International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.05,Issue.15
June-2016,
Pages:2941-2946

www.ijsetr.com

A Survey on Different Attacks in Wireless Sensor Ad-Hoc Network

SACHIN GUPTA[1], HARSHA CHAWLA[2]
[1]PG Scholar, Dept of CSE, NGF College of Engineering & Technology, Palwal, Haryana, India.
[2]Assistant Professor, Dept of CSE, NGF College of Engineering & Technology, Palwal, Haryana, India.

Abstract: Mobile Ad-hoc Network (MANET) is a technology used to create a wireless network without pre existing infrastructure. In MANET nodes be free to move dynamically form a network to other network without any centralized administration. Despite making sensor networks possible, the every wireless nature of the sensors presents a number of security threats when deployed for certain applications like surveillance, military etc. Security is main concern in wireless network due to the wireless natures of the sensor networks and constrained nature of the resources on the wireless sensor nodes, which means that security architectures is used for traditional wireless networks are not viable. So in this paper we will discuss about different types of attacks and its securities threats that took place in Ad hoc network.

Keywords: Wireless Sensor Networks (WSN), Denial of Service (DoS), Vampire Attack, Wormhole Attack, Protocol, Attack, Countermeasure.

I. INTRODUCTION

Wireless sensor networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, Wireless sensor networks do not rely on any fixed infrastructure. Wireless sensor network is a collection of a numbers of wireless mobile nodes that self-configure to construct a network without the need for any established infrastructure or backbone. Wireless sensor networks use mobile nodes to enable communication outside wireless transmission range. However there are different attacks and threats in the wireless sensor network. These attacks can be Denial of Service attacks or Routing attacks. Due to these attacks wireless sensors network are badly affected. The unique property of WSNs increases flexibility and reduces user involvement in operational tasks such as in battlefields. Achieving security in resource constrained WSNs is a challenging research task. Secrecy, data integrity, authentication, establishment of key, availabilities, privacies, secures routing are the main challenges in the Wireless sensor network. The best example is the node capture attack, where an attacker physically captures a sensor node and extracts all of its stored information and makes it useful for himself so that he can easily use those data to modify the content. In this paper we will discuss about the different attacks which took place in ad hoc network. Also discuss about countermeasures of the different attacks.

II. REVIEW OF LITERATURE

From the last few years, researchers have been actively explored many mechanisms to ensure the security of control and traffic of data in wireless networks. These mechanisms can be broadly categorized into the following class authentication and services of integrity, and protocols that rely on path diversities, protocols that use specialized hardware, protocol that requires explicit acknowledgment or use statistical methods and protocol that overhears neighbour communications. DoS attacks and defences in including using one-way hash chains to limit the number of packets sent by a given node, limiting rate on which node can transmits packets. While this strategy may protect against traditional DoS, where malefactors overwhelms honest nodes with large amount of data, it does not protect against “intelligent” adversaries who use small number of packets or do not originate packets at all. Another attack that can be thought of as path-based wormhole attack. It allows two non neighboring malicious nodes with either a physical or virtual private connections to emulate a neighbor relationship, even in a secure routing systems. Moreover, many of these schemes are more expensive for the resource-constrained networks due to the data redundancy.

III. ROUTING PROTOCOLS IN MANET

The routing protocols are broadly classified into two categories such as Proactive and Reactive.

A. Proactive Routing Protocols

In the Proactive Routing protocol each node in the network has routing table to broadcast the data packets and try to establish connection with other nodes in network. In MANETs all node records information about presented destinations, number of hops that are required to arrive at each destination in the routing table. Each station broadcasts and modifies its routing table time to time to retain stability. How many hops that are required to arrive at particular node and accessible stations are results of broadcasting of packets between nodes? Data broadcast by node contains its new sequence number and for each new route node will contain the following information:

- How many hops that are required to arrive that particular destination node?
- Generation of new sequence number marked by the destination
- The destination address.

From the study we can conclude the proactive protocols are useful for less number of nodes in networks, they are needed to update nodes entries for each and every node in the routing table of every node. It results is more routing overhead problem due to consumption of more bandwidth.

