Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks

Virendra Pal Singh
Dept. of Computer Science & Engineering
TIT&S, Bhopal

Aishwarya S. Anand Ukey
Dept. of Computer Science & Engineering
GGITM, Bhopal

Sweta Jain
Dept. of Computer Science & Engineering
MANIT, Bhopal

ABSTRACT

Wireless sensor network is a highly distributed network of small lightweight wireless sensor nodes, deployed in large numbers to monitor the environment or system. These sensor networks have limitations of system resources like battery power, radio range and processing capability. Low processing power and wireless connectivity make such networks vulnerable to various attacks like sink hole, black hole, Sybil attacks, selective forwarding, worm hole, hello flood etc. Among these hello flood attack is an important attack on the network layer, in which an adversary, which is not a legal node in the network, can flood hello request to any legitimate node using high transmission power and break the security of WSNs. The current solutions for this type of attack are mainly cryptographic, which suffer from heavy computational complexity. Hence these are less suitable in terms of memory and battery power. In this paper a method has been proposed to detect and prevent hello flood attack using signal strength of received Hello messages. Nodes have been classified as friend and stranger based on the signal strength of Hello messages sent by them. Nodes classified as stranger are further validated by sending a simple test packet; if the reply of test packet comes back in a predefined time then it is treated as valid otherwise it is treated as malicious. The algorithm is implemented in ns-2 by modifying the AODV-routing protocol. The performance of algorithm has been tested under different network scenarios. The simulation results show improved performance of the new algorithm in terms of number of packet delivery ratio as compare to AODV with hello flood attack.

Keywords

WSN, Keywords, Hello Flood

1. INTRODUCTION

Wireless sensor network is a collection of homogenous, self-organized nodes called sensor nodes. These nodes have the capabilities of sensing, processing and communication of data with each other wirelessly using radio frequency channel. The basic task of sensor networks is to sense the events, collect data and send it to their requested destination. They have many distinct features whisk make them different from the traditional wired and wireless distributed systems. Traditional wired or wireless networks have enough resources like unlimited power, memory, fixed network topologies, better communication range and high computational capabilities. These features make the traditional networks able to meet the communication demands [1] [2].

Due to limitations of system resources and wireless nature of communication, sensor networks are vulnerable to various kinds of network attacks. Hello flood attack is one of the most common attacks on routing protocols which require nodes to send Hello packets to advertise themselves to their neighbors. If a node receives such packet, it will assume that it is inside the radio range of the node that sent that packet. However, this assumption could be false because a laptop class adversary could easily send these packets with enough power to convince all the network nodes that the adversary is their neighbor. Consequently, nodes close to the adversary may try to use the adversary as a route to the base station, while nodes further away would send packets directly to the adversary. But the transmission power of those nodes is much less than that of the adversary, thus the packets would get lost, and that would create a state of confusion in the sensor network [9].

The rest of this paper is organized as follows. In Section 2, we present security attacks on wireless sensor networks. In Section 3, we describe about hello flood attack and various countermeasures of hello flood attack. In Section 4, we describe proposed approach and algorithm for hello flood detection and prevention. In Section 5 we present simulation parameters used in simulating the proposed approach. In section 6, we describe results analysis. Finally in section 7, we present our concluding remarks and future work.

2. SECURITY ATTACKS ON WIRELESS SENSOR NETWORKS

The wireless nature of the WSN and its resources limitations make them vulnerable to several types of attacks. Such attacks can be carried out in a variety of ways, common types of attacks are the denial or service attacks (DoS), traffic analysis attacks, eavesdropping, physical attacks, and others [9][10].

Most attacks on network layer protocols fall into one of the following categories:

- Spoofed, Altered, or Replayed Routing Information

By spoofing, altering, or replaying routing information, the adversaries could potentially create routing loops, attract or repel network traffic, lengthen or shorten routes, generate fake error messages, partition the network, increase node to node latency [9].

