ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

Attack and Counter Measurement of Worm Hole and False Data Injection in Wireless Sensor Networks: A Survey

Uma Narayanan[1], Arun Soman[2]

Department of Information Technology, Rajagiri School of Engineering and Technology, Rajagiri valley, Cochin, India[1,2]

Abstract: Advance in wireless networking, micro-fabricationand integration (for example, sensors and actuators manufactured using micro-electromechanical system technology, or MEMS), and embedded microprocessors have enabled a new generation of massive-scale sensor networks suitable for a range of commercial and military applications. Wireless sensor network are usually unattended, self-organizing, multi-hop network very open to anyone. Their biggest advantage is also one of their biggest disadvantages: Due to small size and unattended mode of operation anyone with the proper hardware and knowledge of the network topology and protocols can connect to the network and create different attack which will compromise the entire network. This paper discusses the modes of attack in wireless sensor network and the counter measurement of worm hole and false data injection.

Keywords: WSN; Malicious; Wormhole; Sybil; Sinkhole; Counter measures

I. INTRODUCTION

An attack is an event that diminishes or eliminates a network's capacity to perform its expected function and an adversary is a person or another entity that attempts to cause harm to the network by unauthorized access or denial of service. The attack is introduced with the help of malicious node or a compromised node[2] which can be of single malicious or two consecutive or more as shown in fig 1.

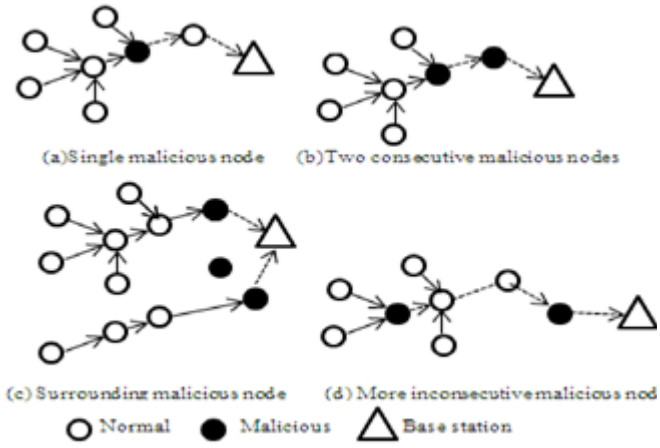

Fig 1: Deployment of malicious sensor node

There are different types of attack in wireless sensor network and they can be classified as routing attack and the attack on transit. The routing attack can be again divide as Selective forwarding, Sink hole attack, Sybil, Worm hole, Hello flood and Altered routing information. Attack on transit can be classified as Interruption, Interception, Modification and False data injection .Classification of attack is shown in fig 2.

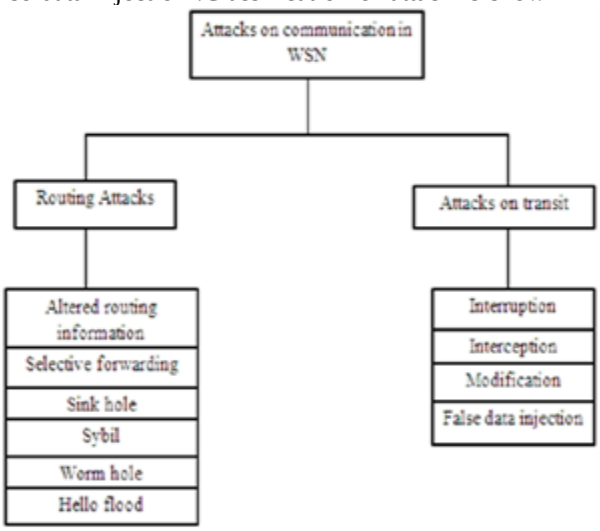

Fig 2: Classification of attacks on communication in WSN

II. ROUTING ATTACK

Wireless sensor networkconsist of sensor nodes in lager number perform distributed sensing task with help of wirelesslink usually deployed in unattended or hostile environment are more vulnerable to attack.

A. Selective Forwarding

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

The Selective Forwarding attack is a serious threat in wireless sensor networks, especially in monitor systems. Malicious sensor nodes work like normal sensor nodes but selectively drop sensitive packets in selective forwarding attack. The dropped packets may contain some crucial information; hence, the loss of some packets may destroy the entire networks.

B. Sink Hole Attack

Attracting traffic to a specific node in called sink hole attack. In this attack, the adversary‘s goal is to attract nearly all the traffic from a particular area through a compromised node. Sink hole attacks typically work by making a compromised node look attractive to surrounding nodes. How sink hole effect the network is shown in fig 3.