B. Reactive Routing Protocol

Reactive protocol has lower overhead because routes are discovered on the demand and it employs flooding concept. The reactive protocol searches routes on-demand basis and set the link in order to send and receive packets from source to destination node. Route discovery process is used on the demand of routing by flooding RREQ message throughout the network. DSR, AODV are examples of reactive routing protocols. Due to their simplicity, and inherent support for data on demand, they are predominant choice in the wireless sensor networks. However, uses of sensor networks differ from MANET. For example, environmental monitoring this involves stationary sensors collecting readings over time from fixed points in space contrast to hand-held devices of mobile users.

IV. APPRAISE ON ATTACKS IN WSN

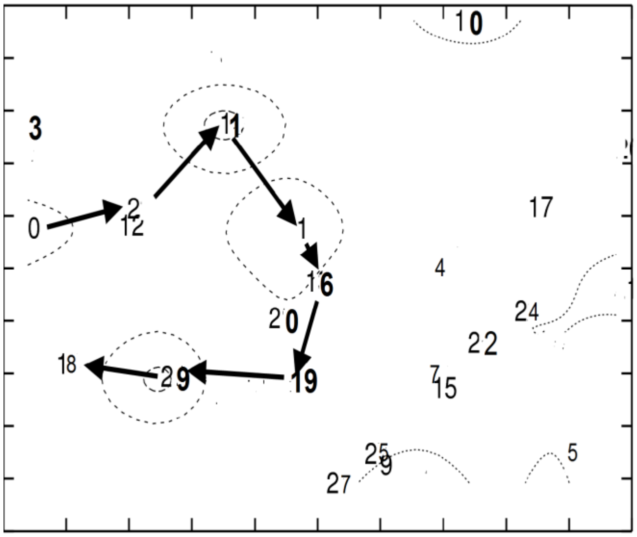
Computer viruses, bugs and attacks have a history as long as computer networking itself. The first bug was identified in 1945. In 1960 the first threat to network security was identified: a white-collar crime performed by a programmer for the financial division of a large corporation. In 1983 Fred Cohen coined the term computer virus. One of the first PC viruses was created in 1986, called “The Brain”. The history about computer and network security has been well documented .Accordingly with improvements in the security of networks and computers; we are now facing increasingly sophisticated attacks and threats. In this section we will describe and discuss attacks and threats those are related to WSN. The most of attacks are similar to those attacks applied to the traditional networks. In this section we will describe attacks which are noxious and can potentially lead to considerable damage of the network.

A. Vampire Attack

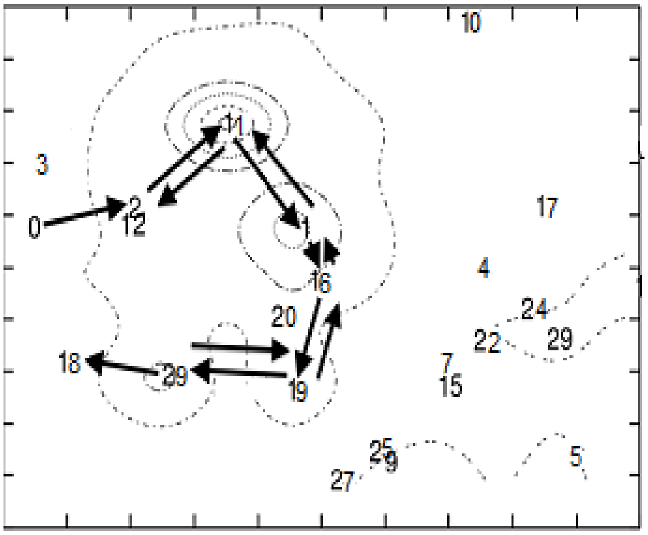
The most of permanent denial of service attack is to entirely deplete nodes battery [1]. This is an instance of a resource decreasing attack, with battery power as the resource of interest. Vampire Attacks that drain the life from networks nodes they never disrupt availability and rather work over time to entirely disable a network. It is not protocol-specific. Vampire attack is a composition and transmission of a message that causes more energy may be consumed by the network, if an honest node transmits message of similar size to the destination using different packet headers. Author classifies this attack as follows.

