A Trust and Co-Operative Nodes with Affects of Malicious Attacks and Measure the Performance Degradation on Geographic Aided Routing in Mobile Ad Hoc Network

Sudhakar Sengan[1], Dr.S.Chenthur Pandian[2]

[1.] Research Scholar, Anna University, Chennai, Tamil Nadu, India.
[2.] Principal, Dr.Mahalingam College of Engineering and Technology, Pollachi, TamilNadu, India.
sudhakarsengan@gmail.com

Abstract: This paper proposes to study the impact of malicious nodes on Mobile Ad hoc Networks (MANETs). Due to their flexibility and independence from network infrastructure like base stations, it is being widely researched. Routing in MANETs is more challenging when compared to conventional networks due to various characteristics like dynamic network topology, limited bandwidth and limited battery power. Early research focused on developing efficient routing mechanisms in dynamic and resource-constrained networks in MANETs. Most of the routing protocols were suggested mainly based on the assumption of trust and cooperative nature amongst the nodes. Thus, the MANET is vulnerable to malicious node attacks. Geographic routing research, a recent approach compared to topological routing received attention due to improved routing capability resulting from accurate geographic information. This study investigates the impact of malicious nodes on geographic routing; through simulations conducted to evaluate network performance degradation caused by malicious node activity. Simulation studies demonstrate that the networks with 15% malicious nodes show significant performance degradation.
[Sudhakar Sengan, S.Chenthur Pandian**. A Trust and Co-Operative Nodes with Affects of Malicious Attacks and Measure the Performance Degradation on Geographic Aided Routing in Mobile Ad Hoc Network.** *Life Sci J* 2013;10(4s):158-163] (ISSN:1097-8135). http://www.lifesciencesite.com. 24

Keywords: MANET, Ad hoc Network Routing, Position-Based Routing, Malicious Attacks, Throughput.

1. Introduction

A MANET consists of assorted mobile devices in a network sans centralized administration and infrastructure. MANETs are low cost constructions as they do not rely on network infrastructure and are also highly mobile. Such MANET characteristics are helpful in emergency operations, military service, disaster relief, campus networks, vehicle networks, maritime communications and casual meetings (N.S.Chen *et al.,* 2008). Unlike traditional networks, a MANET due to node mobility has a dynamic, continuously changing network topology (Song Ci *et al*.,2006). This causes problems in MANET routing when compared to traditional wired networks. Resource constraint is another MANET characteristic, such as limited bandwidth and limited battery power, which affects its routing. So naturally, early MANET research aimed to provide routing at minimum cost regarding bandwidth and battery power.

Routing protocols used at present are classified into reactive and proactive routing protocols. Reactive protocols such as Ad hoc On Demand Distance Vector (AODV) (Charles.E, *et al.,*2003), sources routes to the destination nodes only when required. Whereas in proactive protocols such as Optimized Link State Routing (OLSR) protocol (P.Jacquet *et al.,* 2001), nodes updates network topology information regularly and route information is also updated in its cache. Routing protocols relies on inter node cooperation, and assumes that nodes are trustworthy and behave without malicious intention. Though, due to lack of central administration, MANETs face attacks disrupting routing operations or denial-of-service (DoS) attacks launched by malicious node (Shevtekar.A *et al.,* 2005).The malicious behaviour affects legitimate nodes services resulting in network performance degradation. Various studies were recently undertaken with the view of countering malicious attacks, as earlier works aimed to provide preventive procedures to protect MANET routing (Thanigaivel.G *et al., 2012;* Quan Jia *et al.,* 2011).

Usually, key management/encryption techniques based schemes are incorporated in the routing to ensure that unauthorized nodes do not join networks. The issue with such approaches is heavy traffic load which are introduced to exchange and verify keys, leading to the escalating cost regarding bandwidth-constraint for MANET nodes with limited resources. Routing for ad hoc networks like Ariadne (Yih-Chun Hu *et al*.,2005), ARAN (Kimaya Sanzgiri *et al.,* 2002),secure AODV (SAODV) (Manel Guerrero Zapata *et al.,* 2002)are available in the literature, which outline preventive schemes based on authentication. Though, not many works are available to offset malicious attacks in Geographic routing protocols. This study proposes to learn malicious nodes impact in MANETs for Geographic routing protocols. Simulations evaluate network degradation performance caused by malicious nodes.

