Volume 3, Issue 1, January 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Worm Hole Attack In MANET And Avoidance Using Robust Secure Routing Method

K. Sivakumar, M.Sc, MCA, M.Phil, (Ph.D).
Assistant Professor,
Dept of Comp Application,
SNMV CAS, Cbe.

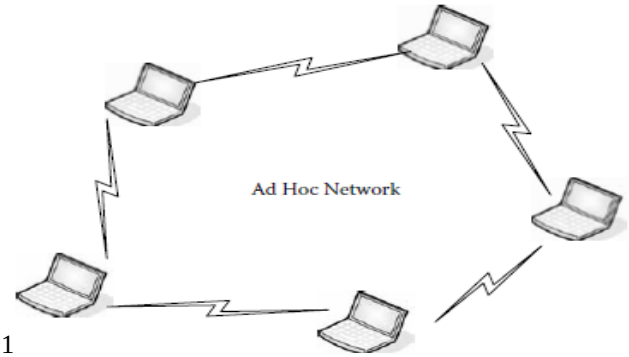
Dr. G. Selvaraj,
Professor,
Dept of Comp. Sci & Engg,
Oxford College of Engg, Thiruvannamalai.

Abstract:- Mobile ad hoc networks (MANETs) are collections of self-organizing mobile nodes with dynamic topologies and no fixed infrastructure. In MANET, the more security is required in comparison to wired network. Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack. The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route with fewer. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. One particular type of attacks our protocol cannot prevent is wormhole exploits In wormhole attacks, an attacker receives packets at one point in a network, tunnels them to another point in the network, and replays them into the network from that point. Colluding adversaries can use this attack. To avoid this worm hole attack using the RSR protocol and using different approach and it is simulated using OPNET Modeler.

Keywords: - RSR, DSR, Security, attack, wormhole, Path, Tracing, OPNET.

I. Introduction

An ad hoc network is a collection of wireless mobile nodes (or routers) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the Internet. Multihop, mobility, large network size combined with device heterogeneity, bandwidth, and battery power constraints make the design of adequate routing protocols a major challenge. Some form of routing protocol is in general necessary in such an environment, because two hosts that may wish to exchange packets might not be able to communicate directly, as shown in Figure



1.1

Fig 1.1: Ad Hoc Network

A mobile ad hoc network (MANET) group has been formed within IETF. The primary focus of this working group is to develop and evolve MANET specifications and introduce them to the Internet standard track. The goal is to support mobile

ad hoc networks with hundreds of routers and solve challenges in this kind of network. Some challenges that ad hoc networking faces are limited wireless transmission range, hidden terminal problems, packet losses due to transmission errors, mobility- induced route changes, and battery constraints. Mobile ad hoc networks could enhance the service area of access networks and provide wireless connectivity into areas with poor or previously no coverage (e.g., cell edges). Connectivity to wired infrastructure will be provided through multiple gateways with possibly different capabilities and utilization. To improve performance, the mobile host should have the ability to adapt to variation in performance and coverage and to switch gateways when beneficial. To enhance the prediction of the best overall performance, a network-layer metric has a better overview of the network. Ad hoc networking brings features like easy connection to access networks, dynamic multihop network structures, and direct peer-to-peer communication. The multihop property of an ad hoc network needs to be bridged by a gateway to the wired backbone.

II. Attacks In MANET

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types.

Network either as internal, external or/ as well as active or passive attack against the network.