B. Carousel Attack

In this attack, an adversary sends a packet with a route details as a series of loops, the same node appears in the route many times. This mechanism may be used to increase the route length beyond the number of nodes in the network.



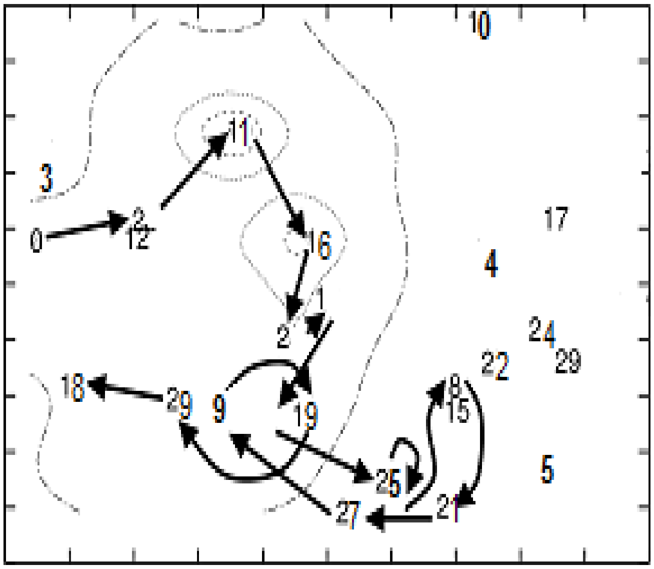
(a) Honest Scenario: node 0 send a single message to the node



(b) Carousel attack (malicious node 0): the nodes traversed by the packet are the same as in (a), but the loop over all forwarding nodes roughly triples the route length (the packet traverses the loop more than once). Note the drastically increased energy consumption among the forwarding nodes.

C. Stretch Attack

In stretch attack is a packet traverses to every node in the network, due to this causes energy usages increase of factor .O(min(N,λ)), where N represents number of nodes in the network and λ represents the maximum path length allowed.



(c) Stretch attack the route diverts from the optimal path between source and destination, roughly doubling of length.
Fig.1.

(b) the region of increased energy consumption is larger. The energy consumption is larger than carousel attack and spread more over network nodes.

(c) Stretch attack (malicious node 0): the route diverts from the optimal path between source nodes to destination node, roughly doubling in length. Overall energy consumption is greater than carousel attack, and spread more evenly over more network nodes.

Measure the Strength of This Attack: Strength of this attack can be defined as ratio between power utilization and malicious nodes present to energy usage with only honest nodes when the number of packets and size of packets sent are remains constant. Safety from Vampire attacks implies that this ratio is 1. These types of attacks contains new open problem for researchers.

Countermeasure for Vampire Attacks: Vampire attacks, which are devastating, it is difficult to detect, and are easy to carry out using as few as one malicious insider sending only the protocol compliant message. In worst case single Vampire can increases network-wide energy usage by factor O(N), where N in represents number of nodes in the network. A method to mitigate these types of attacks, including a newest proof of concept protocol that probably bounds the damage caused by Vampires during the packet forwarding phase. By Parno, Luk, Gaustad, and Perrig can be modified to Vampire attacks during the packet transmission. The original version of the protocol designed for security, is vulnerable to Vampire attacks. PLGP consists of topology discovery phase and followed by a packet forwarding phase, with the former optionally repeated on fixed schedule to ensure topology information. Nodes discover their neighbours using local broadcast, and form expanding neighbourhoods", are stopping when the entire network is a single group. Throughout of this process and nodes build tree of neighbour and group membership used to address and routing.

D. Denial of Service Attacks

A Denial of Service (DoS) is a attack that attempts to prevent victim from others being able to use all or part of his/her network connection [2]. Denial of service attack extends to all layers of the protocol stack. They target all the services available or the authorized users access to a service provider. DoS attacks in MANETs may not only bring damage to the victim node, due to limited battery it may degrade the performance of the whole network and the network can be congested due to availability of limited bandwidth as compared to fixed networks [3]. In wireless sensor networks, several types of DoS attacks may be performed at different layers.

