Performance Analysis of AODV for Wormhole Attack Using Different Mobility Models

Gurmeet Kaur[1] and Amanpreet Kaur[2]
[1,2]Centre for Computer Science and Technology, Central University of Punjab, Bathinda, India
E-mail: [1]gurmeetpatil@gmail.com, [2]pandheraman@gmail.com

***Abstract*— Mobile Ad-Hoc Network (MANET) is a type of temporary wireless network, in which the nodes are mobile and have dynamic network topology. Communication among nodes in these networks is accomplished via different routing protocols. But these protocols have different security flaws and using these flaws, an attacker can launch many attacks. Wormhole attack is one of the serious attacks in the context of mobile ad-hoc networks that can disrupt any routing channel completely. In this work, an attempt has been made to analyze and compare the performance of on-demand reactive routing protocol: Ad hoc On Demand Distance Vector (AODV) with two approaches: AODV without attack and AODV under wormhole attack using two mobility models viz. Random Way Point Model and Reference Point Group Mobility Model. The performance metrics evaluated for the two examined approaches are Average Throughput, Packet Delivery Ratio, Average End to End Delay and Jitter. Along with this, an approach has also been used to analyze participated malicious nodes.**

Keywords: AODV, Mobility, RPGM, RWP, Tunnel

I. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is emblematic and ubiquitous in nature, which is the extension of wireless networks. According to structural arrangement, wireless networks are classified into two main categories: fixed infrastructure wireless networks and infrastructure less wireless networks. Mobile Ad-Hoc Networks (MANETs) fall under the category of infrastructure less wireless networks [13] [3].

The original idea of MANET started out in the early 1970s and during this period of time, MANET was called "packet radio" network sponsored by DARPA. The whole life cycle of ad hoc networks could be categorized into three generations and present ad hoc networking systems are considered the third generation, which was started out in 1990s [23].

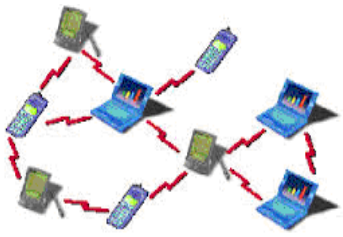

Fig. 1 Infrastructure Less Wireless Network (Mobile Ad-hoc Network) [1]

There are various MANET routing protocols as no single routing protocol works well in all environments [15]. The reason is that the traditional routing protocols (which have already written for the wired network) do not perform well in MANETs. Hence there was a need to design new protocols for mobile ad hoc networks [24].

Depending upon the many ways by which computers can communicate, the routing protocols in mobile ad-hoc network can be divided into three categories [18]: Demand Oriented, Table Oriented and Hybrid Routing Protocols. But in this work, a demand oriented or reactive routing protocol is used for analysis: AODV (Ad Hoc On-Demand Distance Vector).

The first version of AODV was published in November 2001 by Working Group for routing of the IETF community. It uses sequence numbers to solve the count-to-infinity and loop creation problem [16]. It includes two main steps for the proper working namely Route Discovery and Route Maintenance with the help of four types of control messages: RREQ, RREP, RERR and HELLO [12].

The remaining paper is organized into various sections as follows: section II gives the brief introduction to mobility models, which are used in simulation process. Section III illustrates the scenario of wormhole attack in AODV protocol and its types. In section IV, the simulation environment and methodology is explained. Section V lists the various results. Section VI provides the conclusion followed by references.

II. MOBILITY MODELS

Nowadays, for the simulation of realistic movements that are produced by users of a mobile or wireless network, different mobility models are used [20]. There are two main categories of mobility models namely purely synthetic models and trace-based mobility models [22]. But amongst them, purely synthetic models are commonly used in research. In this research work random waypoint and reference point group mobility models are used.