A. Internal Attacks Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them.

B. External attacks These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories.

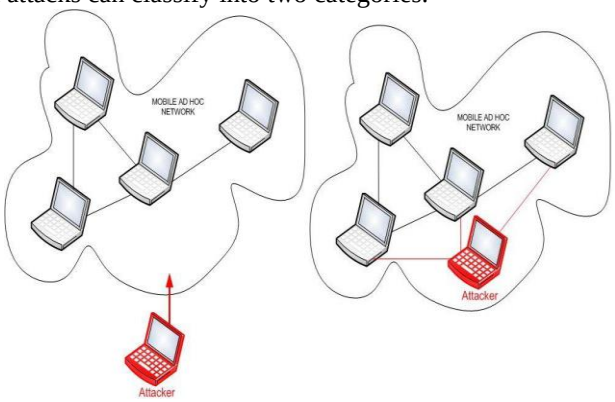


Fig 2.1: External & Internal Attack in MANETs

Passive attacks MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic.

Active Attacks Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination.

Active attacks are classified into four groups:

- ***Dropping Attacks:*** Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point. Most of routing protocol has no mechanism to detect whether data packets have been forwarded or not.
- ***Modification Attacks:*** Sinkhole attacks are the example of modification attacks. These attacks modify packets and disrupt the overall communication between network nodes. In sinkhole attack, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing information and uses it for further attacks such as dropping and selective forwarding attacks.
- ***Fabrication Attacks:*** In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.
- ***Timing Attacks:*** In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

In a standard network (Local Area Network or LAN) there are 7 OSI layers (Physical, Data link, Network, Transport, Session, Presentation, Application layer). In comparison to LAN or WLAN, the security of MANET can be divided into 5 OSI layers: Application layer, Transport layer, Network layer, Data link layer and Physical layer. According to the specific layer there are various types of attacks which differ in their essence.

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Eavesdropping, jamming, active interference

Table 2.1: Different Types of Attacks according to Layers

III. WORM HOLE ATTACK

Network layer is the third lowest layer of OSI reference model. The function of network layer in OSI layer model is to provide the services for exchanging the individual piece of data/information over the network between identified end devices. To achieve the integrity four basic processes are involved in it.

- Addressing.
- Encapsulation.
- Routing.
- De-capsulation.

The network layer in MANET uses ad hoc routing and does packet forwarding. In MANET nodes act as host and router. Therefore router discovery and router maintains in the MANET is effectively concern.

Thus attacking on MANET routing protocol not only disrupt the communication on the network even worst it paralyzed the whole communication all over the network. Therefore, a security in network layer plays a vital role to ensure the secure data communication in the network.

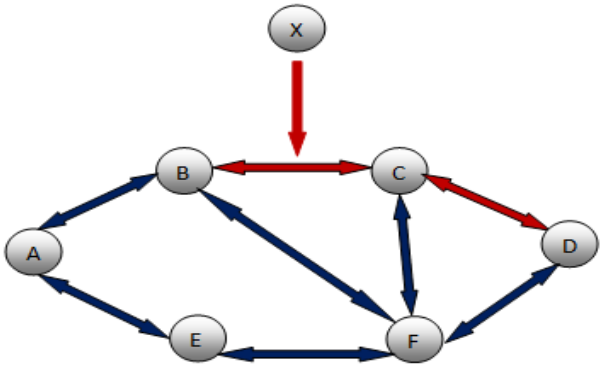


Fig 3.1: Routing Attack by Malicious Node

The wormhole attack is one of the most efficient and merciless attacks, which can be executed within MANET. Therefore two collaborating attackers should establish the so called wormhole link (using private high speed network e.g. over Ethernet cable or optical link): connection via a direct low-latency communication link between two separated distant points within MANET. As soon as this direct bridge (wormhole link) is built up one of the attackers captures data exchange packets, sends them via the wormhole link to the second one and he replays them.