Geographic routing protocols have many advantages when compared to traditional ad hoc routing strategies. To begin with such protocols allow path adaptation through best next hop selection based on the availability of an intermediate node used earlier. Path selection does not depend on table maintenance procedures due to lack of route creating process. Other advantages include capacity utilization of weight additional metrics for the next hop selection. Route alternation is one a node by node taking into consideration neighbour related QoS like bandwidth and delay (Lemmon.Colin *et al.,* 2009).

2. Material and Methods

Geographic Routing Protocol

Geographic routing protocols (GRP) are considered as a type of stateless routing(Hui Cheng *et al.,* 2008). Nodes perform maintenance functions for topological information only with its one-hop neighbourhood. The advantage of GRP over topological routing is that network-wide control message dissemination is not required, and it is feasible for large-scale networks. The memory usage of nodes is lower in GRP due to local information maintenance. Usually, GRP has two components: location service and geographic forwarding process. Location service helps to identifying the destination packet position which improves routing process by creating a path from the source node through intermediary nodes. The packet header of the message contains the Packet destination position thus ensuring that intermediate hops identify the packet's ultimate destination (Chen.D *et al.,* 2007).

GRP periodically transmit hello message called beacons to 1-hop neighbors to discover neighbor's positions. This often leads to problems such as collisions, waste of resources, imprecise neighborhood tables. Beaconless GRP are proposed in literature which avoids the overhead caused by the beacons (Sanchez.J *et al.,* 2009; Basagni .S *et al.,* 2009). Most of the beaconless GRP are based on reactive neighbourhood discovery.

GRP uses either a geographic greedy-forwarding mode or void-handling mode. In greedy-forwarding mode, the next-hop node for packet forwarding is defined to considering current node, neighbouring node and destination node positions. The node's position is sourced either by GPS receiver or localization algorithms. The neighbouring nodes positions are maintained in the node's centralized neighbourhood table (Zorzi.M *et al.,* 2003*)*. Finally, the destination node's position becomes part of the packet header from the source node. However, if an intermediate node knows a better destination position, this is updated in path header before packet forwarding.

Related Work

(Marin-Perez R *et al.,* 2011) proposed a Self-Protected Beaconless Geographic Routing (SBGR) protocol to mitigate insider attacks such as Sybil and Sinkhole attacks. SBGR ensures secure delivery of data packets to destinations in presence of malicious nodes. The proposed SBGR enhances the forwarding logic in GRP to include additional transmissions on detection of suspicious traffic. In the proposed mechanism, the attacks are dealt with no extra cost or overhead. Simulation results demonstrate that the SBGR performs better than the existing reputation based systems and achieves nearly a 100% packet delivery ratio.

(Shim.Y.C.2009) proposed a novel geocast protocol for transmitting packets within a specific geographic region. The proposed protocol is based on a multicast tree for geocast node connections for energy efficient broadcasting techniques. The multicast tree does not restrict geocast region shape. Reduced energy consumption and in-network data aggregation achieved in the suggested method. Security mechanisms are integrated for protection of the multicast tree from inside and outside attackers. Malicious nodes in the network are identified by Watch nodes.

(Dhanalakshmi.S *et al.,* 2008) developed RSF (Reliable and Secure Framework) for detection and isolation of malicious nodes. Destination nodes on detection of malicious nodes isolate them by discarding the route. A Reliable Multipath Routing (RMR) algorithm is introduced for identifying a set of node-disjoint dependable paths. Dispersion algorithm is used for finding multiple paths and data packets are transmitted along with them. Simulation results proved that this method achieved reduced overhead, less amount of delay and improved packet delivery ratio.

(Rashid Hafeez Khokhar *et al.,* 2008) studied various routing attacks in MANET. Attacks such as flooding, link spoofing, colluding misrelay attacks, black hole and wormhole were studied and an overview of available solutions to secure MANET protocols was discussed. Most of the proposed countermeasures in literature are based on cryptography and key management. These solutions are effective, but have higher overhead network. The study concludes that though some countermeasures perform well for one malicious node but are not effective for multiple colluding attackers.

(Kannhavong.B *et al.,* 2008) proposed security aware optimized link state routing to secure network routing. In the proposed method, on successful control traffic arrival, two hop neighbours acknowledge it. Attacks like link spoofing, wormhole attack and colluding misrelay attacks were offset by this method. Location information/complete topology were not needed for network protection. Simulation proved that the proposed methods achieved higher

packet delivery ratio before malicious nodes than the standard OLSR.