A. Random Way Point Model (RWP)

It was first proposed by Johnson and Maltz. It is elementary synthetic model, which is used to evaluate the MANET routing protocols [6] [7]. In this model, at every instant, a node randomly chooses a destination anywhere in the specified network field and moves towards it with a velocity chosen randomly from a uniform distribution between {0, V_max}, where V_max is the maximum allowable velocity for every

mobile node. To overcome sudden stop and start, 'pause time' parameter is used by nodes. For this duration, the node stops after reaching the destination. Fig. 2 illustrates an example of a topography showing the movement of nodes for RWP [8] [17].

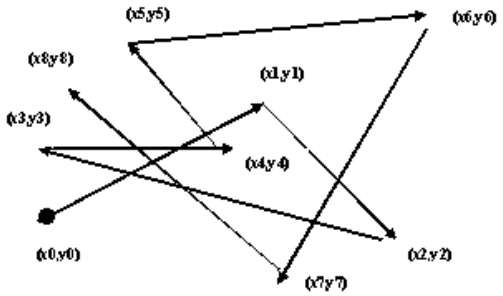

Fig. 2 Node Movement in Random Way Point Model [7]

B. *Reference Point Group Mobility Model (RPGM)*

In contrast to RWP, there are some spatial dependencies in RPGM. To simulate the group movement behavior in the real world such as communication in military battlefield and disaster areas, reference point group mobility model was proposed [5].

In RPGM, nodes are divided into groups or clusters. Each group has a logical center called group leader that defines the whole group's motion behavior and leader's mobility follows random waypoint. Initially each member of the group is uniformly distributed in the neighborhood of the group leader. Then, at each instant, every node has speed and direction that is derived by randomly deviating from that of the group leader [21].

Figure 3 shows an example topography illustrating the movement of nodes for Reference Point Group Mobility Model.

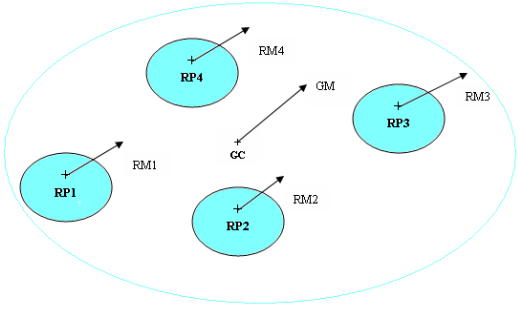

Fig. 3 Reference Point Group Mobility Model [21]

where, RP: Random Point
RM: Random Motion
GC: Group Center
GM: Group Movement

III. WORMHOLE ATTACK & ITS TYPES

Security in MANET plays a vital role for basic network functions. Availability, Authorization, Confidentiality, Integrity and Non-repudiation are some basic requirements that effective security architecture must ensure in order to combat passive and active attacks [15] [2] [14].

A. *Wormhole Attack in AODV Protocol*

According to [9] [19] wormhole attack is an active attack. Wormhole attacker affects the original functionality of MANET routing protocols such as AODV, DSR and OLSR etc, but this research work emphasizes on wormhole attack in AODV routing protocol. A simplified view of wormhole attack is shown in Fig. 4.

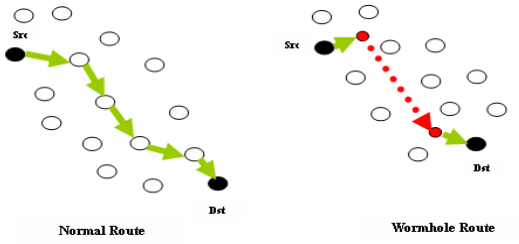

Fig. 4 Scenario of Wormhole Attack [4]

Suppose a source wants to talk with destination. And this communication is possible through shortest path provided by AODV protocol (called normal route). But if two malicious nodes are kept at two different locations in the network and a malicious node accepts the traffic at one location, tunnels them through wormhole link to another malicious node, then replays packets into the network at that location, then this is called wormhole route [10].

