International Journal of Wireless Networks and Communications.
ISSN 0975-6507 Volume 4, Number 1 (2012), pp. 19-29

http://www.irphouse.com

Performance Analysis of DSR, AODV Routing Protocols based on Wormhole Attack in Mobile Ad-hoc Network

[1]Lokesh N.S., [2]Vanajakshi P. and [3]Shivaraj V.B.

[1]Assistant Professor & Research Scholar
, [2]Assistant Professor & HOD, [3]Lecturer,
Dept of CSE, Vivekananda Institute of Technology, Bangalore, India
E-mail:lokgwd20@gmail.com, hodcsevkit@gmail.com
shivu076@gmail.com

Abstract

Mobile ad-hoc network are able work without any existing infrastructure. MANET is a self configure network connected by wireless links. Mobile ad-hoc network uses temporary network which is able to work without any centralize administration or stand alone infrastructure. In mobile ad-hoc network each device move in any direction without any restriction so it changes it links to often with other devices present in same network. Mobility of mobile device anywhere in the network without any centralize administration makes it difficult to manage routing. In mobile ad-hoc network each device need to forward traffic that is not related to its own use and therefore each device work as a router. MANET's protocol has different security flaws and using these flaws many kind of attack possible on mobile ad-hoc-network. Wormhole is one of these attacks. Wormhole attack causes serious affect on performance of the MANET protocol and preventing the attack has proven to be very difficult. In wormhole attack attacker place some malicious node in the network. A malicious node captures data packets from one location in the network and tunnels them to another malicious node at distinct location, which replays them locally. These tunnels works like shorter link in the network and so act as benefit to unsuspecting network nodes which by default seek shorter routes. This paper illustrates how wormhole attack affects performance of routing protocol in mobile ad-hoc network using random waypoint mobility model with varying node mobility.

Index Terms: AODV, CBR, DSR, MANET

Introduction

Mobile networks can be classified into infrastructure networks and mobile ad hoc networks (MANET) according to their dependence on fixed infrastructures [2]. In infrastructure based mobile network wired access point is used and within the transmission range of access point all mobile device are free to move in any direction. In mobile ad-doc network each device is free to move any direction so the routes use to reach from one device to another change frequently. In mobile ad- hoc networks each device need to forward traffic that is not related to its own. Routing paths in MANETs potentially contain multiple hops, and every node in MANET has the responsibility to act as a router [4]. There are various mobility models such as random way point, reference point group

Mobility model (RPGM), Manhattan mobility model, freeway mobility model, Gauss Markov mobility model etc. that have been proposed for evaluation [6, 13]. Several parameters such as mode mobility, traffic load and node density and pause time has been used to evaluate performance of MANET routing protocols.. Biradar, S. R. et al.[11] have analyzed the AODV and DSR protocol using Group Mobility Model and CBR traffic sources. Biradar, S. R. et. al.[11] investigated that DSR performs better in high mobility and average delay is better in case of AODV for increased number of groups. Also Rathy, R.K. et. al [8] investigated AODV and DSR routing protocols under Random Way Point Mobility Model with TCP and CBR traffic sources. They concluded that AODV outperforms DSR in high load and/or high mobility situations.

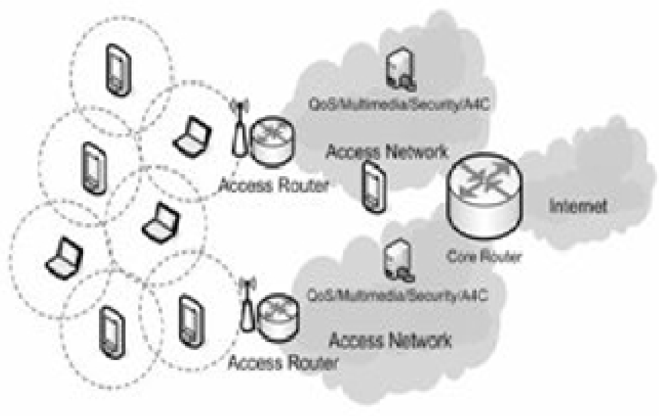

Figure 1: Mobile Ad-hoc Network.

