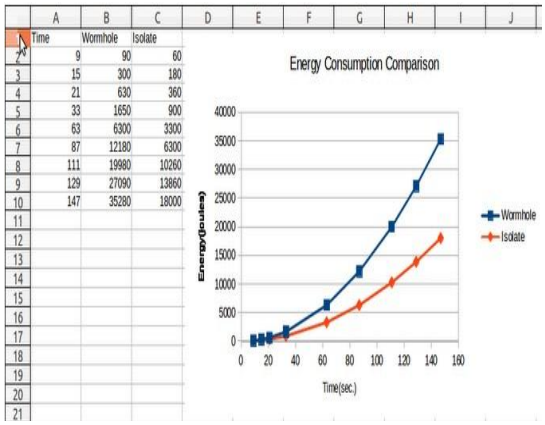

Figure 14 Energy consumption comparison of both tcl files

Figure 14 shows the energy comparison of both the tcl files. In this graph y-axis shows the energy consumed by the nodes and x-axis shows the time. Blue curve represents wormhole file energy consumption while orange line represents isolate file energy consumption. It can be clearly seen from the table and graph that the energy consumption of isolate file is less than that of wormhole file.

Table III Energy Consumption Comparison

Time	Wormhole file	Isolate file
9	90	60
15	300	180
21	630	360
33	1650	900
63	6300	3300
87	12180	6300
111	19980	10260
129	27090	13860
147	35280	18000

4. CONCLUSION

In this paper wormhole attack and routing protocol IALERT has been implemented on two tcl files name wormhole and isolate. In wormhole tcl file wormhole attack is implemented due to which the packets starts to drop while in isolate file wormhole attack has been countered and packet drop has been prevented. Results and simulations show that throughput of isolate file is greater than that of wormhole file. Energy consumption of isolate file is less than wormhole file.

5. FUTURE WORK

In the future work new routing protocol can be implemented on the nodes and after that parameters can be compared. New attack can be implemented or no. of nodes can be increased.

6. REFRENCES

[1] P. I. Basarkod, S. S. Manvi, D.S.Albur "Mobility Based Estimation of Node Stability in MANETs" 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013) pp no.126-130.

[2] Hemant Dandotiya, Rachit Jain,Rinkoo Bhatia "Route Selection in MANETs by Intelligent AODV" 2013 International Conference on Communication Systems and Network Technologies pp no.332.

[3] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng "Anonymous Secure Routing in Mobile Ad-Hoc Networks" Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04)

[4] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE proceedings on wireless Communications, vol.11, no.1, pp: 38-47, Feb. 2004.

[5] M.K. Kumar and R. S. Rajesh, "A Survey of MANET Routing Protocols in Mobility Models," International Journal of Soft Computing Vol. 4, I. 3, pp. 136-141, 2009.

[6] T. Fahad & R. Askwith, "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks.

[7] Y. Zhang, W. Louy, W. Liu and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks," proc. of Journal on Wireless Networks, vol. 13, no. 5, pp. 569-582, October 2007

[8] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. On Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[9] I. Khalil and S. Bagchi, "MISPAR: Mitigating stealthy packet dropping in locally-monitored multi-hop wireless ad hoc networks," Proceedings of the 4th International conference on Security and Privacy in Communication networks (SecureComm'08), Turkey, Sep 2008, pp. 1–10.