Hence, the functioning of AODV protocol is completely disrupted by this attack. It affects various QoS parameters such as delay, jitter, throughput, packet delivery ratio and energy consumption etc [9] [4]. The various metrics such as strength, packet delivery ratio, path length, attraction and robustness etc can also be used to detect wormhole attack in the network [25].

B. *Types of Wormhole Attack*

According to [6], there are various types of wormhole attack as follows:

1. *All Pass:* Here malicious nodes can pass all the packets regardless of their size.
2. All Drop: Here malicious nodes can drop all the received packets in the network.
3. *Threshold:* Sometimes, there is a constraint as a threshold value in network and malicious node can drop all the packets having size greater than or equal to the threshold value.

4. *Replay:* Here, one malicious node can replay the packets after tunnelling in the network.
5. *Tunnelling:* Wormhole attack is also called tunnelling attack. So here, a malicious node tunnels the packets from one location to another location in the network via wormhole link.
6. *Propagation Delay:* The propagation delay in the network is increased as more time is taken by malicious nodes to send packets from source to destination.

IV. Simulation Setup & Methodology

To construct a real distributed testing environment, the cost and complexity is very high. So simulation is widely used in network research. Simulation is the manipulation of the model of a system that is used to observe the behavior of a particular system in a setup similar to real-life [11]. NS2 simulator is used in this research work and it is the most widely used simulator in academia. This study was performed on Intel Core i7 computer system using Ubuntu Linux 12.04 Operating System.

A. Simulation Methodology

This work has been divided into following steps:

Step 1: Simulation of the demand-oriented routing protocol AODV under two synthetic mobility models: RWP (Random Way Point) and RPGM (Reference Point Group Model).

To simulate AODV under random waypoint mobility model, a number of nodes (from 10-50) are uniformly distributed in an area size of 1186*584 sq. m. having CBR traffic type. And to simulate AODV under reference point group mobility model, five configurations with different number of nodes have been configured as follows:

- *Configuration I:* When network size is small i.e. network is having 10 nodes only, then 1 group with 10 nodes is configured.
- *Configuration II:* For 20 nodes, 2 groups are configured with 10 nodes each.
- *Configuration III:* For 30 nodes, 3 groups are configured with 10 nodes each.
- *Configuration IV:* For 40 nodes, 4 groups are configured with 10 nodes each.
- *Configuration V:* For 50 nodes, 5 groups are configured with 10 nodes each.

The movement scenarios of nodes for both mobility models are generated through bonnmotion tool.

Step 2: Simulation of AODV under wormhole attack using two mobility models: RWP (Random Way Point) and RPGM (Reference Point Group Model).

To simulate wormhole attack, malicious nodes are kept at different locations in the already created topology for both mobility models and the required coding is done to create wormhole tunnel with the help of other nodes in the network, which bypass normal route. In this scenario, minimum number of malicious nodes is 1, but tunnel length increases as network size increases.

Step 3: Graphical analysis and performance comparison of normal AODV and AODV under attack environment using RWP and RPGM.

Using AWK scripts, various performance metrics such as PDR, average throughput, jitter and average end to end delay have been analyzed graphically and comparison is done between AODV without attack and AODV under attack by varying number of nodes.

Step 4: Analysis of the malicious nodes which are participating to make wormhole peer list in the network.

To analyze malicious nodes, an implementation has been done at NS2 link layer. Required coding has been done in ll.cc and ll.h files at link level. Firstly, in ll.cc and ll.h files, parameters such as size of wormhole peer list (tunnel) and properties of nodes are defined and then in Tcl file, the definition of nodes is configured. During this analysis, the tunnel length varies from 1 to 5 nodes.