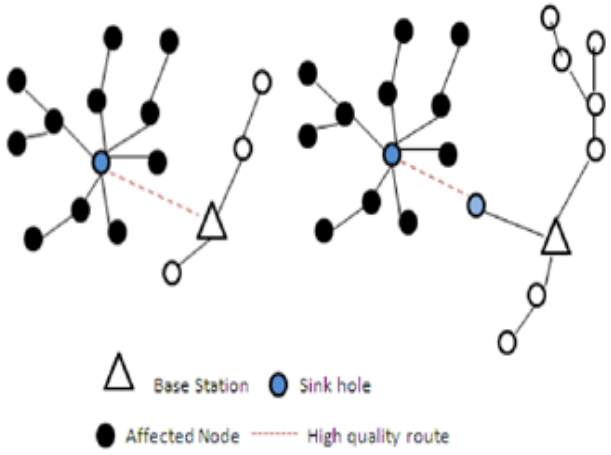

Fig 3: Sink Hole Attack

C. HELLO flood attacks

An attacker sendsor replays a routing protocol‘s HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbour. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbour and are ultimately spoofed by the attacker.

D. Altered Routing Information

Attack against the routing information exchanged between nodes. An adversary can alter or replay routing information.

E. Sybil Attacks

A single node duplicates itself and presented in the multiple locations. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network

F. Wormholes Attacks

In the wormhole attack, an attacker records packet (orbits) at one location in the network, tunnels them to another location, and retransmits them into the network.

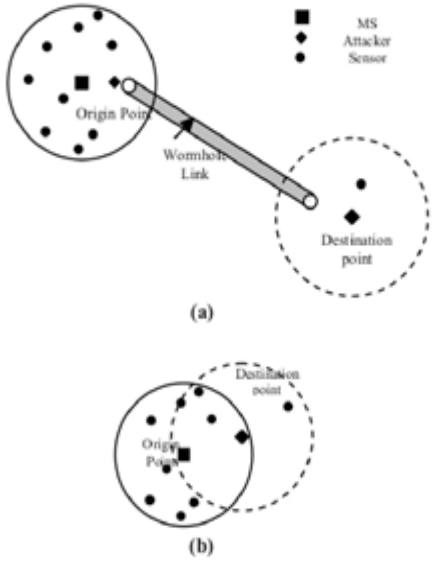

Fig 4: Example of worm hole attack

III. ATTACK ON TRANSIT

It is a type of attack which effects the data that is being send. Since sensed data is the inevitable part of sensor network, its compromise cannot be entertained. So we can consider this attack as one of the hot research area in the field of network security. Attack on transit can be broadly classified as follows.

A. Interruption

Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption and insertion of malicious code.

B. Interception

Interception is an attack on confidentiality. The sensornetwork can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

C. Modification

Modificationis an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with false data.

D. False data injection

Sensor nodes are not tamper resistant and can be easily compromised by an adversary. In this attack an adversary injects false data and compromises the trust worthiness of the information communicated. False sensing reports can be injected through compromised nodes. The fig 4 shows how false data can be injected to network.

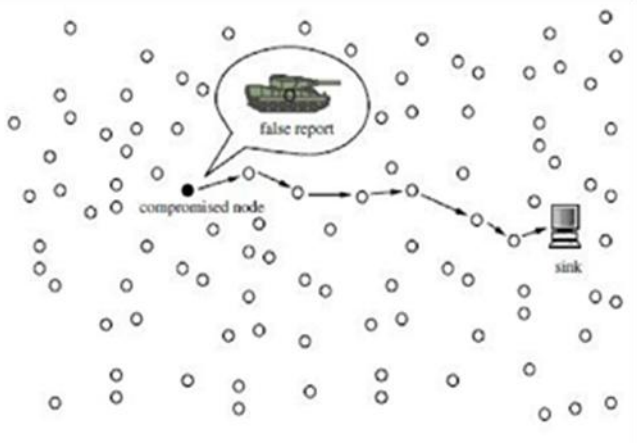

Fig 4: False Data Injection by compromised node

IV. COUNTER MEASURE

A. False Data Injection

Sensors are usually deployed in unattended or even hostile environments, and an adversary may capture or compromise sensor nodes. Node compromise occurs when an attacker gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network. Once this happens, the compromised nodes can easily inject false data reports of non-existent events. Even worse, when an adversary compromises more nodes and combines all the obtained secret keys, the adversary can freely forge the event reports which not only happenat the locations where the nodes are compromised, but also at arbitrary locations in the field. These fabricated reports not only produce false alarms, but also waste valuable network resources, such as energy and bandwidth, when delivering the falsified reports to the base station. Therefore, it is important to design an effective filtering scheme [8] to defend and minimize the impacts of false data injection attack. Some of the research works onbandwidth-efficient filtering of injected false data in wireless sensor networks have been appeared in the literature in [1], [3], [4], [5], [6], and [7].