- Selective Forwarding

In a selective forwarding attack, malicious nodes could prevent forwarding certain messages or even discard them; consequently, these messages would not propagate through the network. [10].

- Sinkhole Attacks

In a sinkhole attack, the goal of the adversary is to attract all the traffic to a certain area or the network through a compromised node, creating a sinkhole.

- Sybil Attacks

In a Sybil attack a node presents multiple identities to the rest of the nodes. Sybil attacks are a threat to geographical routing protocols, since they require the exchange of coordinates for efficient packet routing. Ideally, a node only sends a set of coordinates, but under a Sybil attack, an adversary could pretend to be in many places at once.

- Wormhole Attacks

In a wormhole attack an adversary builds a virtual tunnel through a low latency link that takes the messages from one part of the network and forwards them to another.

- Hello Flood Attacks

Some protocols require nodes to send HELLO packets to advertise themselves to their neighbors. If a node receives such packet, it would assume that it is inside the RF range of the node that sent that packet. However, this assumption could be false because a laptop class adversary could easily send these packets with enough power to convince all the network nodes that the adversary is their neighbor. But the transmission power of those nodes is much less that the adversary's, thus the packets would get lost, and that would create a state of confusion in the sensor network [9].

3. HELLO FLOOD ATTACK DESCRIPTION

Hello flood attack is an attack on the network layer [5][9]. Many routing protocols require nodes to broadcast Hello packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within normal radio range of the sender. This assumption may sometimes be false; a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is it neighbors. For example, an adversary advertising a very high quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion. Thus the network is left in a state of confusion (as shown in figure 1). A node realizing the link to the adversary, which is false, could be left with few options: all its neighbors might be attempting to forward packets to the adversary as well. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are also subject to this attack [9].

An adversary does not necessarily need to be able to construct legitimate traffic in order to use the HELLO flood attack. It can simply re-broadcast overhead packets with enough power to be received by every node in the network. HELLO floods can also be thought of as one-way, broadcast wormholes.

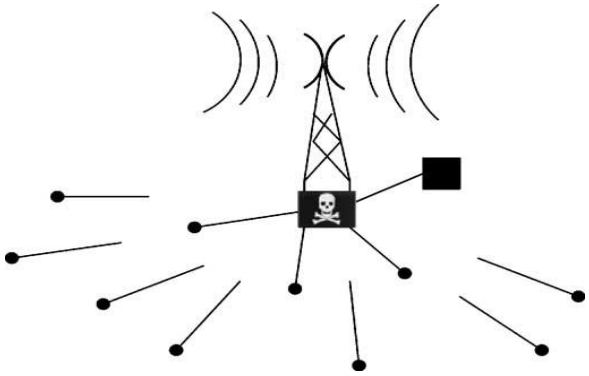

Figure 1 A laptop-class adversary that can retransmit a hello message and other routing information with enough power to be received by the entire network nodes. They are out of normal radio range from the adversary but they have chosen as their neighbor [9].

3.1 HELLO FLOOD ATTACK COUNTERMEASURES

Many techniques have been proposed in the past by different researchers to detect and prevent hello flood in WSN. Brief descriptions of these are given below.

3.1.1 In [9] authors suggest that hello flood attack can be prevented using "identity verification protocol". This protocol verifies the bi-directionality of a link with encrypted echo-back mechanism before taking meaningful action based on a message received over that link; this defense gets less effective when an attacker has a highly sensitive receiver as well as a powerful transmitter. If an attacker compromises a node before the feedback message, it can block all its downstream nodes by simply dropping feedback messages. And thus, such an attacker can easily create a wormhole to every node within range of its transmitter/receiver. Since the links between these nodes and attacker are bidirectional, the above approach will unlikely being able to locally detect or prevent Hello flood.