(Li Zhao *et al.,* 2007) proposed MARS, a MultipAth Routing Single path transmission approach for locating misbehaving node. The protocol defends against misbehaving nodes by coordinating multipath routing, single path data transmission, and whole feedback mechanism. Simulations were conducted to evaluate MARS approach and improved E-MARS approach under different adverse situations. The simulation results demonstrated the improved performance regarding network overhead for MARS and E-MARS approaches. The MARS attained 45% more data delivery when the network had 20% misbehaving nodes.

3. Results

Simulation Tool

To simulating the OPNET 14.5 modeler is used with the help of a tool. OPNET consists of network and application based software which is used for network management and analysis [Opnet; 2010]. An OPNET model provides communication devices, various protocols, architecture of different networks and technologies and gives simulation of their performances in virtual environment. In various research and development areas, OPNET generally delivers the solution which helps in research of analysis and improvement of various wireless technologies like WIMAX, Wi Fi, UMTS, analysis and designing of MANET protocols, improving core network technology, providing power management solutions in wireless sensor networks.

Simulation Environment

By this criterion, we used OPNET for modeling of network nodes, selecting its statistics and then running its corresponding simulation to get the outcome of their result for analysis.

The simulation environment includes 20 nodes which act as client and one node as server. All nodes run on a TCP/IP or UPD/IP network. An 11 Mbps data rate is maintained for nodes, and their transmission power of 0.005 watts and reception power threshold set at -95dBm is maintained. Nodes are mobile at random trajectories. FTP traffic was generated randomly. Experiments simulated geographic routing protocol with all nodes cooperating and only 15% of them are being malicious. Figure 1 shows simulation setup test bed with one server node and 20 client nodes. Table I reveals simulation values from the first six minutes simulation.

To consider the simulation area is taken as 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). Random way point mobility is to select with the constant speed of 10 meter/seconds and limited pause time of content 100 seconds. After delivering data to their destination, the corresponding pause time is taken.

Our goal was to determine the protocol with a little amount of vulnerability in case of malicious attacks. To choose GRP routing protocols for mainly reactive and proactive protocols respectively. In both the cases of GRP, malicious node buffer size is lowered level which is to increase the packet drop. Furthermore the simulation parameters are given in Table 1.

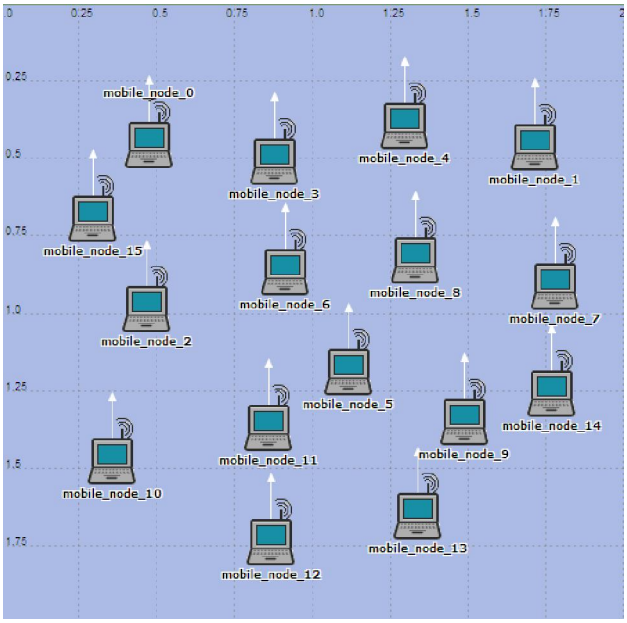

Figure. 1: The Layout used in our Simulated Environment with 20 Nodes.

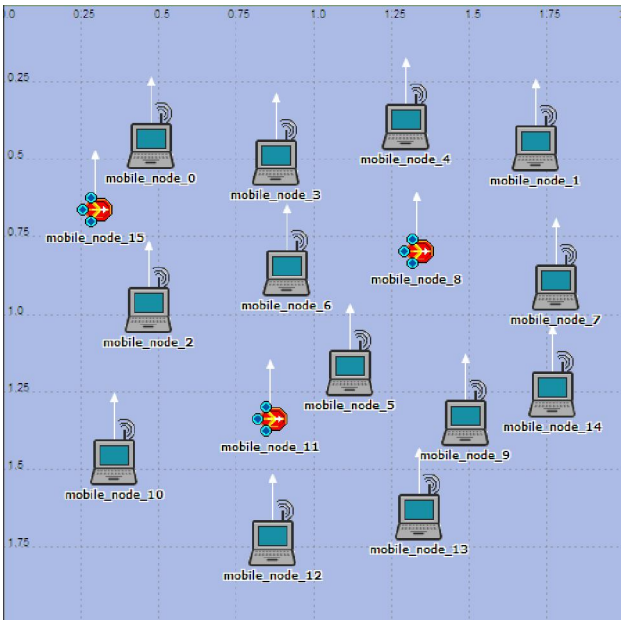

Figure.2: The Layout used in our Simulated Environment with 20 Nodes with Attacks.