The simulation parameters for all above steps are shown in Table 1:

TABLE I SIMULATION PARAMETER

Parameters	Value
Simulator	NS-2 Version 2.35
Number of Nodes	10, 20, 30, 40, 50
Topography Dimension (m*m)	1186*584
Simulation Time	90 seconds
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground Model
MAC Type	802.11 MAC Layer
Data Rate	2.0 Mb
Mobility Models	Random Waypoint, Reference Point Group
Routing Protocol	AODV
Interface Queue	Drop Tail/Priority Queue
Channel	Wireless Channel
Link Layer Type	LL
Antenna Type	Omni direction
Minimum Number of Malicious Nodes	1
Tunnel Length	1-5 nodes
Probability of Group Change	0.01
Maximum Distance between Groups	1.0
Average Number of Nodes in a Group	10
Min Speed and Max Speed of Nodes	0.5 and 1.5 m/s
Performance Metrics	PDR, Average Throughput, Average End to End Delay and Jitter
Examined Approaches	without attack and under attack

V. RESULTS & DISCUSSION

A. *Performance Analysis of AODV Protocol under RWP and RPGM*

AODV Protocol is simulated by varying number of nodes using CBR traffic and two mobility models.

1) *Average throughput*

The throughput tends to fluctuate with the increase in network size under random waypoint model. Reference point group mobility model offers higher throughput than the random waypoint.

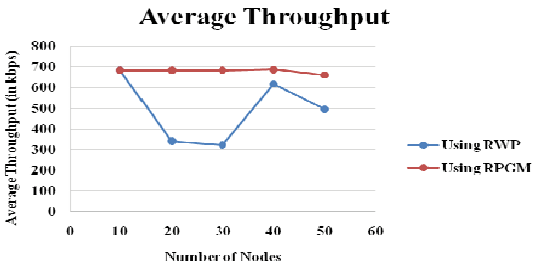

Fig. 5 Average Throughput of AODV under Different Mobility Models

2) *Average end to end delay*

Random waypoint model exhibits lesser delay than the reference point group mobility model. Due to configuration of various groups in reference point group model, delay is high in case of RPGM, but value of delay decreases as number of nodes or groups increases in RPGM.

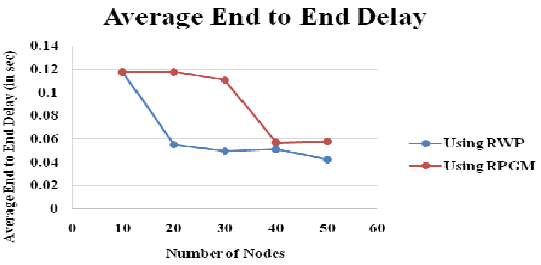

Fig. 6 Average End to End Delay of AODV under Different Mobility Models

3) *Packet delivery ratio*

The packet delivery ratio decreases with increase in network size. And the value of PDR under RPGM is more as compared to RWP. Initially, packet delivery ratio remains constant for network size of 10 and 20 in RPGM, but then decreases gradually.

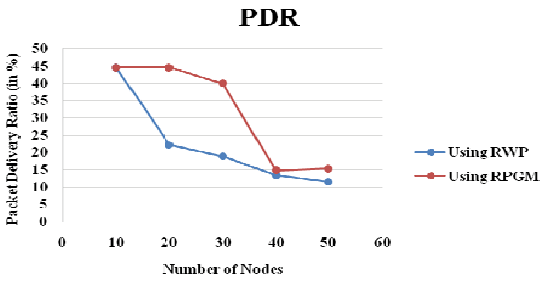

Fig. 7 Packet Delivery Ratio of AODV under Different Mobility Models

4) *Jitter*

There is a fluctuation in jitter graph for RWP. But for RPGM, the values are nearly same as number of nodes increases up to 40 nodes, but after that it decreases. Overall jitter is high in case of RPGM.