Random Waypoint Mobility Model

MANET's protocol performance frequently observes and studied by simulation and their performance depends heavily on the mobility model that governs the movement of the nodes [5]. Random way point is a mobility model that use random based mobility to manage mobility of mobile devices in a wireless communication system. This mobile model describes various property of mobility like movement patter of the mobile users and their location velocity and acceleration change over time. Mainly this type of mobility model is use for simulation when network protocol performance is evaluated. The Random waypoint model, first proposed by Johnson and Maltz[17], soon became a "benchmark" mobility model[20] to evaluate the Mobile ad hoc network (MANET) routing protocols, because of its simplicity and wide availability.

Description of Routing Protocol

In this section we will provide review on couple of typical ad-hoc network protocol namely DSR and AODV.

Ad-Hoc on Demand Distance Vector (AODV)

The Ad-hoc On-demand Distance Vector routing protocol [1, 3, 12] enables multi hop routing between the participating mobile nodes wishing to establish and maintain an ad-hoc network. AODV is a reactive protocol based upon the distance vector algorithm. ADOV uses many type of message in order to find route from one mobile device to another mobile device. Route discovery process starts when a source node needs to send a packet to destination node but it does not have a valid route to destination node. AODV initiate a path discovery process to locate the other node. Source node broadcast route request (RREQ) packet to all it neighbors. Then their entire neighbors forward this request to their neighbors and so on. This process is continuing until either the destination node is found or an intermediate node with "fresh enough" route to destination is located. Sequence number is use by AODV to ensure all route are loop-free and contain most recent route information. In AODV to avoid looping each node maintains it own sequence number as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies an RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ. AODV uses periodic local broadcast hello message. Hello message help a node to inform its neighbor that it active and working. However, the use of hello messages is not required for Nodes listen for retransmissions of data packets to ensure that the next hop is still within reach. If such a retransmission is not heard, the node may use any one of a number of techniques, including the reception of hello messages. Hello messages may list the other nodes from which a mobile has heard, thereby yielding a greater knowledge of network connectivity.

Dynamic Source Routing (DSR)

This is an on-demand routing protocol based on source routing concept. In DSR mobile nodes stores source routes in it caches for which mobile device are aware. When new routes are learned by nodes entries of cache is updated for these new routes. Working of this protocol can be divided in two parts. (a) Route discovery (b) Route maintenance. When a mobile node need to send any packet it first consults with its route cache that whether it already have a route for destination. It an unexpired route is present it send the packet using this route. But if node does not have such route it initiates broadcasting of route request packet. This route request message contains the address of the destination, along with the source node's address and a unique identification number. Each node that receive that packet check it cache to know whether a route for this destination exists or not. If route does not exists it adds it own information to the packet and send it to outgoing link. To limit the number of route requests propagated on the outgoing links of a node, a mobile only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address has not already appeared in the route record. A reply packet is generated when request packet either reach to destination node or it reach to a intermediate node who have unexpired route for destination in its cache. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken.

The paper is organized as follows. In the section II, we give brief description of Random waypoint Mobility Model. In section III, we give brief introduction of AODV and DSR routing protocol. Section IV, describes the wormhole attack. In section V, cover the simulation setup and result of simulation and at the end in section VI, we draw the conclusion of simulation scenarios.

Wormhole attack

In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point [20]. Malicious nodes are connected via a link called "wormhole link" using private high speed network. Wormhole attack is simple to deploy but it may cause significant damage to network. Wormhole attack can be carry out by using different techniques. Here we discuss two methods to generate wormhole attacks in mobile ad-hoc network. In the first type of wormhole, all packets which are received by a malicious node are duly modified, encapsulated in a higher layer protocol and dispatched to the colluding node using the services of the network nodes. These modified packets reach to colluding node just like normal node traverse form one node to another node. Once packets reach to intended malicious node, its extract the packet make the requisite modifications and send them to intended destination. In second type of attack after packets are modified and encapsulated they are sending using a point to point specialized link between the malicious nodes.