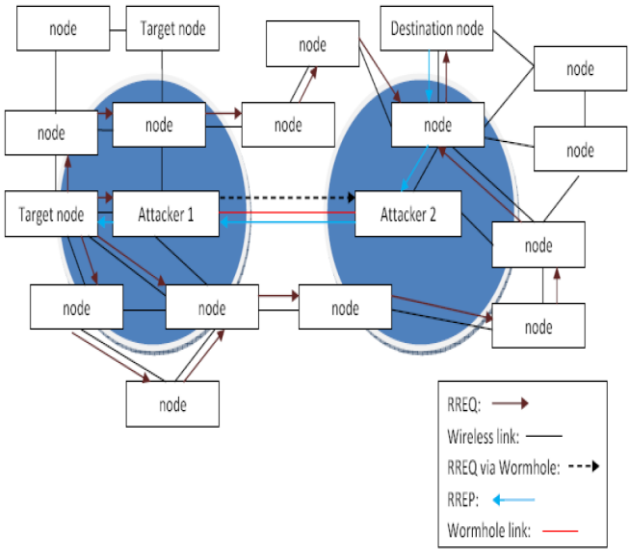


Fig 3.2: Wormhole Attack

In wormhole attack, a tunnel is created between two nodes that can be used to secretly transmit packets. In a wormhole attack, an attacker 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.

For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multihop route, for example through use of a single long range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole.

If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently.

The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbor of) that node. For example, when used against an on-demand routing protocol such as DSR or AODV, a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery.

3.1 Classification of Wormhole Attack

It is difficult to detect such dangerous attacks and no one can predict what the wormhole nodes can do and where and when. The wormhole attack is invisible at the higher layer and therefore, two end points of the wormhole are not visible in the route in which detection becomes much more complex. Wormhole can be classified into further five categories as proposed,

- Wormhole using Encapsulation.
- Wormhole using out of band channel.
- Open wormhole attack.
- Closed wormhole attack.
- Half open wormhole attack.
- Wormhole with high power transmission.

3.1.1 Wormhole Using Encapsulation

When nodes S broadcast for the RREQ to its neighbors node C and node D, where as node A1 and node A2 are colluding attacker. Nodes A1 records the RREQ request as forward from node C. Node A1 tunnels the RREQ to its partner A2, and rebroadcast to its neighbors H. The request is transmitted quicker than the request from node S to node A1. As a result node

D decide a route D-H-C-S and delete the route it had it before in its routing table. On the other side node S choice route S-H-D which pass through A1 and A2. As shown in the figure 3.3

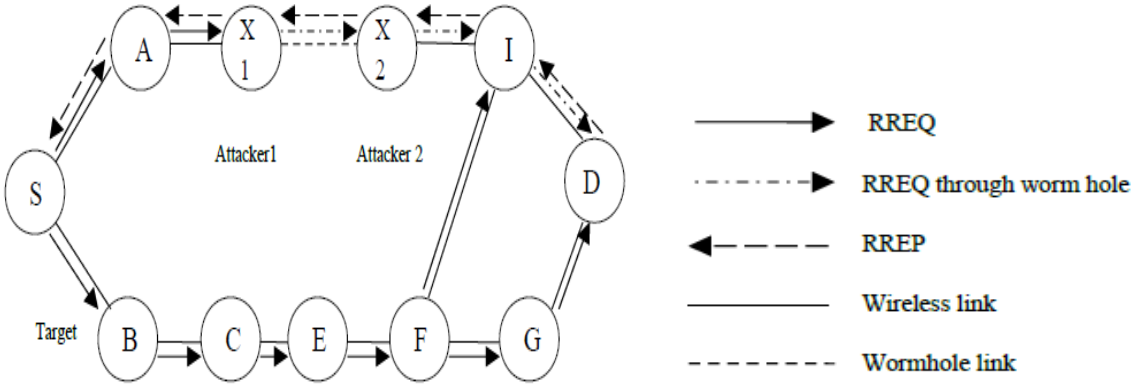


Fig 3.3: Wormhole Attacker Redraw

3.1.2 Open wormhole attack

In this attack malicious node keep examine the wireless medium to process the discovering RREQ packets, in the presence of malicious node in the network other node on the network suppose that malicious node are present on path and they are their direct neighbours.