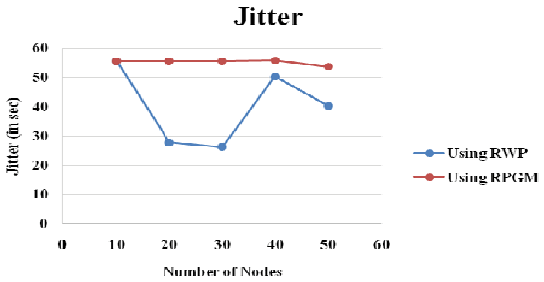

Fig. 8 Jitter of AODV under Different Mobility Models

B. *Performance Analysis of AODV under Attack Environment using RWP and RPGM*

1) *Average throughput*

The value of throughput decreases as network size and tunnel length increases in case of RPGM. But in RWP, throughput varies.

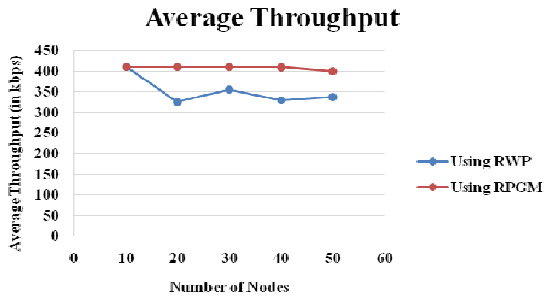

Fig. 9 Average Throughput of AODV under Attack using Different Mobility Models

2) Average end to end delay

There is a variation in delay in both scenarios. But delay increases as network size and tunnel length increases. Overall RPGM exhibits more delay due to increase in network size, tunnel length and number of groups.

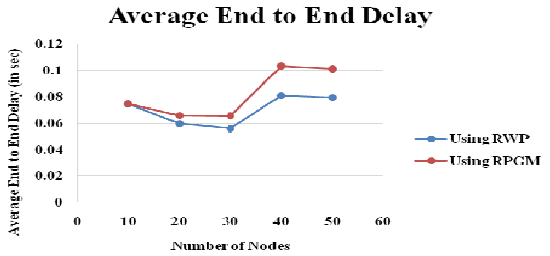

Fig. 10 Average End to End Delay of AODV under Attack using Different Mobility Models

3) Packet Delivery Ratio

Initially, the value of PDR decreases up to 30 nodes and then suddenly increases for 40 nodes and then again decreases. The sudden increase is due to the tunnelling and replaying nature of attack. More tunnel length and replay, more packets will be delivered.

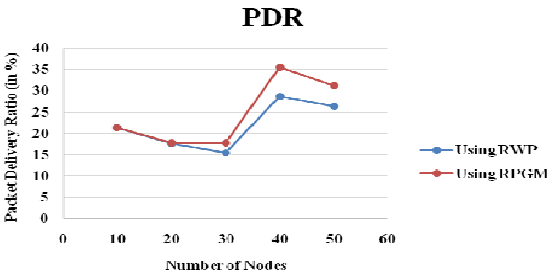

Fig. 11 Packet Delivery Ratio of AODV under Attack using Different Mobility Models

4) Jitter

Jitter is more in case of reference point group mobility model and it remains almost same up to 40 nodes and then decreases. But in case of random waypoint model, initially jitter is high and then variation starts.

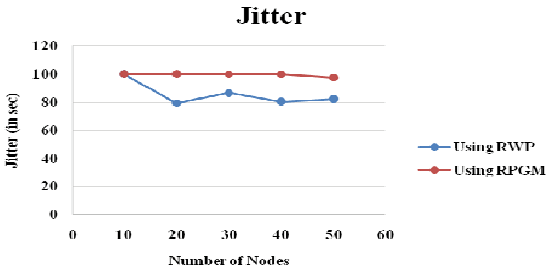

Fig. 12 Jitter of AODV under Attack using Different Mobility Models

C. Analysis of Malicious Nodes in Wormhole Peer List

Fig. 13 shows that malicious nodes 20, 21 and 22 are participating to make tunnel (having tunnel length 3 nodes) and disrupt the normal path of AODV protocol.

