International Journal of
Sensor Networks and Data Communications

Khara, Int J Sens Netw Data Commun 2017, S1
DOI: 10.4172/2090-4886.S1-001

Review Article Open Access

A Review on Security Issues in Wireless Sensor Network

Shweta Khara*

Computer Science and Engineering (Information Security), PEC University of Technology, Chandigarh, India

Abstract

The conflux of sensing technique, data processing, and low-priced wireless communication has yielded a group of smart devices and when such devices used collectively, lead to the development of a technology called Wireless Sensor Network (WSN). A WSN is used to aggregate, monitor and analyze real-time data in a variety of applications, thus becoming an indispensable part of smart cities. But the gathering of sensitive information and the incorporation of wireless communication has arisen so many security related issues. This paper will concentrate on the issues and their corresponding solutions in wireless sensor network.

Keywords: Wormhole; Blackhole; Sybil attack; HELLO flood attack

Introduction

Wireless sensor network is an innovative technology which contains numerous portable sensors that are designed to sense tiny information of physical and environmental conditions. Also, the connectivity infrastructure is provided by the Gate-way, therefore, the sensed data is collectively sent to the base station through the gateway. WSN also emerges as both, a centralized stage in the IT as well as an advanced area of research incorporating various protocols, programming models, data acquisition, hardware, networking design, and security factors [1]. Examples of sensors include temperature sensors, speed sensors, ultrasonic sensors, humidity sensors, open-close sensors that detect four doors open or closed etc. These little pieces of information are extremely valuable to companies because it provides insights into defence that might happen in their business process. A typical wireless sensor network is shown in Figure 1. Each sensor node collects, process, and distributes the data wirelessly to the database.

Because of the distributed and highly vulnerable wireless communication, anyone can intercept into the network and therefore the risk of transmitting the data securely has in-creased. There is a chance of eavesdropping, tempering with data etc. Because sensors do not have high computation re-sources, therefore, traditional methods with huge computation for data transmission are unsuitable for WSN [2]. Therefore WSN requires different protocols and security mechanisms such that systems stability and security both can be preserved simultaneously.

Various attacks are possible in the wireless sensor network, for example, wormhole, Sybil attack, Blackhole etc. In the further sections, types of attacks and their corresponding solutions have explained.

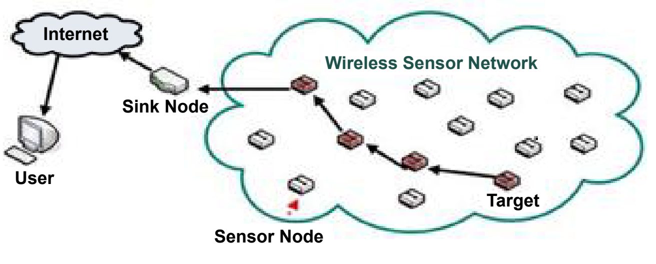

Figure 1: Wireless sensor network.

Wormhole

In this type of attack, malicious nodes make a tunnel which is hidden from the other genuine nodes. The data packets are sent from one malicious node to another via that tunnel, that is, the malicious node attract the packets from one area and passes them to other malicious node in another area [3]. Tunnel can be made through many ways such as in-band and out-of-band. To launch this attack, there is no need to compromise the other genuine network nodes. Therefore, this operation can extremely affect the routing procedures and the localization and can also launch attacks such as eavesdropping, replay attacks etc. against traffic packets. This attack can be established by using following techniques: wormhole using encapsulation, packet relay, high power transmission, out-of-band channel [4].

Blackhole

In this type of attack, an attacker do the re-programming in the captured set of nodes in the network in order to block the packets or once the intruder has been able to intrude himself into the communication network he can do anything with the captured packets passing between them and can generate false messages inspite of forwarding them to the base station in WSN [5].

Sybil attack

In this type of attack, a malicious node forges the identities of many other nodes. This malicious node can strongly influence the systems in which there is no centralized entity which can verify the identity of each communicating node. So this attack can occur in multipath routing, distributed systems etc. [6].

HELLO flood attacks

This attack uses HELLO packets in order to convince and attack other nodes in the network. The HELLO packets help the nodes to announce themselves to the neighbouring nodes. A node which

***Corresponding author:** Shweta Khara, Computer Science and Engineering (Information Security), PEC University of Technology, Chandigarh, India, Tel: 0172 2753851; E-mail: shwetakhara94@gmail.com

Received June 24, 2017; **Accepted** July 05, 2017; **Published** July 12, 2017

Citation: Khara S (2017) A Review on Security Issues in Wireless Sensor Network. Int J Sens Netw Data Commun S1: 001. doi: 10.4172/2090-4886.S1-001

receives these HELLO packets assumes that it is within the radio range of the sender. But sometimes this assumption prove out to be wrong when the malicious sender sends HELLO packets at such a high speed and processing power to a number of sensor nodes deployed over a wide area within a WSN such that it might convince every other node in the network that the attacker is their neighbour. Consequently, when nodes send the information to the base station they send via the malicious node because they think that the malicious node is in their neighbour [7].