Simulation Setup and Result

We have used Network Simulator Qualnet 5.0.2 in our evaluation. In Scenario we have place 50 nodes uniformly distributed in area of 500m x 500m. For this study, we have used random waypoint mobility model for the node movement with 0 sec pause time and 5, 10, 15, 20, 25, 30, 35, 40 meter/sec node mobility speed. The parameters used for carrying out simulation are summarized in the table 1.

Performance Metrics

We have used the following metrics for evaluating the Performance of two on-demand Reactive routing protocols (AODV & DSR):

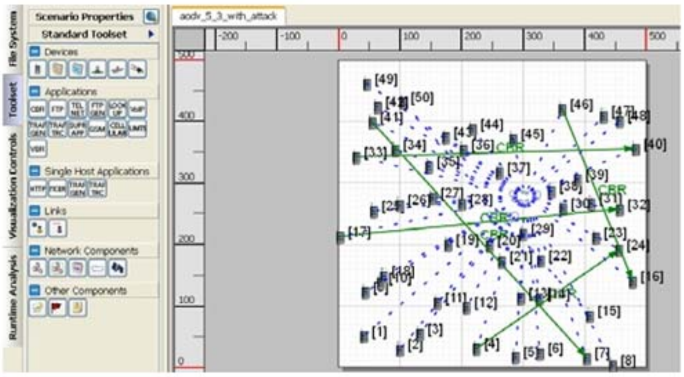

Figure 2: Simulation scenario in qualnet simulator.

Packet delivery ratio

It is the ratio of data packets delivered to the destination to those generated by the sources. It is calculated by dividing the number of packet received by destination through the number packet originated from source.

PDF = (Pr/Ps)*100

Where Pr is total Packet received & Ps is the total Packet sent.

Table I: Simulation Parameters.

Parameters	Value
Routing Protocols	AODV, DSR
MAC Layer	802.11
Packet Size	512 bytes
Terrain Size	500m * 500m
Nodes	50
Mobility Model	Random waypoint
Data Traffic Type	CBR
No. of Source	5
Simulation Time	200 sec.
Node Mobility Speed	5, 10, 15, 20, 25, 30, 35, 40
CBR Traffic Rate	8 packet/sec
Maximum buffer size for packets	50 packets
No of Malicious Node	2, 3, 4

Average End-to-End Delay (second)

This includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, retransmission delay at the MAC, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination. D = (Tr - Ts) Where Tr is receive Time and Ts is sent Time

Average jitter

Jitter is used as a measure of the variability over time of the packet latency across a network. A network with constant latency has no variation (or jitter). Packet jitter is expressed as an average of the deviation from the network mean latency. Jitter is cause by network congestion, timing drift, or route changes. At the sending side, packets are sent in a continuous stream with the packets spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, this steady stream can become lumpy, or the delay between each packet can vary instead of remaining constant.

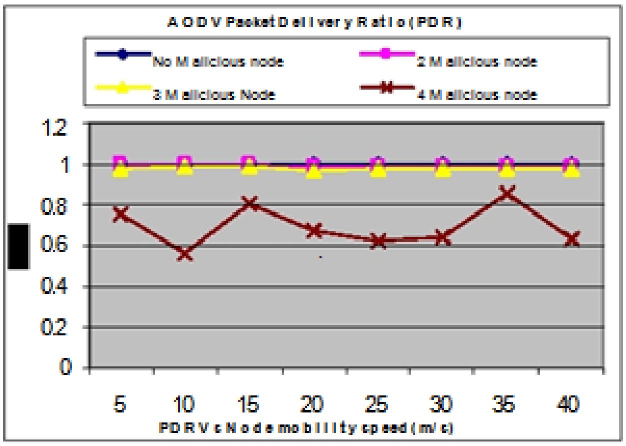

Figure 3: Packet Delivery Ratio vs. nodes mobility speed.