3.1.2 To defend against hello flood attack, each request (REQ) message forwarded by a node is encrypted with a key. In tree protocol when two sensor nodes share some common secrets, the new encryption key is generated on-the-fly (during communication). In this way, a node reachable neighbor can decrypt and verify the RREQ message while the attacker will not know the key and will be prevented from launching the attack. We show that the new key combined with the echo-back mechanism can protect this attack. [10]

Each node locally broadcasts an echo message to its neighbor with format:

s_1: ECHO||Enew-key (IDs_1||nonce)

Where, ECHO is the message type, ID is the ID of the sensor node s_1, nonce is the random number. If a node, say, s_2 receives this message; it sends echo reply with format:

$S_2 \rightarrow s_1$: ECHOBACK||Enew-key (IDs_2||nonce).

When node s_1 receives this message, it records node s_2 as its verified neighbor. If an attacker obtains the shared secrets after a node has received its new encrypted key, it cannot know the new pair wise key. Computing the pair wise key is more robust and secure in multiple tree protocol as we have

described earlier, where we have shown that the probability of compromise of a secret is very low. However, if an attacker obtains the new key, it can initiate echo-back many times by sending several echo messages. The attacker can generate false identities and can initiate Sybil attack, adding new nodes with false identities. To prevent such attacks, node should destroy its new key from memory after a certain time that is long enough to set up pair wise keys with all its neighbors. Again, during communication, it can calculate new key from the secrets they share.

3.1.3 The approach in [11] , considering minimal energy resources of sensor nodes used probabilistic Approach which forces few randomly selected nodes to report base station about hello request which can analyze the request authenticity. The author assumed identical sensors sensitivities where coverage is depend only on geometrical distances from sensors and also assumed a centralized control server where nodes are connected with each other in peer-to peer fashion which leads to connectivity with base station.

3.1.4 A mechanism [12] based on signal strength and geographical information for detecting malicious nodes staging HELLO flood and wormhole attacks is presented. The idea is to compare the signal strength of a reception with its expected value, calculated using geographical information and the pre-defined transceiver specification. A protocol for disseminating information about detection of malicious nodes is also proposed. The detection rate of the solution depends on different parameters. In this proposed scheme, all transmissions in the network are subject to scrutiny: all nodes monitor all transmissions they hear. For each transmission a node hears, it compares the expected and the actual signal strengths of the received signal, independently of whether it is the intended recipient of the transmission. When the difference between both is greater than a given threshold, the message is regarded as suspicious.

Each node also keeps a local table containing the “reputation” of other nodes in the system. Each entry contains the node id, the number of suspicious votes, and the number of unsuspicious votes. After checking the suspiciousness of a received message, the node updates its table accordingly: if the message is suspicious, it increases the message originator’s suspicious count by one; otherwise, the unsuspicious count is increased. Note that the message’s originator can be determined, given that its id is included in the message. If the message is suspicious, the node takes a further action: it disseminates this information among its neighbors.

3.1.5 In [13] a security solution framework is proposed tailored to the base station for its defending against DoS attack. After initial DoS detection and analysis prerequisite, base station challenges clients with cryptography puzzles to protect it. Compared with traditional puzzle schemes, they introduce the novel reputation based client puzzles, which applies a dynamic policy to adjust the puzzle difficulty for each node in terms of node’s reputation value, so that the punishment for malicious nodes becomes more and more pressing without introducing extra unnecessary burden to most normal nodes.

4. PROPOSED APPROACH

A node broadcasts a hello message, to indicate its presence. On receiving a hello message, each node updates its neighbor table, to indicate route towards the base station node. This might not be always true because in some cases a power full malicious node broadcasts high power hello message to indicate its existence. Legitimate nodes start considering this malicious node as their neighbors. This creates state of confusion in whole network and results in message loss or link failure.