Denial of Service (DOS) attack

The aim of this attack is to make network resources unavailable temporarily. In WSN various types of DOS attacks at various layers can be performed. For example, at physical layer it is tempering and jamming, at data link layer it is exhaustion and collision, at network layer it is homing, misdirection and black hole, at transport layer it can be performed by de-synchronization and flooding [3,7].

Physical attacks

Unlike the previous attacks, physical attacks are irreparable. Attackers can change the programming of the sensors or can replace a particular sensor with an illegitimate sensor which is under their control, can modify the associated circuitry etc. [3].

Solution to Attacks

Detection of Wormhole

The detection can be performed using methods like: Two phase detection algorithm [4] and using protocol AOMDV [8].

Two phase detection algorithm

This algorithm contains two phases [4]. In phase I of this algorithm, RCN (Rate of Change of Neighbourhood) is calculated. The RCN of node B at time s is calculated by using the following formula:

RCN(s)=1-(N(s1) R(s2-s1))/max(N(s2), N(s1))

Where N(s1) shows number of neighbours of node B at time s1, N(s2) shows number of neighbours of node B at time s2, R(s2-s1) shows number of new nodes at time s2 as compare to time s1. A lower and upper threshold values are predefined. If resulted RCN value is greater than the upper threshold value then definitely wormhole attack is present. If the RCN value lies in between lower and upper threshold then new neighbours are put into a doubtful zone and phase II is executed. In phase II, the trusted neighbours of node B find out the shortest path to the suspected node C which is not the direct link and also the one-hop neighbours of node B are being avoided. The path from node B to node C is not included. The reported path length is collected and checked. If the predefined threshold is less than any path length then that B -¿ C link is declared as fake link and wormhole attack got detected.

Using protocol AOMDV

In AOMDV (Adhoc On-demand Multipath Distance Vector) routing protocol, sender node checks whether there exists any route for the communication of any two nodes or not using the route table. If there exists the path then that route table gives the routing information otherwise it will broadcast the RREQ packet its neighbours which thus checks whether any route or path is present to the required destination or not. At whatever point when destination receives RREQ packet, it sends back the RREQ packet to the source along the same path along which it received the RREQ packet. In this way AOMDV calculates the multiple paths from source to destination [8].

Using AOMDV protocol along with RTT (Round Trip Time) we can detect whether Wormhole attack is present or not [8]. During the start of the communication when sender node finds out the route to locate receiver and broadcasts RREQ packet then it will note down the time s1. Receiver receives the route request and sends back the route replies along the same path through which it received the request. For each route reply received by sender node, it notes down the time s2. Then sender node calculates the RTT for all the routes using the following formula:

S3 i=s2 i-s1

Take RTT of each route and divide it by its corresponding hop count, that is, Sn i=S3 i/hop count

Calculate average of Sn i for i number of paths. The resulted value will be the threshold RTT. Compare each RTT with the threshold RTT. If the RTT of any route is very less than the threshold RTT and its hop count = 2 then definitely there would exist the wormhole in that link otherwise no wormhole. After knowing the wormhole attack, sender send the dummy RREQ packet and got to know about the m1 (1st malicious node) and when receiver receive the dummy RREQ then it got to know about the 2nd malicious node m2. Then m1 and m2 both entries are removed from routing table by source node and also source node broadcast this information to other nodes. Thus link which is affected by wormhole got jammed and no more use (Table 1).

Detection of Blackhole attack

The steps of algorithm [9] to detect the Blackhole are as follows:

1. A list of cluster of sensor nodes is maintained as D=C1, C2, C3, Cn.
2. ID to all the nodes are assigned as ID=ID1, ID2, ID3.. IDn.
3. A coordinator (E) for the set D is being selected according to criteria such as a node can be a coordinator only if it has sufficient battery power and can be a coordinator only upto certain time limit, all the remaining nodes remain under the supervision of the selected coordinator node.
4. The coordinator (E) has the information of IDs of sensor nodes maintained in the form of a table.
5. E can verify the IDs of the sensor nodes from the set D after a regular interval of time by sending beacons and If (Response and Data packets both arrived) then no threat else if (Response packet and data packet both not arrived) If (t1¿= t2) then Node failure else t1++; else if (Response packet arrived but not data packet) if (t1¿=t2) then // t1 is the time period for the intermediate node makes the coordinator node to wait for the incoming packet and t2 is the threshold time for which the coordinator node is supposed to wait for an incoming packet.
6. Node perhaps malicious and Blackhole detected, rename the ID of suspected node to IDj else t1++.

S. No.	Attack	Detection Mechanism
1	Wormhole	Two phase detection algorithm [4]
2	Wormhole	Using AOMDV protocol with RTT [8]
3	Blackhole	Algorithm [9]
4	Sybil	Modified centralized IDS scheme [10]
5	HELLO flood	LEACH protocol with RSS and Distance Threshold [11]

Table 1: Solution attacks and its Detection mechanisms.