In [3], Ye et al. propose a statistical en-routing filtering mechanism called SEF. SEF requires that each sensing reportable validated by multiple keyed message authenticated (MACs), each generated by a node that detects the same event. As the report being forwarded, each node along the way verifies the correctness of the MACs at earliest point. If the injected false data escapes the en-routing filtering and is delivered to the sink, the sink will further verify the correctness of each MAC carried in each report and reject false ones.

In [6], Ren et al. propose more efficient location-aware end-to-end data security design (LEDS) to provide end-to-end security guarantee including efficient en-routing false data filtering capability and high-level assurance on data availability. Because LEDS is a symmetric key based solution, to achieve en-routing filtering, it requires location-aware key management, where each node should share at least one authentication key with one node in its upstream/downstream report-*auth cell*.

In [7], Zhang et al. provide a public key based solution to the same problem. Especially, they propose the notion of location-based keys by binding private keys of individual nodes to both their IDs and geographic locations and a suite of location-based compromise-tolerant security mechanisms. To achieve en-routing filtering, additional 20 bytes authentication overheads are required.
In[1],Rongxing,Lu,XiaodongLin,HaojinZhu,Xiaohui Liang and Xuemin (Sherman) Shen, BECAN filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbor _ router (CNR)-based filtering mechanism. If source node has data send to the neighbours, then neighbour verify the message M and time stamp T and generate a MAC code for the message .The MAC code generated by each neighbour are send back to the source . Even if a node is compromised the message is verified by the neighbour thus prevents the false data generation. In all other method if node is compromised the attacker can obtain the key information and can inject false data, but in this case even if the attack obtain the key information they can‘t inject the false data because it should be authenticated by the neighbours. The source then combines the MAC and generates a MAC for Message which will be checked by the routers. Thus the burden for the sink is reduced and the false data is detected and removed early as possible. The BECAN achieving bandwidth-efficient authentication and early detecting the injected false data by the en-route sensor nodes

B. Worm Hole

A wormhole attack is very difficult to detect, because it can be launched without compromising either the host or the integrity and authenticity of the communication network [8], [9], and [10].

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

In [8], Y. Hu, A. Perrig, and D. Johnson describe a solution for the threat of a wormhole attack, based on geographical and temporal packet leashes. The use of geographical leashes assumes knowledge of the node location. The use of temporal leashes requires all nodes to have tightly synchronized clocks and demands computational power, which according to the authors, is beyond the capability of sensors. When temporal leashes are used, the sending node append the time of transmission to each sent packet *ts* in a packet leash, and the receiving node uses its own packet reception time *tr* for verification. The sending node calculates an expiration time *te* after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from travelling farther than distance L, the expiration time is set to:

$$t_e = t_s + L/c \qquad \text{------- (1)}$$

where *c* is the speed of light and is the maximum clocksynchronization error. All sending nodes append the time of transmission to each sent packet. The receiver compares the time to its locally maintained time and assuming that the transmission propagation speed is equal to the speed of light, computes the distance to the sender. The receiver is thus able to detect, whether the packet has travelled on additional number of hops before reaching the receiver. Both types of leashes require that all nodes can obtain an authenticated symmetric key of every other node in the network. These keys enable a receiver to authenticate the location and time information in a received packet.
Wang and Bhargava [11] introduce an approach in which network visualization is used for discovery of wormhole attacks in stationary sensor networks. In their approach, each sensor estimates the distance to its neighbours using the received signal strength. All sensors send this distance information to the central controller, which calculates the network‘s physical topology based on individual sensor distance measurements. With no wormholes present, the network topology should be more or less flat, while a wormhole would be seen as a _string‘ pulling different ends of the network together.

In [12] Hu and Evans propose to use directional antennas to detect wormhole attacks. Their approach uses a periodic HELLO message to determine the direction to each neighbour. When two nodes A and B wish to communicate, they find a correctly-positioned *verifier* V which ensures that the directions towards A and B are consistent. Their approach is promising; however, it relies on perfectly aligned, completely directional antennas, and cannot detect all wormhole instances, especially those using more than one wormhole.

In[13]LITEWORP uses secure two-hop neighbour discovery and local monitoring of control traffic to detect nodes involved in the wormhole attack. It provides a countermeasure technique that isolates the malicious nodes from the network thereby removing their ability to cause future damage. LITEWORP can be used to handle all but one of these attack modes. LITEWORP has several features that make it especially suitable for resource-constrained wireless environments, such as sensor networks.