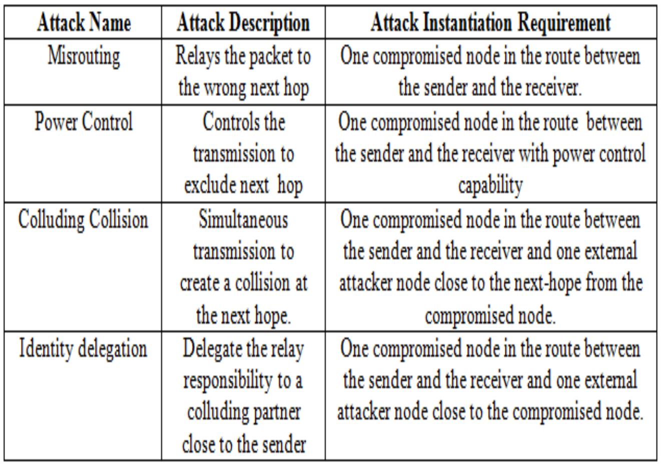
Countermeasure for DOS Attacks:

- Firewall and router filtering
- Firewall as semi-transparent Gateway:
- Firewall as a Relay:
- Ingress filtering:
- Egress filtering:

E. Stealthy Attack

In this attacker achieves the objective of disrupting the packets reaching to destination by malicious behaviour at an intermediate node. However, malicious nodes give impression to its neighbours participating in local network it has performed all the required action. This class of attacks is applicable to those packets that are, neither acknowledged end to end, nor hop by due to the constraint of bandwidth, energy, and much traffic in multi hop ad- hoc wireless networks is unacknowledged or only selective acknowledged.

TABLE I: Summary of the Stealthy Attacks



Attack Name	Attack Description	Attack Instantiation Requirement
Misrouting	Relays the packet to the wrong next hop	One compromised node in the route between the sender and the receiver.
Power Control	Controls the transmission to exclude next hop	One compromised node in the route between the sender and the receiver with power control capability
Colluding Collision	Simultaneous transmission to create a collision at the next hope.	One compromised node in the route between the sender and the receiver and one external attacker node close to the next-hope from the compromised node.
Identity delegation	Delegate the relay responsibility to a colluding partner close to the sender	One compromised node in the route between the sender and the receiver and one external attacker node close to the compromised node.

Countermeasure for Stealthy Attacks: A protocol called SADEC that can be detect and isolate stealthy packet dropping attack efficiently. SADEC presents two techniques those can be overlaid over baseline local monitoring: having the neighbours maintain additional information about the routing paths, and adding some checkable responsibility to each neighbour. Additionally, SADEC provides an innovative idea for better utilization of local monitoring by considerably increasing the number of nodes in a neighbourhood that can do monitoring.

F. Node Replication Attack

Node Replication attack [7] is the harmful attack against Wireless Sensor Networks (WSN) where one or more nodes illegitimately claim an identity in the network. Replication attack can be exceedingly harmful for important functions of the sensor network such as routing, replication attack where one or more nodes illegitimate claim is an identity of legitimate node and replicated in whole WSN network. Reason behind choosing such attack is that it can form the basis of several of attacks such as Sybil attack, routing attacks and link layer attacks also called as DoS attacks. The fundamental problem is the detection of node replication attacks in a wireless sensor network . A few centralized and distributed solutions have been proposed and discussed in section of related work. However, these types solutions are not satisfactory they are energy and memory demanding: It is a serious drawback of any protocol is that it must be used in resource constrained environment.

Countermeasure for Node Replication Attacks: There is a method such as Randomized and Trust based witness finding strategy used for replication of attack detection wireless sensor networks with trust factor. Resilient to malicious witness increase detection rate by avoiding malicious witness selection. Performances compared with the existing witness finding approach and how the malicious witness drop claim may without processing and how those malicious witnesses are avoided with trust based approach.

G. Wormhole Attack

Sender node sends a message to another node in the network that is known as receiver node [8]. Then the receiving node tries to send the same message to its neighbour nodes. The neighbouring nodes try to send this message to the originating node, since it is too far away so it never arrives. Wormhole attack is a significant threat to wireless sensor networks, because, this type of sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when all the sensors start to discover neighbouring information. Wormhole attacks are difficult to counter because all the routing information supplied by a node is difficult to verify.