AODV Packet delivery ratio under wormhole attack

In AODV protocol if many nodes are sending and receiving data traffic simultaneously placing more malicious node uniformly in MANET network causes severe damage because it increases the probability of route affected malicious node. As show in figure 3 when no of malicious node are less (2 or 3) there is very less probability that any route involve malicious node and packet delivery ratio decreases only one percent as compare to the network that has no malicious node. But once the number of malicious node increases a particular level and it placed uniformly all over network effect of attack become severe as we can see in figure 3 when number of malicious node become 4, packet delivery ratio decreases significantly (Between 60% to 80%). One more important behavior is observed that packet delivery ratio under wormhole attack does not affected by node mobility speed.

AODV Average Jitter under wormhole attack

Jitter is another significant application layer parameter in mobile ad-hoc network especially in case where quality of Service is required. Study of wormhole attack effect on jitter in AODV protocol show that when the number of malicious node in mobile ad-hoc network are low (2 or 3) Jitter increase almost two times as compare to network without any malicious node. this is because when number of malicious nodes are less then number of route affected by these malicious node are also low which cause less delay. Another important characteristic can be seen from this figure 4 that in case of less malicious nodes in network (2 or 3) jitter increases as node mobility speed increases. When we increase number of malicious node from 3 to 4 there is a significant increase is jitter but at this case jitter decreases at very high node mobility speed (35 and 40 m/s).

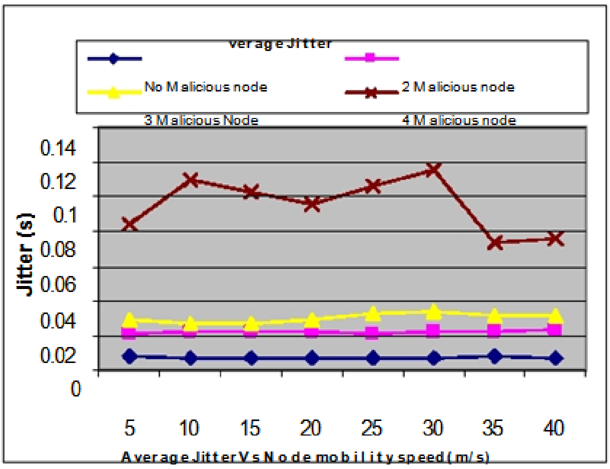

Figure 4: Average jitter vs. Nodes mobility speed.

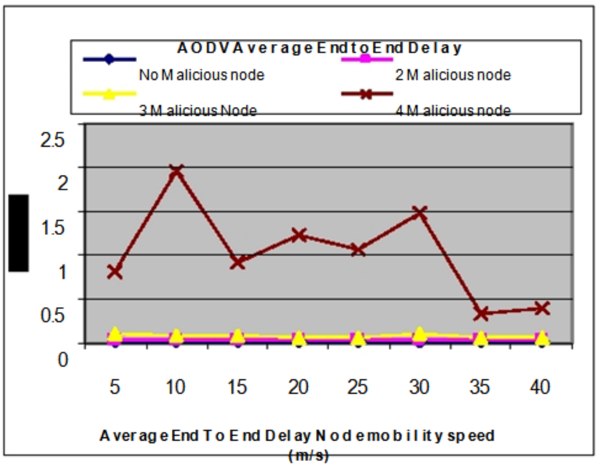

Figure 5: Average End to End-Delay vs Nodes mobolity speed.

AODV Average End to End delay under wormhole attack

Average End to End delay does not affected by the attack much when number of malicious nodes or less (2 or 3 nodes) also these is no change in End to End delay with respect to node mobility speed. However there is a significant increase in average end to end delay when number malicious node are high (4 nodes) and there is a negative relationship between End to End delay and node mobility speed. As we can see from figure 5 that in case when number of malicious node are high(4 nodes) with high node mobility (35 and 40 m/s) Average end to end delay become almost 3 time less as compare to other (5 to 30 m/s) node mobility speed.