3.1.3 Closed wormhole attack

The attacker does not modify the capture packet nor did it modify the packet field head. The attacker take the advantage when the packets are in the process to find a route know as route discovery. At route discovery process attack tunnel the packet from one side of the network to another side of the network and re-broadcast packets.

3.1.4 Half open wormhole attack

In this attack only one side of the packet is modify from the malicious node and the other side of the malicious node do not modify the packet subsequently route discovery procedure.

3.1.5 Wormhole with high power transmission

In this attack malicious node use maximum level of energy transmission to broadcast a packet, When malicious node received a Route Request (RREQ) by using route discovery process, it broadcast the Route Request (RREQ) at a maximum level of energy of it power so the other node on the network which are on the normal power transmission and lack of high power capability hears the maximum energy power broadcast they rebroadcast the packet towards the destination.
By doing this malicious node get more chances to create a route between source and destination without using colluding node.

IV. ROBUST SECURE ROUTING

A secure on-demand, multipath source routing protocol, called robust source routing (RSR). In addition to providing data origin authentication services and integrity checks, RSR is able to mitigate against intelligent malicious agents that selectively drop or modify packets they agreed to forward. Simulation studies confirm that RSR is capable of maintaining high delivery ratio even when a majority of the MANET nodes are malicious.
RSR has two phases: route discovery and route utilization and maintenance. We give an overview of each phase below.

1. Route Discovery
2. Route Utilization and Maintenance.

4.1 Threat Model

In wormhole attacks, an attacker receives packets at one point in a network, tunnels them to another point in the network, and replays them into the network from that point. Colluding adversaries can use this attack, for example, to forward route request packets in an attempt to increase the likelihood of adversarial entities controlling routing paths.
If a wormhole exhibits adversarial activities, our protocol mitigates against these exploits by treating the wormhole as a single link and make efforts to avoid utilizing it.
The following specific example gives the malicious behaviors and show how RSR mitigates against these possible exploits.

1. A Single Malicious Node on a Routing Path.
2. Colluding Malicious Nodes Adjacent to Each Other.
3. Colluding Malicious Nodes two Hops Away From Each Other.

4.2 Simulation Evaluation

OPNET Modeler was chosen as a simulation environment because it is one of the leading environments for network modeling and simulation.

It supports large number of built-in industry standard network protocols, devices, and applications. In addition, its programming library helps researchers to easily modify the network elements and measure their performance in the simulation environment. OPNET also provides rich data analysis features.

In the simulation implementation, malicious nodes do not comply with the protocol. For example, they do not verify the signatures on the packets they forward, nor do they add nodes to their tabu list or exclusion links or send negative ACKs. In addition, they selectively drop or modify packets they are asked to forward. The exception being that they do not drop or modify RREQ or RREP packets, since their adversarial effects are more pronounced when they are on as many routing paths as possible.

V. RSR PROTOCOL PERFORMANCE METRICS

We used the following metrics to evaluate the performance of our scheme.

1. Packet delivery ratio.
2. Number of data packets delivered.
3. Routing overhead (bytes).
4. Routing overhead (packets).
5. Average end-to-end latency of the data packets.

The results of the simulation for RSR is compared with that of DSR, which currently is perhaps is the most widely used MANET source routing protocol.