Table 1. Simulation Parameters

Simulation Parameters	
Tested Protocol	GRP
Time	1000 seconds
Area (m x m)	1000 x 1000
Number of Nodes	20
Travel Type	TCP/IP or UPD/IP
Performance Factor	Traffic Sent and Received , Retransmission Attempts and Throughput
Pause Time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time(s)	exponential(1)
Packet Range (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint
Power Threshold	-95dBm

Figure 3 to Figure 6 disclose network performance with regard to traffic received, sent, retransmission attempts and throughput respectively. The graphs show that network performance is degraded, and throughput is drastically reduced before attacking malicious nodes.

From figure 3, it describes that the routing traffic is transmitted from various sources to destinations decreases by 39.63% due to the presence of malicious nodes.

Traffic Received Comparison *(bps)*

The following Tables of the simulation results are obtained during the first 6 minutes of simulation of during the packet transmission to occur the traffic by received.

Table 2. Traffic Received in *bps*.

Simulation Time	Traffic Received in *bps*	
	Normal	Attack
0	7686.8889	3315.7778
36	15031.556	6481.7778
72	16920	5503.3333
108	15867.333	5738.6667
144	16002.889	5753.3333
180	15333.556	6427.7778
216	15750.222	5838
252	14532	6132.4444
288	17249.556	6601.7778
324	16057.556	5803.5556
360	15125.778	6042.8889

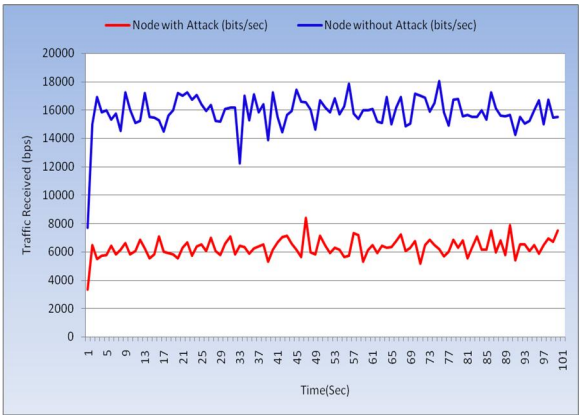

Figure 3. Traffic analysis for packet received.

Traffic Sent Comparison *(bps)*

The following Tables of the simulation results are obtained during the first 6 minutes of simulation of during the packet transmission to occur the traffic by sent.

Table 3.Traffic Sent in *bps*.

Simulation Time	Traffic Sent in *bps*	
	Normal	Attack
0	7820	3444
36	15376.67	6485.556
72	17481.11	5638.889
108	16074.22	6168
144	16257.33	5985.333
180	15825.56	6595.111
216	16201.11	6141.111
252	15071.11	6436.889
288	17717.33	7040.444
324	17104.89	5938.222
360	15935.33	6379.556

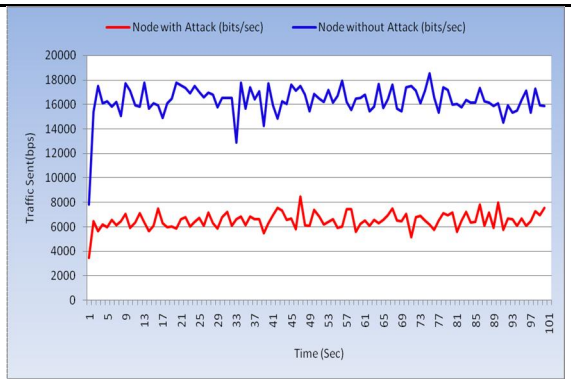

Figure 4. Traffic analysis for packet sent.

Packet Retransmission Comparison *(bps)*

The following Tables of the simulation results are obtained during the first 6 minutes of simulation of during the packet retransmission.