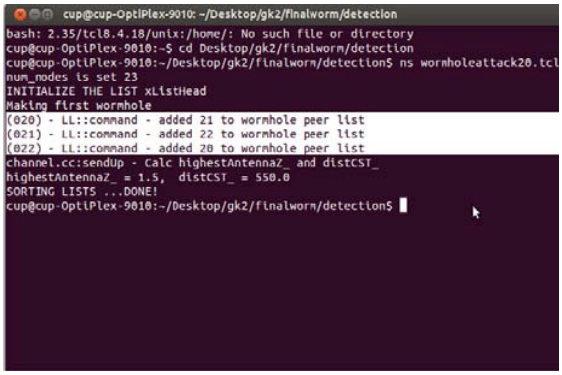

Fig. 13 Analysis of Three Malicious Nodes

Similarly, Fig. 14 shows that malicious nodes 30, 31, 32 and 33 are participating to make tunnel (having tunnel length 4 nodes) and disrupt the normal path of AODV protocol.

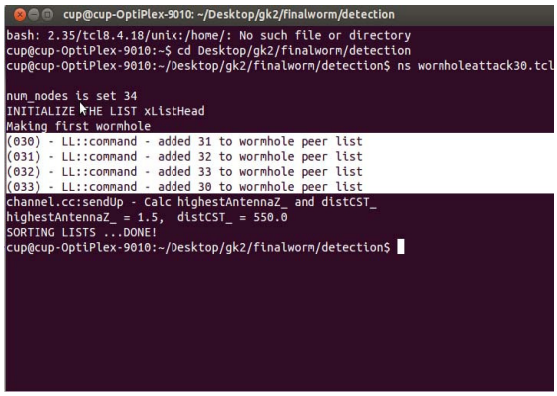

Fig. 14 Analysis of Four Malicious Nodes

VI. CONCLUSION

The performance analysis of AODV without attack and under attack has been carried out in a comprehensive manner using random waypoint and reference point group mobility models.

Firstly, AODV without attack is analyzed under random waypoint and reference point group models. Results show that AODV performs well for throughput, PDR and packet drop rate under RPGM and for delay and jitter under RWP. Secondly, AODV under wormhole attack is analyzed using two mobility models namely random waypoint and reference point group models. Analysis shows that AODV under attack gives high value for throughput, PDR, delay and jitter in RPGM and low for packet drop rate in RWP.

Along with above, one more step has been taken to analyze the malicious nodes which are making tunnel to perform attack.

REFERENCES

[1] ACoRN, "Ad Hoc Networks", *ARC Communications Research Network*, 2010, Available at: http://www.acorn.net.au/telecoms/adhocnetworks/adhocnetworks.html.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", *IEEE Wireless Communications*, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[3] C.E. Perkins, "Ad Hoc Networking with AODV", 2013, Available at: http:// www.psg.com/~charliep/txt/Daedeok2002/AODV-Daedeok.pdf.

[4] C. P. Vandana, and A. F. S. Devaraj, "Evaluation of Impact of Wormhole Attack on AODV", *International Journal of Advanced Networking and Applications*, vol. 4, no. 4, pp. 1652-1656, 2013.

[5] D. Kumar, A. Srivastava, and S. C. Gupta, "Routing in Ad Hoc Networks under Reference Point Group Mobility", *European Modelling Sysposium, IEEE Computer Society*, pp. 595-598, 2013.

[6] F. A. Jenefer, and D. Vydeki, "Performance Analysis of Mobile Ad Hoc Network in the Presence of Wormhole Attack", *International Journal of Advanced Computer Engineering and Communication Technology*, vol. 1, no. 1, pp. 13-18, 2013.

[7] F. Bai, and A. Helmy, "Chapter 1: A Survey of Mobility Models", pp. 1-30, Available at: www.cise.ufl.edu/~helmy/papers/Survey-Mobility-Chapter-1.pdf.