Wormhole Attack Prevention: The mechanism of wormhole attack include, DAWWSEN, a proactive routing protocol based upon design of a hierarchical tree where root node is base station, and other sensor nodes are leaf nodes of the tree. The great advantage of this is, it doesn't need geographical information of the sensor nodes, and does not take the time stamp of packets as approach for the detecting a wormhole attack, which is very important for resources constrained natures of the sensor nodes.

Countermeasure for Wormhole Attacks: Wormhole attacks are the passive in nature; the algorithm uses a hop count technique for probe procedure, reconstructs the local maps in each node, and then uses a diameter feature for detecting abnormalities caused by wormholes. The main advantage of this algorithm is that it can provide the approximate locations of wormhole, which are useful to implement countermeasures.

H. Sybil Attack

In this attack, a single node will be appeared as a set of nodes and will send incorrect information to a node in the network. The incorrect information may be varieties of things [10], including position of nodes, strengths of the signal, making up nodes that do not exist. Authentication and encryption techniques can be prevented as outsider node to launch the Sybil attacks on sensor networks. However, an insider node cannot be prevented from participating in the networks, but that should be able to do so using the identities of the nodes has compromised. Public key cryptography can be prevented such as an insider attack, but it is too costly for using in the resource constrained sensor networks.

Countermeasure for Sybil Attacks:

- Radio resource testing which relays on the assumptions each physical device has only one radio.
- Pre distribution of random key which associates the identity of each node to the keys assigned to it and validates the keys to establish whether the node is really who it claims to be.
- Registration of the nodes is identified at a centralized base station.
- Position verification which makes all the assumption that the WSN topology is static.

I. Black Hole Attack

A Black hole attack is a kind of DOS attack where a malicious node can attracts all packets by falsely claiming a fresh route for destination and then absorbs without forwarding them to the detonation [15]. A black hole attack has two faces, in first face the malicious node exploit the Ad-hoc routing protocols as AODV to advertising itself as having a valid route to a destination node. In second phase attackers node drop the intercepted packets without forwarding them. The false route reply message from a malicious node contains the following parameters:

- Maximum destination sequence number − It makes the route up to date.
- Single hop-count – It makes a route with the shortest path.
- Life-long route – It informs a route will exist as long as the network.
- Destination IP addresses – It is address of the destination node copied from RREQ.
- Time-stamp – It is a amount of time the RREP was generated.

Countermeasure for Blackhole Attacks: An approach for better analysis and improve securities of AODV, that is the one of best routing protocols for MANET based on AODV Protocol. It is improved by deploying advanced DRI table with additional check bit. The Simulation on NS2 is carried out and the proposed schemes have produced results and demonstrate the effectiveness of the mechanism in detection and elimination of attacks and maximize performances of the networks by reducing packet dropping ratio in network.

J. Hello Flood Attack

Some routing protocols in WSN are required nodes to broadcast the hello messages to announce themselves to their neighbours [17]. A node which receives a such type message may be assumed that it is within a radio range of the sender however in some cases this assumption may be false; and sometime laptop-class attacker broadcasts routing or other information with large enough transmission power could be convinced every other node in the network that the attacker is its neighbour. For example an adversary advertises a very good quality route to base station could be caused a large number of nodes in the network that attempts to use such route. But those nodes which are sufficiently far away from the adversary would be sending the packets in the oblivion. Hence networks are left in a confusion state. The protocols depend upon localized information exchange between neighbour nodes for topology maintenance or flow controls are mainly affected by this type of attack.

Countermeasure for Hello Flood Attacks: The Multi-path multi-base station data forwarding technique is proposed in which a sensor node maintains number of different secrets information in the multiple trees. Sensor node can forward sensed data to the multiples routes by using these secret information. There are multiple base stations in the network have controls over the specific number of nodes and there are common means of communication among base stations. The base station has all secret information shared by all the sensor nodes, covered by sensor nodes, according to the key assignment protocol. Both, shared secret information and generated the new key information between two sensor nodes, the process of route setup requires much processing hence it is inefficient hello flood attack can also be counteracted by using protocol known such as identity verification. Purpose of this protocol is to verify the bi-directionality of a link with encrypted echo-back mechanism and before taking appropriate action based on a message received over that link.