Table 4. Packet Retransmission Attempts in *bps*.

Simulation Time	Packet Retransmission in *bps*	
	Normal	Attack
0	0.191898	0.363095
36	0.158991	0.088496
72	0.243043	0.206997
108	0.166327	0.395706
144	0.130297	0.108504
180	0.137931	0.209091
216	0.155533	0.233236
252	0.192227	0.1875
288	0.162562	0.233596
324	0.20854	0.152738
360	0.197581	0.302671

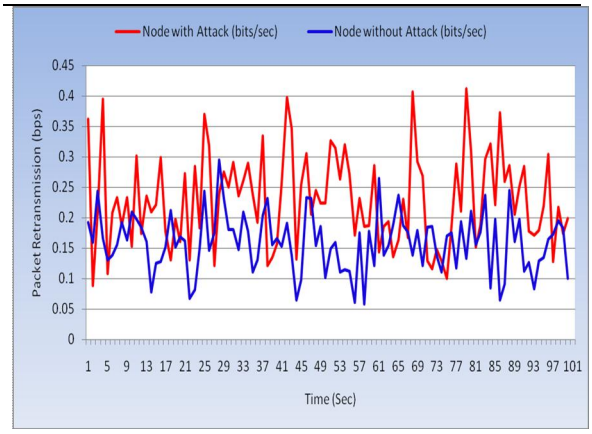

Figure 5. Retransmission attempts in number of packets.

Throughput Comparison *(bps)*

The following Tables of the simulation results are obtained during the first 6 minutes of simulation of during the throughput.

Table 5. Throughput Achieved in *bps*.

Simulation Time	Throughput in *bps*	
	Normal	Attack
0	63732.44	32487.556
36	56122.44	24854.889
72	60652	22918.667
108	57289.11	23120.889
144	59785.11	24023.778
180	56484.67	23797.556
216	59319.33	23887.111
252	55708.67	24040
288	60939.11	25750.222
324	59104.67	24087.778
360	57302.22	23782

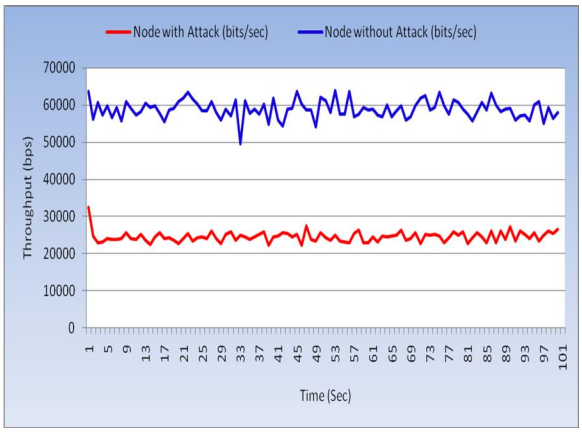

Figure 6. Throughput Analysis of no. of nodes with attack and without attack.

It is observed for the simulation results that the routing traffic sent from various sources falls by 39.9 % due to the presence of the malicious nodes. Since routes could not be created for random traffic from various sources to destinations, the throughput of the network falls down by 41.8% when the network contains 15% malicious nodes.

4. Discussions

In ad hoc network, the Performance degradation with geographic routing protocol under malicious nodes is investigated in this study. Simulation studies were conducted using 20 nodes of which 15% were malicious. Network throughput reduced significantly due to the malicious nodes in the network. Further work is required and throughput evaluated for larger networks. More investigations are needed only for larger networks and various malicious node types. Also, mechanisms to improve network performance and negate effect of malicious nodes should also be proposed.

Corresponding Author:
Sudhakar Sengan
Research Scholar
Anna University , Chennai,Tamil Nadu, India
E-mail: sudhakarsengan@gmail.com.

References

1. Nian-Shing Chen,Kinshuk,Chun-Wang Wei and Stephen J.H. Yang. Designing a Self-Contained Group Area Network for Ubiquitous Learning. Educational Technology & Society 2008;11(2):16-26.
2. Song Ci,Guizani.M,Hsiao-Hwa Chen, Sharif.H. Self-Regulating Network Utilization in Mobile Ad-hoc Wireless Network. IEEE Transactions on Vehicular Technology.2006;55(4):1302–1310.