A signal strength and time threshold based AODV-HFDP (Ad-hoc On demand Distance Routing with Hello flood Detection cum Prevention) is proposed for detection of node that generates hello flood attack. It is assumed that signal strength of all nodes is same in a given radio range. Each node checks the signal strength of the received hello request with respect to its radio range strength, if it is found same then node is classified as friend if not then stranger. Initially signal strength is calculated as two ray propagation model [14].

$P_r= (P_t*G_t*G_r*H_t^2*H_r^2)/(d^4*$ ……………………………..…(1)

In eq. 1 P_r is received signal power (in watts). P_t is transmission power (in watts), G_t is the transmission antenna gain , G_r is the receiver antenna gain, H_t is the transmitter antenna height(in meter) and H_r is the receiving antenna height(in mete), d is the distance between transmitter and receiver (in meter), and L is the system loss(a constant). A signal is only detected by a receiving node if the received signal power P_r is equal or greater than the received signal power threshold P_{thres}.

When any laptop class attacker sends hello message request to a legitimate node in a fixed radio range then node checks its hello message signal strength, if it is same then requesting node is a legal node in network; if it differs, it categorizes the sender node as stranger.

Signal strength = Fixed signal strength in radio range=friend

Signal strength > Fixed signal strength in radio range=stranger

If hello message signal strength is approximately same but not equal to fixed signal strength then it may be a stranger or friend. To distinguish between a friend and a stranger a technique based on simple test packet is applied. The test packet is like a probe message. The Hello message receiving node sends simple test packet to hello sending node, if the reply comes in allotted time threshold then hello sending node is considered as a friend, if not then it is classified as a stranger. After declaring the node as malicious, the information of hello sending node is deleted from the routing table and this information is broadcast throughout the network. All nodes in the network delete malicious node information from routing table.

Assumptions

Some primary assumptions considered while simulation are:

- Communication is within fixed radio range and all the communication links are bi-directional
- All sensor nodes in a fixed radio range have same transmitting and receiving signal strength.

- All sensor nodes are homogeneous (same hardware and software, battery power etc.).
- Every sensor node knows the fixed signal strength used in its communication range.
- A time threshold is used, which denotes the time of reply of the test packet.

4.1 ALGORITHM AODV-HFDP

In route establishment process a node first sends hello message to all neighbors to make them aware of its existence. If a node receives a hello message from a node it first checks the signal strength of hello message. If hello message signal strength is same as defined signal strength in radio range then hello receiving node accept hello message and classifies the sender as friend and related routing information is included in routing table. If hello message signal strength differs from radio range signal strength then hello sending node is classified as stranger. Stranger validity is verified by sending a simple test packet to the stranger node.

If the reply of test packet comes in predefined time threshold (two times of propagation delay) then stranger node is a friend node and includes node information in routing table. If the test packet reply does not come in the specified time threshold then stranger node is declares as a malicious stranger and the node deletes all the information related to malicious stranger.

In future, if a malicious node again sends hello message to neighboring nodes then neighboring nodes reject that request.

Algorithm

1: If A node receives hello request from a node S **then**

2: if Signal strength of S= fixed signal strength in radio range

3: then node s is classified as a friend

4: Node accepts hello request and perform function

5: Else

6: if Signal strength of S ≈ fixed signal strength in radio range **then**

7: Nodes sends test packet to node S

8: If reply of test packet comes in fixed time threshold **then**

9: Node is classified as friend and accepts the request include information in routing table

10: Else Signal strength of S> fixed signal strength in radio range

11: Node S is classified as Malicious and rejects the request.

End

5. SIMULATION PARAMETER

In order to implement the efficiency and effectiveness the new algorithm AODV [19] routing protocol has been modified. NS-2 network simulator [7][15][17] has been used for simulation purpose. A square area of 1000m × 1000m is considered for simulation experiments. The network topology consists of 100 stationary nodes. Initially, the nodes are randomly placed in fixed position. Out of 100 nodes maximum of five nodes may have high transmission, receiving and carrier sensing power, one node is a base station (Resource full node). Simulation time for each test run is taken to be 100 seconds. We have used Constant Bit Rate (CBR) has been used to generate UDP packets. Data rate used 512 kbps.