DSR Packet delivery ratio under wormhole attack

In mobile ad-hoc network DSR protocol uses a complete list of node that contain by each packet that it has to traverse in order to reach destination node. This feature, although excludes intermediate nodes form making any routing decisions. Still From figure 3 and 6 we can see that DSR is more badly affected by wormhole attack as compare to AODV. And it shows that wormhole attack does not depend on working of intermediate nodes. When number of malicious nodes are less (2 or 3 nodes) packet Delivery ratio decreases as nodes mobility speed increase.

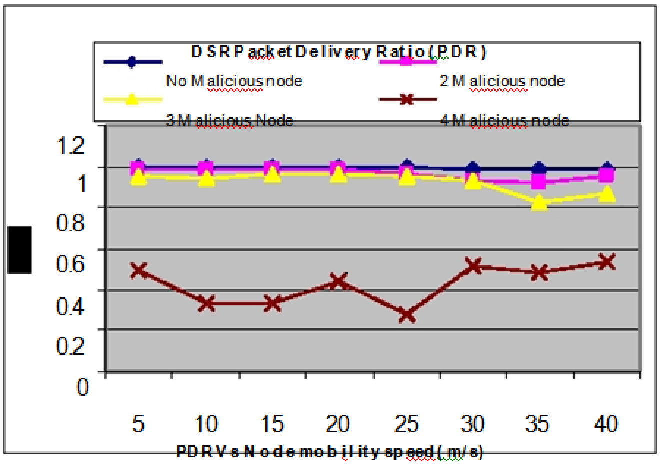

Figure 6: Packet Delivery Ratio vs. Nodes mobility speed

However result of packet delivery ratio with high malicious (4 nodes) node show that packet delivery ration increases as node mobility speed increases. As in case of DSR nodes maintain exiting or secondary route to it cache memory it increase the probability that a attack route is use by more than one source node to send traffic to destination node over a period of time which further magnify the impact of wormhole attack in DSR protocol.

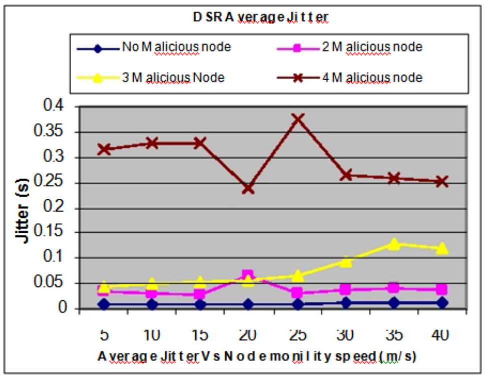

Figure 7: Average jitter vs. Nodes mobility speed.

DSR Average Jitter

AODV perform better then DSR under wormhole attack for jitter parameter. As DSR maintain existing route and secondary route so route discovery process is faster but this property DSR help wormhole attack to become more danger for DSR protocol. Once a root is attack by wormhole it used again and again by DSR since it maintain existing root from figure 5 we can see that average jitter become low when node mobility is high (35 to 40 m/s). In the case of AODV Average jitter is almost three times less than the DSR. When number of malicious node is less (2 or 3) and node mobility speed is also low average jitter is very low (Between.05 to.10 sec.). However average Jitter increases as node mobility speed increases. Performance of jitter with high number of malicious node (4 nodes) shows that average jitter is very high in this case (.30 to.35 sec) and as Jitter decreases as node mobility increases.

DSR Average End to End delay under wormhole attack

AODV outperform DSR when we compare Average End to End delay under wormhole attack. In the case of DSR there is no significant difference in average End to End delay when no malicious node present and less malicious nodes (2 or 3nodes) are place in network. But with high number of malicious nodes are high (4 nodes) average End to End delay increases significantly (between.25 to 43 sec.) as show in figure 8.

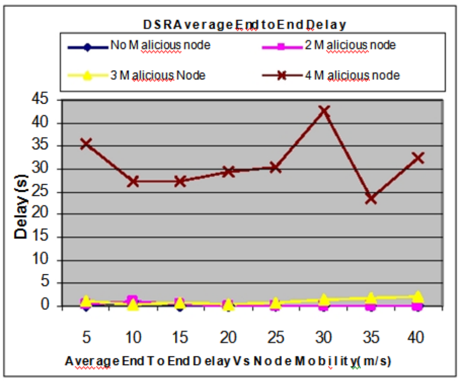

Figure 8: Average jitter vs. Nodes mobility speed.