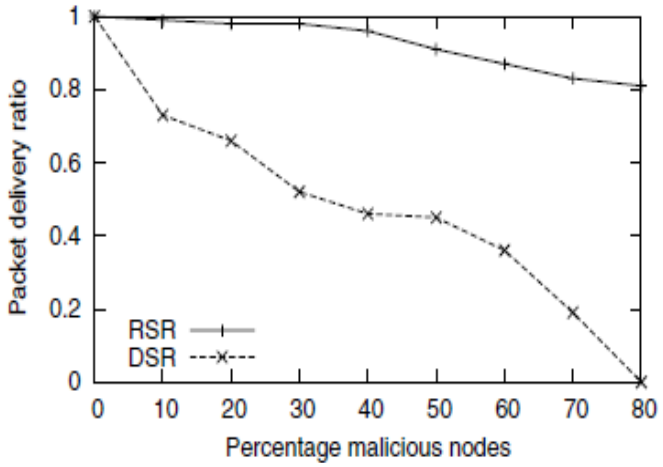


Fig 5.1: Packet Delivery Ratio

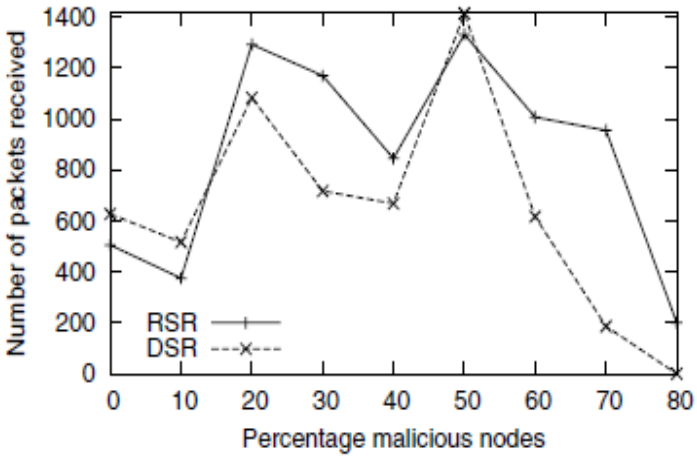


Fig 5.2: Number of data packets delivered

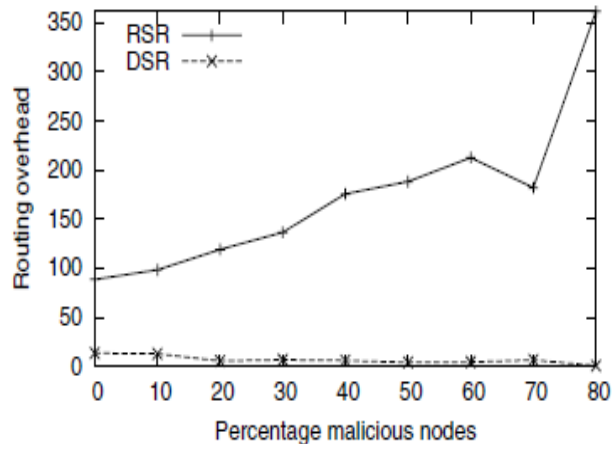


Fig 5.3: Routing overhead (bytes).

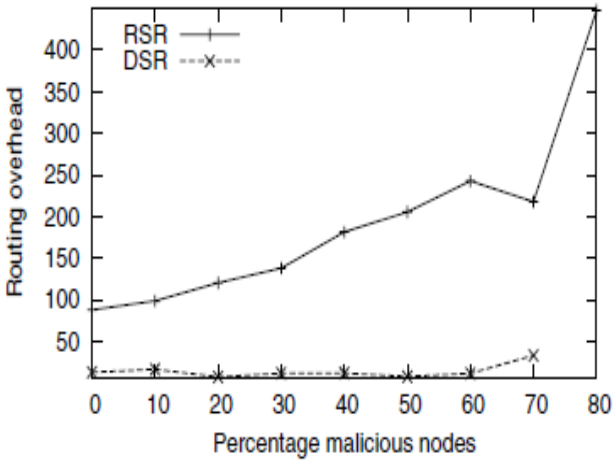


Fig 5.4: Routing overhead (packets).