6. RESULT ANALYSIS

The performance of the algorithm is studied through series of simulation test in wireless sensor network with different number of malicious nodes. For comparison purpose AODV-HFDP has been compared with AODV-HF (Ad-hoc on demand Distance Routing with Hello flood Attack).

The performance is evaluated in terms of different parameters: Packet Delivery Ratio, Number of packets dropped, Number of packets sent and Number of packets received under different scenarios. The final results are obtained by taking average of six experimental runs.

- When no malicious node is present in both routing protocol in the network.
- When one malicious node is present in both routing protocol in the network.
- When two malicious nodes are present in both routing protocol in the network.
- When three malicious nodes are present in both routing protocol in the network.
- When four malicious nodes are present in both routing protocol in the network.
- When five malicious nodes are present in both routing protocol in the network.

6.1 TOTAL PACKET RECEIVED

Figure 2 shows comparison of AODV-HFDP and AODV-HF in terms of number of packets received with varying number of malicious nodes.

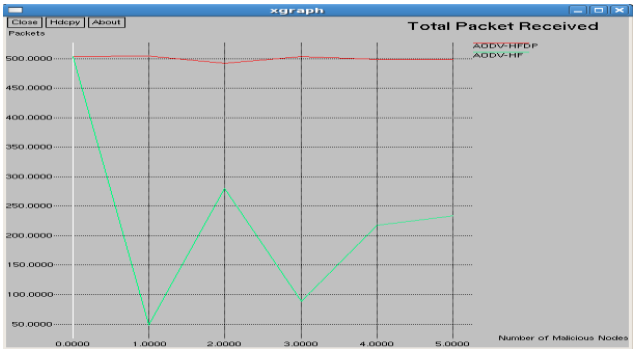

Figure 2 Number of malicious nodes vs. Packets

From figure 6.1 it can be observed that at point 2 on x-axis when there were two malicious nodes in the networks then the total packet received in AODV-HFDP are greater than AODV-HF. The reason of this increase in number of received packets is due to malicious node position in the network; i.e. one of the malicious nodes did not lie in the path between any source and destination.

6.2 TOTAL PACKET DROPPED

Figure 3 shows that the total packet dropped in both AODV-HFDP and AODV-HF. It is clear from the graph that the total packet dropped is much higher in AODV-HF as compared to AODV-HFDP for all the scenarios. In AODV-HF case, as the number of malicious nodes increases number of dropped packet also increases. Packets dropped increases abruptly because of the position of malicious which is near to receiving nodes. If malicious node and receiving nodes are very close to each other, than finding secure alternative paths becomes difficult and hence packet drop increases.

In AODV-HFDP all malicious nodes are detected and isolated hence packet drop rate remains constant to a small value.

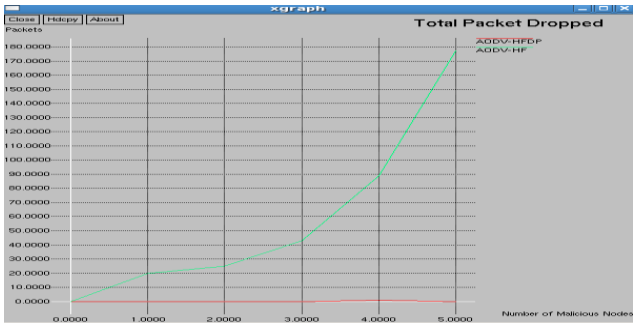

Figure 3 Number of malicious nodes vs. Packets

6.3 PACKET DELIVERY RATIO

In simulation time 100 seconds, measure the Packet Delivery Ratio in both AODV-HFDP and AODV-HF protocols with increasing malicious nodes from 1 to 5.