[8] F. Bai, N. Sadagopan, and A. Helmy, "User Manual for IMPORTANT Mobility Tool Genarators in NS-2 Simulator", pp. 1-12, Feb. 2004.

[9] G. K. Singh, A. Kaur, and A. L. Sangal, "Performance Analysis of DSR, AODV Routing Protocols based on Wormhole Attack in Mobile Ad-hoc Network", In *Proceedings of the 5th IEEE International Conference on Advanced Computing & Communication Technologies*, pp. 31-36, 2011.

[10] G. Kaur, and A. Kaur, "A Comprehensive Review on Performance of AODV Protocol for Wormhole Attack", *International Journal of Research in Engineering and Technology*, vol. 3, no. 5, pp. 531-537, May 2014.

[11] J. Singh, K. Kumar, M. Sachdeva, and N. Sidhu, "DDoS Attack's Simulation using Legitimate and Attack Real Data Sets", *International Journal of Scientific & Engineering Research*, vol. 3, pp. 1-5, June 2012.

[12] N. Gandhewar, and R. Patel, "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Ad Hoc Network", In *Proceedings of the Fourth International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society*, pp. 714-718, 2012.

[13] N. Khemariya, and A. Khuntetha, "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs", *International Journal of Computer Applications*, vol. 66, pp. 18-24, March 2013.

[14] P. G. Argyroudis, and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, Third Quarter, vol. 7, no. 3, pp. 2-21, 2005.

[15] R. Agrawal, R. Tripathi, and S. Tiwari, "Performance Comparison of AODV and DYMO MANET Protocols under Wormhole Attack Environment", *International Journal of Computer Applications*, vol. 44, no. 9, pp. 9-16, April 2012.

[16] R. Baumann, "AODV: Ad hoc On Demand Distance Vector Routing Protocol", pp. 1-19, April 2002, Available at: http://www.rainer-baumann.ch/public/qec.pdf.

[17] R. Mohan, C. Rajan, and N. Shanthi, "A Stable Mobility Model Evaluation Strategy for MANET Routing Protocols", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 12, pp. 58-65, Dec. 2012.

[18] S. Gandhi, N. Chaubey, N. Tada, and S. Trivedi, "Scenario-based Performance Comparison of Reactive, Proactive and Hybrid Protocols in MANET", In *Proceedings of the IEEE International Conference on Computer Communication and Infomatics*, pp. 1-5. 2012.

[19] S. Gupta, S. Kar, and S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", In *Proceedings of the* IEEE International Conference on Innovation Technology, pp. 226-231, 2011.

[20] S. Kumar, D. Singh, and M. Chawla, "Performance Comparison of Routing Protocols in MANET Varying Network Size", *International Journal of Smart Sensors and Ad Hoc Networks*, vol. 1, no. 2, pp. 51-54, 2011.

[21] S. Kumar, S. C. Sharma, and B. Suman, "Impact of Mobility Models with Different Scalability of Networks on MANET Routing Protocols", *International Journal of Scientific & Engineering Research*, vol. 2, no. 7, pp. 1-5, July 2011.

[22] T. Issariyakul, and E. Hossain, "Introduction to Network Simulator", *Computer Networks*, 2011, Available at: books.google.co.in/books?isbn=1461414067.

[23] V. C. Patil, "Chapter-3: Overview of Mobile Ad Hoc Networks", pp. 19-36, 2012, Available at: http://www.shodhganga.inflibnet.ac.in/bitstream/10603/4106/.../11_chapter%203.pdf.

[24] V. K. Upadhyay, and R. Shukla, "An Assessment of Worm Hole Attack over Mobile Ad-Hoc Network as Serious Threats", *International Journal of Advanced Networking and Applications*, vol. 5, pp. 1858-1866, 2013.

[25] V. Mahajan, M. Natu, and A. Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", In *Proceedings of the IEEE Military Communications Conference (MILCOM)*, pp. 1-7. 2008.