7. Remove the node with ID as IDj from the set D.
8. The nodes that were previously responding to the node with ID as IDj will be informed about the node with which now they have to communicate.
9. (viii)The detection process will remain continued.

Detection of Sybil attack

The detection of Sybil attack can be performed using modified centralized IDS [10]. The process of this method goes as follows:

1. Firstly, a cluster head with the highest energy is selected among the sensor network.
2. In this network, if the Sybil node is present then it may use the same cluster head ID and can send beacons to the other nodes of the network asking them to join the cluster.
3. The nodes which received the beacons will join the respective cluster heads and will form a cluster.
4. After the cluster has formed a control packet is being sent by the cluster heads to the base station, which contains ID and location of the cluster head as well as ID and location of its corresponding members.
5. Sybil node has used the ID of the cluster head, therefore the base station will receive the same ID from 2 cluster heads and so it will mark both of the cluster heads as suspects.
6. Base station will then send a message to the nodes and will ask them to again select their cluster head.
7. Again the Sybil node will replicate the ID of newly selected cluster head and again will send the control packet to base station.
8. Base station will now check the ID and location of new cluster heads. Because Sybil node is same, therefore its location will not be changed. Hence base station will detect the Sybil node.
9. Base station will send out a message to the member nodes about the location of the Sybil node so as the member do not join that node.

Detection of HELLO flood attack

LEACH (Low Energy Adaptive Clustering Hierarchy) protocol arranges the nodes in the network into small clusters and chooses one Cluster-head (CH) among them. Non-CH nodes after sensing their CH send data to the CH, after then CH compresses the data collected from all the non-CH nodes and send it to the base station [11].

Mahajan et al. [11] has considered that in each WSN, the non-CH nodes compare the RSS of receiving HELLO packets with threshold RSS as well as compare the distance between non-CH and elected CH with the Distance threshold. Also in Mahajan et al. [11] has assumed that every node has its location information such that when CH nodes advertise HELLO packets at that time they also send their location information. Other nodes which receive HELLO packets along with distance coordinates from advertising CH calculate the distance between them by using the following formula:

Distance=sqrt[sq(x-x1)+sq(y-y1)]

In this, x and y are the location coordinates of CH node which receiver receives along with HELLO packets, x1 and y1 are the location coordinates of the receiver. Receiver node also calculates a threshold value for RSS and threshold value for Distance. For each non-CH node, if RSS is less than the threshold RSS and distance is less than threshold distance then CH node is accepted as CH by non-CH node otherwise CH node is put into suspicious zone or got blacklisted. Then in future no more packets are received from that blacklisted CH node [11]. Using above procedure the HELLO flood attack can got identified.

Conclusion

WSN has its many types and features due to which there arise many problems in various scenarios. Security remains the linchpin of good WSN. Therefore the only need is to choose right solution for the right situation in order to get the maximum advantage from the WSN. This paper shows various solutions corresponding to various attacks and also enhances the base for this emanating technology.

References

1. Jain A, Kant K, Tripathy M (2012) Security solutions for wireless sensor networks in Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on IEEE pp: 430-433.
2. Mishra KB, Nikam CM, Lakkadwala P (2014) Security against black hole attack in wireless sensor network-a review in Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on IEEE pp: 615-620.
3. Mulla RI, Patil R (2016) Review of attacks on wireless sensor network and their classification and security. Imperial J Interdiscipl Res 7: 2.
4. Patel MM, Aggarwal A (2016) Two phase wormhole detection approach for dynamic wireless sensor networks in Wireless Communications Signal Processing and Networking (WiSPNET), 2016 International Conference on IEEE pp: 2109-2112.
5. Krishnan NS, Srinivasan P (2016) A qos parameter based solution for black hole denial of service attack in wireless sensor networks. Indian J Sci Technol 9: 38.
6. Healy M, Newe T, Lewis E (2009) Security for wireless sensor networks: A review in Sensors Applications Symposium (SAS), 2009 IEEE pp: 80-85.
7. Pathan KSA, Lee WH, Hong SC (2006) Security in wireless sensor networks: Issues and Challenges in Advanced Communication Technology (ICACT), 2006 The 8th International Conference on IEEE 2: 6.
8. Amish P, Vaghela V (2016) Detection and prevention of wormhole attack in wireless sensor network using aomdv protocol. Proc Comput Sci 79: 700-707.
9. Wazid M, Katal A, Sachan SR, Goudar R, Singh D, et al. (2013) Detection and prevention mechanism for blackhole attack in wireless sensor network in Communications and Signal Processing (ICCSP), 2013 International Conference on IEEE pp: 576-581.
10. Prabhjotkaur CA, Singh S (2016) Review paper of detection and prevention of sybil attack in wsn using centralizedids. Int J Eng Sci 8399.
11. Mahajan M, Reddy K, Rajput M (2016) “Design and simulation of a blacklisting technique for detection of hello flood attack on leach protocol”. Proc Comp Sci 79: 675-682.