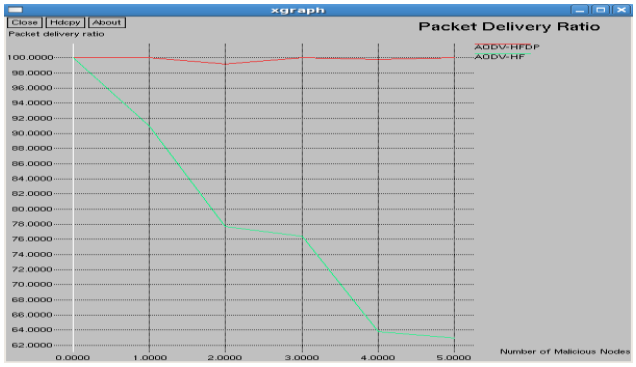

Figure 4 Number of malicious nodes vs. Delivery Ratio

Figure 4 depicts the variation of Packet Delivery Ratio in both AODV-HFDP and AODV-HF protocols. From the graph it is visible that the Packet Delivery Ratio is higher in AODV-HFDP compare to AODV-HF for all the network scenarios. In AODV-HF case, packet delivery ratio decreases with increasing number of malicious nodes. At point 1, one malicious node is present and hence the packet delivery ratio decreases suddenly in AODV-HF as malicious node drops the data packets. But packet delivery ratio is constant in AODV-HFDP case due to detection and isolation of malicious node instantly. In AODV-HFDP all malicious nodes are detected and isolated hence the packet delivery ratio remains almost same for all network scenarios.

From the above analysis it can be concluded that AODV-HFDP gives better performance even when the network is under hello flood attack. However in some cases AODV-HFDP performance degrades due to misclassification of nodes. Such misclassification occurs due to use of stringent threshold values of signal strength and time of reply of test packet which are used for classifying nodes as stranger or friend.

In ns-2, all simulation experiments were carried out with 100 mobile nodes moving in a 1000×1000 m. Transmission range of each mobile node is 250 m. IEEE 802.11 MAC layer was used. A random waypoint mobility model is chosen with maximum speed of 2 m/sec with pause time of 0 second. CBR transfer is used for the communication between pairs of nodes. For each CBR pairs, source and destination are chosen randomly. Each simulation lasts for 200 seconds. Experimental threshold value for misbehavior counter (allowable misbehavior per node) and time to receive acknowledgement packet (i.e. Ack-1 and Ack-2) is set to 5 and 10 respectively.

7. CONCLUSIONS

Security plays a crucial role in wireless sensor networks as they are prone to various network threat and intrusion. A new security framework for hello flood detection proven that this requires less computational power, hence is suitable for sensor networks. The new algorithm is implemented in ns-2 by modifying AODV [19] source code. Hello flood attack is generated by making selected malicious nodes send hello message using high transmission power as compared to regular nodes.

The performance of the new algorithm has been compared with AODV-HF that is AODV under hello flood attack. The simulation results show that the new technique is effective in improving the performance of the network. It results in higher packet delivery ratio as compare to AODV-HF as it is successful in isolating the malicious node.

In future more comprehensive research is needed to measure the current efficiency of algorithm, in terms of resources, so that improvement of its future version is possible.

8. ACKNOWLEDGEMENT

Virendra Pal Singh received Bachelor degree in Technology from Uttar Pradesh Technical University, Lucknow, India, in 2005 and Master Degree in Technology from Maulana Azad National Institute of Technology, Bhopal, India, in 2010. He is working as Assistant Professor in the dept. of Computer Sci. & Engg. at Technocrats Institute of Technology, Bhopal, India. His research interest includes ad hoc and sensor networks, information security and data warehousing.