Conclusion

From the figure 3 to 8, we obtain some conclusion that under wormhole attack with CBR traffic sources, AODV perform better than DSR for packet delivery ratio, average jitter and End to End delay parameter on both low (2 or 3) and high (4 nodes) number of malicious nodes scenarios. In this paper, only two routing protocol are used and their performance have been analyzed under wormhole attack. This paper can be enhanced by analyzing the other MANET routing protocols under different mobility model and different type of attack.

References

[1] S. Das, C. E. Perkins, E. Royer, "Ad Hoc On Demand Distance Vector (AODV) Routing", IETF Draft, June 2002

[2] C-K Toh "Ad Hoc Mobile Wireless Networks Protocols and Systems", First Edition, Prentice Hall Inc, USA, 2002

[3] C.E. Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, pages 90-100, February 1999.

[4] Elizabeth M. Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, pages 46-55, April 1999.

[5] Fan Bai, Ahmed Helmy "A Framework to systematically analyze the Impact of Mobility on Performance of Routing Protocols for Adhoc Networks", IEEE INFOCOM 2003

[6] Tracy Camp, Jeff Boleng, Vanessa Davies "A Survey of Mobility Models for Ad Hoc Network Research", Wireless Communication & Mobile Computing (WCMC): vol. 2, no. 5, pp. 483-502, 2002

[7] D. Johnson, Dave Maltz, Y Hu, Jorjeta Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", Internet Draft, February 2002

[8] Suresh Kumar, R.K. Rathy and Diwakar Pandey, "Traffic Pattern Based Performance Comparison of Two Reactive Routing Protocols for Ad-hoc Networks using NS2", 2nd IEEE International Conference on Computer Science and Information Technology, 2009.

[9] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile", RFC 4728, Feb 2007

[10] S.Corson and J.Macker, "Routing Protocol Performance Issues and Evaluation considerations", RFC2501, IETF Network Working Group, January 1999.

[11] S. R. Biradar, Hiren H D Sharma, Kalpana Shrama and Subir Kumar Sarkar, "Performance Comparison of Reactive Routing Protocols of MANETs using Group Mobility Model", IEEE International Conference on Signal Processing Systems, pages 192-195 2009.

[12] C. Perkins, E. Belding-Royer, S. Das, quet, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003

[13] N.Aschenbruck, E.Gerhands-Padilla, P.Martini, "A Survey on mobility models for Performance analysis in Tactical Mobile networks, " Journal of Telecommunication and Information Technology, Vol.2 pp.54-61, 2008

[14] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang, "A group mobility model for ad hoc wireless networks, " in ACM/IEEE MSWiM, August 1999.

[15] http://www-scf.usc.edu/~fbai/important/, referred on February 2010.

[16] http://nile.usc.edu/important/, referred on February 2010.

[17] Bai, Fan; Helmy, Ahmed (2006). A Survey of Mobility Models in Wireless Adhoc Networks. (Chapter 1 in Wireless Ad-Hoc Networks. Kluwer Academic. 2006.

[18] Broch, J; Maltz DA, Johnson DB, Hu Y-C, and Jetcheva J (1998). "A performance comparison of multi-hop wireless ad hoc network routing protocols". roceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking(Mobicom98), ACM, October 1998.

[19] Broch, J; Maltz DA, Johnson DB, Hu Y-C, and Jetcheva J (1998). "A performance comparison of multi-hop wireless ad hoc network routing protocols". roceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking(Mobicom98), ACM, October 1998.

[20] A. Perrig, Y. C. Hu, and D. B. Johnson, Wormhole Protection in Wireless Ad Hoc Networks, Technical Report TR01-384, Department of Computer Science, Rice University, 2001.

[21] Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3