V. CONCLUSION

All of the security threats serve one common purpose that is to compromise the integrity of the network they attack. Thus focus has not been on the WSNs security, but also with the various security threats arising and the importunacy of data confidentiality, security has become a complicated issue. Although some solutions have been proposed, and even there is no single solution to protect against every threats. In this paper we mainly focus on the security threats in WSN. Hence we conclude that the mechanism of defense presented just gives idea about the WSN security threats; the proper solution depends on the type of application deployed for WSN. There are many security mechanisms which are used in layer-by-layer basis as a security tool. Through this paper we have presented most common securities threats in various layers and their most probable solution.

VI. REFRENCES

[1] Eugene Y. Vasserman∗ and Nicholas Hopper"Vampire attacks:Draining life from wireless ad-hoc sensor networks", IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.2 YEAR 2013,pp 1-15

[2] Heena Ahuja, Er. Jyoti Gupta" Analysis of Malicious Data in Underwater Sensor Network", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 4, July-August 2012, pp.967-971

[3] David R. Raymond and Scott F. Midkiff,(2008) "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.

[4] A. D. Wood and J. A. Stankovic,(2002) "Denial of service in sensor networks",Computer, 35(10):54–62, 2002.

[5] Gajalakshmi J, Radhika," Detecting & Isolating Stealthy Packet Dropping Attack in Multihop Wireless ADHOC Network", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012

[6] Chris Karlof, Naveen Sastry, David Wagner, (2004)Tiny Secure link layer security architecture for wireless sensor networks, Proceedings of the 2nd international conference on Embedded networked sensor systems , Nov 03-05,2004,Baltimore,MD,USA.

[7] Mauro Conti , Roberto Di Pietri , Luigi V. Mancini , Alessandro Mei "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks (2007)

[8] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole attack In Wireless Sensor Network",Proceedings of the Second International Conference on Innovations in Information Technology (IIT"05).

[9] M. Zorzi and R. R. Rao, (2003) "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," IEEE Transactions on Mobile Computing, vol. 2, no. 4, pp. 337-348, 2003.

[10] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin "Highly-resilient, energy-efficient multipath routing in wireless sensor networks,"Mobil Computing and Communications Review, vol. 4, no. 5, October 2001.

[11] Hans Eberle, Arvinderpal Wander, Nils Gura, Sheueling Chang-Shantz, and Vipul Gupta, Architectural extensions for elliptic curve cryptography over GF(2m) on 8-bit microprocessors, ASAP, 2005.

[12] T. English, M. Keller, Ka Lok Man, E. Popovici, M. Schellekens, and W. Marnane, A low-power pairing-based cryptographic accelerator for embedded security applications, SOCC, 2009.

[13] Laura M. Feeney, An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks, Mobile Networks and Applications 6 (2001), no. 3.

[14] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, Strong authentication for RFID systems using the AES algorithm, CHES, 2004.

[15] Miss. Bhandare A. S, Dr.Mrs. Patil S.B "Study of Protocols (AODV, DSR)Of MANET(Mobile ad-hoc network)& Black hole attack in AODV", IOSR Journal of Electronics & Communication Engineering (IOSR-JECE) ISSN : 2278-2834, ISBN : 2278-8735, PP : 50-53

[16] Rodrigo Fonseca, Sylvia Ratnasamy, Jerry Zhao, Cheng T. Ee, David Culler, Scott Shenker, and Ion Stoica, Beacon vector routing: Scalable point-to-point routing in wireless sensornets, NSDI, 2005.

[17] Virendra Pal Singh, Sweta Jain and Jyoti Singhai "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.

[18] J . Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia and B. Bhargava, Lowcost attacks against packet delivery, localization and time synchronization services in underwater sensor networks, Proceedings of the Fourth ACM Workshop on Wireless Security, pp. 87{96, 2005.

[19] L. Lazos and R. Poovendran, SeRLoc: Robust localization for wireless sensor networks, ACM Transactions on Sensor Networks, vol. 1(1), pp. 73{100, 2005.

[20] D. Liu, P. Ning and W. Du, Attack-resistant location estimation in sensor networks, Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks, pp. 99{106, 2005.