LITEWORP does not require specialized hardware, such as directional antennas or fine granularity clocks. It does not require time synchronization between the nodes in the network. It does not increase the size of the network traffic, and incurs negligible bandwidth overhead, only at initialization and on detection of a wormhole.

IV. CONCLUSION

In this paper, we have surveyed the various attack and solutions available for wormhole attacks and false data injection in sensor networks. A summary is presented in Table 1 and 2. Most of the solutions use extra hardware which increases the cost but some of them implement without any added cost. One of example is Liteworp mechanism which is suitable for the sensor network to counter the wormhole attack when compared to all other. In case of False data injection best method is to use the BECAN, which prevent the false data even if the nodes are compromised, since the neighbours are authenticating the message. This mechanisms show good performance with low overhead.

Table 1: Summary of wormhole attack

METHOD	REQUIREMENTS	COMMENT
Packet Leaches Temporal [10]	Tightly synchronized clocks	Straight forward solution but difficult to achieve in case of sensor network
LiteWorp[20]	None	Applicable only to Static, stationary networks.
Directional Antennas by Hu and vans [14]	Node use section of their antennas to communicate with each other	Not suitable if more than one worm hole or sophisticated worm hole
Network Visualization by Wang[11]	Need Centralized coordinator	Good for Dense network

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

Table 2: Summary of False Data Injection

METHOD	REQUIREMENTS	COMMENT
SEF[3]	Key establishment in the network	Cannot verify if sender is malicious
Efficient Location-aware End-to-end Data Security (LEDS)[6]	Symmetric key and location information	Applicable only to static stationary networks.
Zhang et al. Location-Based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks[7],	Use public key cryptography	Not suitable if more than one worm hole or sophisticated Worm hole.
BECAN[1]	Public key cryptography , Diffie- Hellman key exchange and CNR based MAC Generation.	Provide Bandwidth efficiency, En-route filtering and reduce the burden of sink.

REFERENCES

[1]. RongxingLu,Xiaodong Lin, Member,HaojinZhu,Xiaohui Liang and Xuemin (Sherman) Shen, BECAN: ―A Bandwidth-Efficient CooperativeAuthentication Scheme for Filtering Injected False Data inWireless Sensor Networks‖ ,IEEE Parallel and Distributed System,2012.

[2] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, ―Toward Resilient Security in Wireless Sensor Networks,‖ Proc. Sixth ACM Int‘l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc ‘05),pp. 2005

[3]. F. Ye, H. Luo, S. Lu, and L. Zhang, ―Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks, ‖ Proc.IEEE INFOCOM ‘04, Mar. 2004

[4]. S. Zhu, S. Setia, S. Jajodia, and P. Ning, ―An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks Proc.IEEESymp. Security and Privacy 2004

[5] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, ―Toward ResilientSecurity in Wireless Sensor Networks,‖ Proc. Sixth ACM Int‘l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc ‘05),pp. 2005.

[6] K. Ren, W. Lou, and Y. Zhang, ―LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks,‖ Proc. IEEE INFOCOM‘06, Apr. 2006

[7] Y. Zhang, W. Liu, W. Lou, and Y. Fang, ―Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks,‖ IEEE J.Selected Areas in Comm., vol. 24, no. 2, pp. 247- 260, Feb. 2006.

[8] Y. Hu, A. Perrig, and D. Johnson, Packet Leashes: A DefenseAgainst Wormhole Attacks in Wireless Ad Hoc Networks, in: Proc. Of Infocom 2003. San Francisco, CA,USA, April 2003.

[9] S. Capkun, L. Buttyan, J. Hubaux, SECTOR: Secure Traking of Node Encounters in Muti-hop Wireless Networks, in: proc. Of SASN 2003. Fairfax, Virginia,October 2003.

[10] P. Papadimitratos and Z. J. Haas, Secure Routing for Mobile Ad Hoc Networks, in: Proc. Of CNDS 2002.January 2002. Wang, W.; Bhargava, B. Visualization of Wormholes in Sensor Networks. In Proceedings of the 2004 ACM workshop on Wireless Security (WiSe), ACM WiSE‘04, Philadelphia, PA USA, October 2004; pp. 51–60.

[11] Lingxuan Hu and David Evans. Using Directional Antennas to Prevent Wormhole Attacks. In Proceedings of the 2004 Symposium on Network and Distributed Systems Security (NDSS 2004), February 2004.

[12] Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In Dependable Systems and Networks (DSN), pages 612–621, Jun 2005