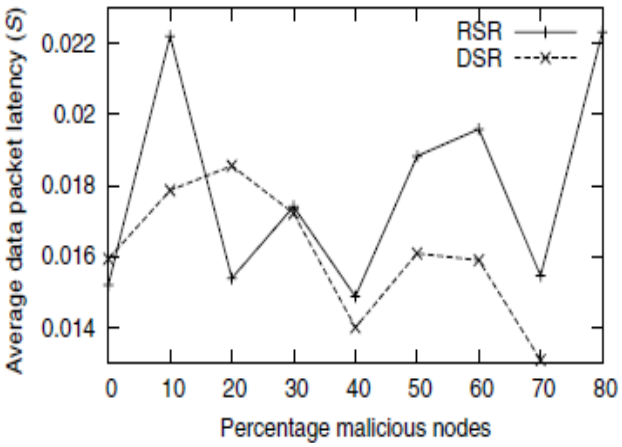


Fig 5.5: Average end-to-end latency

VI. CONCLUSION

We analyzed the wormhole attack which is one of the network layer attacks. This kind of attacker launches attacks by forming a tunnel between two or more malicious nodes and drops all the packets. We presented a robust, secure MANET on demand routing protocol that is capable of delivering packets to their destinations even in the presence of large

proportions of active malicious or selfish agents that selectively drop packets they agreed to forward. We named this protocol RSR. RSR introduced the concept of FR packets, which inform nodes along a path that they should expect specified data flow within a given time frame. The path elements can therefore be on the lookout for the given data flow, and in the event that they do not receive the traffic flow, they can transmit info to the source informing it that the data flow they expected did not arrive. Finally, we provided simulation results that attest to the proficiency of RSR being able to deliver packets to their destination even in the presence of large proportions of malicious or selfish entities. The performance analysis addresses that RSR method has reduced overhead and delay. These results, along with advantage that no additional requirement of hardware makes the proposed system more suitable for resource constrained wireless network applications.

REFERENCES

[1] R.H. Khokhar, Md. A.Ngadi,S.Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2008.

[2] M.A. Gorlatova, P.C. Mason, M. Wang, L. Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis". In *IEEE Military Communications Conference*, pp. 1-7, 2006.

[3] Khin Sandar Win. "Analysis of Detecting Wormhole Attack in Wireless Networks", *World Academy of Science, Engineering and Technology*, 48, pp. 422-428, 2008.

[4] Lee K. Thong. "Performance Analysis of Mobile Adhoc Network Routing Protocols". Thesis Paper submitted to the Department of Computer Science, Naval Post Graduate School, Monterey, CA, 2004.

[5] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," in *1st IEEE International Workshop on Sensor Network Protocols and Applications (WSNA)*, 2003, pp. 113-127.

[6] Imrich Chlamtac, Marco Conti, and Jennifer J.N. Liu, 2003 "Mobile Ad Hoc Networking: Imperatives and Challenges" *Ad Hoc Networks*, Volume 1, Issue 1. pp. 13-64

[7] Chiu, HS; Wong Lui, KS, 2006 "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks" *1st International Symposium on Wireless Pervasive Computing*.

[8] http://www.ietf.org/rfc/rfc2501.txt, date last viewed: 2009-12-21.

[9] OPNET Modeler 14.5 Documentation.

[10] Md. Anisur Rahman, Md. Shohidul Islam, Alex Talevski, ''Performance Measurement of Various Routing Protocols in Ad-hoc Network''.

[11] IEEE-SA Standards Board. IEEE Std 802.11b-1999, 1999.

[12] L. R. Ford Jr. and D. R Fulkerson. *Flows in Networks*. Princeton University Press, 1962.

[13] M. G. Zapata. Secure ad hoc on-demand distance vector routing. *ACM Mobile Comput. Commun. Rev.*, 6(3):106–107, 2002.

[14] M. G. Zapata. Secure ad hoc on-demand distance vector (soadv) routing. INTERNET-DRAFT draftguerrero-manet-saodv-00.txt, August 2001.

[15] C.-K. Toh. Associativity-based routing for ad-hoc mobile networks. *Wireless Personal Commun.*, 4(2):103–139, 1997.

[16] R. Bellman. On a routing problem. *Quart. Appl. Math.*, 16(1):87–90, 1958.