3. Charles E.Perkins, E.Belding-Royer, and S.Das. Ad Hoc On demand Distance Vector (AODV) Routing, Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications 2003:90–100.
4. P.Jacquet, P.Muhlethaler,T.Clausen,A.Laouiti,A.Qayyum,L. Viennot Clausen, T. and P. Jacquet. Optimized Link State Routing Protocol for Adhoc Networks.Proceedings for IEEE Multi Topic Conference INMIC 2001:62-68.
5. Shevtekar.A,Karunakar Anantharam and Ansari. Low rate TCP Denial-Of Service Attack Detection At Edge Routers.IEEE Communications Letters 2005;9(4)**:**363–365.
6. Kimaya Sanzgiri**,** Bridget Dahill. A Secure Routing Protocol for Ad Hoc Networks . Proceedings of 10th IEEE International Conference on Network Protocols.2002:78-87.
7. Yih-Chun Hu , Adrian Perrig and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad-Hoc Networks. Journal Wireless Networks 2005 ;11(1-2):21-38.
8. Manel Guerrero Zapata, N. Asokan. Securing Ad-Hoc Routing Protocol.Proceedings of the 1st ACM Workshop on Wireless Security, Atlanta, Georgia, and USA 2002:1-10.
9. Lemmon.Colin, Lui Siu Man, and Lee. Geographic Forwarding and Routing for Ad-hoc Wireless Network: A Survey. Proceedings of the 2009 5th International Joint Conference on INC, IMS and IDC, NCM ’09, IEEE Computer Society, Washington, DC, USA. 2009:188–195.
10. Hui Cheng, Jiannong Cao. A Design Framework and Taxonomy for Hybrid Routing Protocols in Mobile Ad Hoc Networks. Journal of IEEE Communications Surveys & Tutorials 2008; 10(3):62-73.
11. Chen.D, Varshney.P.K.A. Survey of Void Handling Techniques for Geographic Routing in Wireless Networks. IEEE Communications Surveys & Tutorials 2007; 9(1):50-67.
12. Zorzi.M, Rao.R.R. Geographic Random Forwarding (GERAF) for Ad hoc and Sensor Networks: Energy and Latency Performance. IEEE Transactions on Mobile Computing 2003:349–365.
13. Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala.A Review of Current Routing Attacks in Mobile Ad Hoc Networks.International Journal of Computer Science and Security 2008;2(3):18-29.
14. Kannhavong.B, Nakayama.H, Jamalipour.A. SA-OLSR: Security Aware Optimized Link State Routing for Mobile Ad Hoc Networks.IEEE International Conference on Communications, ICC '08. 2008:1464-1468.
15. Lidong Zhou, Haas .Z.J. securing Ad Hoc Networks.IEEE Network Magazine 1999; 13(6): 24-30.
16. Li Zhao, Delgado-Frias.J.G.MARS: Misbehavior Detection in Ad Hoc Networks. IEEE Global Telecommunications Conference GLOBECOM '07. 2007:941–945.
17. Dhanalakshmi.S, M. Rajaram. A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET. International Journal of Computer Science and Network Security 2008; 8(10):184-190.
18. Shim.Y.C. Secure Efficient Geocast Protocol for Sensor Networks with Malicious Nodes. Proceedings of the 8th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications, Wisconsin, Cambridge, UK. 2009:179-184.
19. Thanigaivel.G, KumarN.A, Yogesh.P. TRUNCMAN: Trust based Routing Mechanism using Non-Cooperative Movement in Mobile Ad-Hoc Network. Second IEEE International conference on Digital Information and Communication Technology and its Applications (DICTAP) 2012:261–266.
20. Quan Jia, Kun Sun, Stavrou A.CapMan: Capability-Based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET. Proceedings of IEEE International Conference on Computer Communications and Networks (ICCCN) 2011:1-6.
21. Marin-Perez R, Ruiz.P.M. SBGR: A Simple Self-Protected Beaconless Geographic Routing for Wireless Sensor Networks. 8th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS) 2011:610-619.
22. Sanchez J, Ruiz.P and Marin-Perez R. Beacon-Less Geographic Routing Made Practical: Challenges, Design Guidelines, and Protocols. IEEE Communications Magazine 2009:85-91.
23. Basagni .S, Nati.M,Petrioli C, Petroccia. R.ROME: Routing Over Mobile Elements in WSNs. IEEE conference on Global Telecommunications GLOBECOM 2009:1-7.
24. Opnet Technologies, Inc. “Opnet Simulator,” Internet: www.opnet.com, date last viewed: 2010-05-05.

1/15/2013