Aishwarya S. Anand Ukey received Bachelor degree in Technology from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, in 2008 and Master Degree in Technology from Maulana Azad National Institute of Technology, Bhopal, India, in 2010. He is working as Assistant professor in the Dept. of Computer Sci. & Engg. at Gyan Ganga Institute of Technology and Management, Bhopal, India. His research interest includes wireless & ad hoc networks, information security and distributed systems.

Sweta Jain received Bachelor and Master degree in Technology from Maulana Azad National Institute of Technology, Bhopal, India. Presently she is pursuing PhD from the same institute. She is working as Assistant Professor in the dept. of Computer Sci. & Engg. at Maulana Azad National Institute of Technology, Bhopal, India. Her research

interest includes Mobile ad hoc network, specifically security issues in MANETs.

9. REFERENCES

[1] F.L. Lewis, "Wireless Sensor Networks," in *Smart Environments: Technologies, Protocols, Applications*, ed. D.J. Cook and S.K. Das, Wiley, New York, 2004.

[2] M. Ilyas and I. Magoub., *Compact Wireless and Wired Sensing System*, CRC Press, 2005.

[3] Md. Abdur Rahman, Abdulmotaleb, "Wireless Sensor Network Transport Layer: State of the Art," Lecture Notes in Electrical Engineering,Vol. 21, Part III, pp. 221-245, Springer Science plus Business Media-2008.

[4] A.Khetrapal, "Routing Techniques for Mobile Ad Hoc Networks Classification and Qualitative/ Quantitative Analysis," Department of Computer Engineering, Delhi College of Engineering University AK-ACWN, 2006

[5] G. Acs and L. Buttyabv., "A Taxonomy of Routing Protocols for Wireless Sensor Networks," BUTE Telecommunication Department, Vol. LXII, pp 32-40, Jan 2007.

[6] J. Fraden., *A Hand Book of Modern Sensor: Physic, Design, and Application*, Springer Science Plus Business Media, 2004.

[7] http://en.wikipedia.org/wiki/Network_simulator. [Accessed-July2010]

[8] I.Akyildiz, W. Su, Y. Sankara subramaniam, "A Survey on Sensor Networks," IEEE Communications Vol. 40 Issue 8, Aug 2002, pp.102-114.

[9] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier Ad Hoc Networks 1 pp 293–315, 2003.

[10] A Hamid, S Hong, "Defense Against Lap-top Class Attacker in Wireless Sensor Network," ICACT, Feb 2006, pp-314-318.

[11] Dr. Moh. Osama K., "Hello Flood Counter Measure for Wireless Sensor Network," International Journal of Computer Science and Security, vol. 2 issue 3, 2007, pp-57-64.

[12] Waldir Ribeiro Pires Junior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, "Malicious Node Detection in Wireless Sensor Networks," 18th International Parallel and Distributed Processing Symposium(IPDPS'04) Vol. 1, pp. 24, 2004

[13] Zhen Cao, Xia Zhou, Maoxing Xu, Zhong Chen, Jianbin Hu, Liyong Tang, "Enhancing Base Station Security against DoS Attacks in Wireless Sensor Networks," International Conference on Wireless Communication, Networking and Mobile Computing, Sept-2007, pp. 1-4.

[14] T.S.Rappaport, *Wireless Communication: Principles and Practice*, Prentice hall 2nd edition-2001.

[15] Teerawat Issariyakul, Ekram Hossain, *Introduction to Network Simulator NS2*, Springer Science plus Business Media, 2008.

[16] Mohammad Sayad Haghighi, Kamal Mohamedpour, "Securing Wireless Sensor Networks against Broadcast Attacks," International Symposium on Telecommunications, Aug-2008 , pp. 49-54.

[17] http://www.isi.edu/nsnam/ns/ [Accessed- July 2010]

[18] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile comp. Sys. And Apps., Feb 1999, pp. 90-100.

[19] Luis E. Palafox, J. Antonio, "Security in Wireless Sensor Networks," IGI Global publishing, Chapter 34, pp. 547-564, 2008.