International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 1, January - 2014

A Survey in Hello Flood Attack in Wireless Sensor Networks

Akhil Dubey, Deepak Meena, Shaili Gaur

M.Tech. Scholars, Dept. of Computer Science & Engg.
IEC-College of Engineering & Technology
Greater Noida, U.P., INDIA

Abstract

Sensors are very useful and play a vital role in human life. Decade ago, wireless sensor networks, since their inception have three important field in research area that is hardware & software of the sensors nodes, application area and most important communication & networking security issues in WSN. Due to the limitations of resources communication range, processing capability & battery power WSN are vulnerable to many types of attacks at the network layer; hello flood attack is one of them. This attack is done through an illegal node in the network by flooding the hello request to the legitimate node continuously and breaks the security. It is an easy task for an adversary to capture the node in the large deployed network; by the use of this slave node he can easily broadcast the hello packet flood. In this paper we describe that how hello flood attack works and up to which stage of damaging occurs. Then we study about cryptographic security scheme, its pros & cons and other upgraded defense mechanisms for hello flood attack.

Keywords—*Wireless Sensor Networks, Flooding, Cryptography, Puzzle, Signal Strength*

1. Introduction

When development step in building, utilities, industrial, home, shipboard, and transportation systems automation is promote to the next generation, the evolutionary role of sensors came to our notice. Wireless sensor networks are the combination of the different sensing nodes and responsible for sensing as well as for the first stages of the processing hierarchy. In the field of wireless networks wireless sensor networks is a special class of ad hoc net works in which small sensors are used. Sensors are small devices that well furnished with advanced sensing functionalities like monitoring temperature, pressure, and acoustics etc.

. In the structure of sensor node it mainly contains radio transceiver, battery, memory, GPS, sensors, microcontroller and power devices.

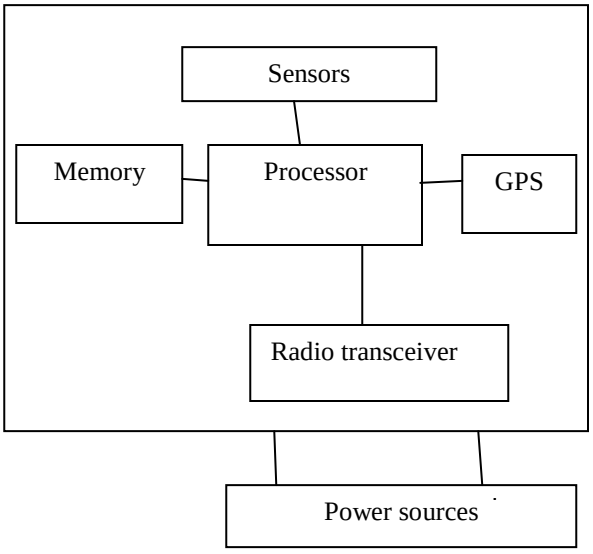

Figure 1. Architecture of Sensor Node [1]

In this networks sensor nodes are responsible for the information interchange. The cost of sensor nodes

varies from thousands rupees to a few hundred rupees, depending upon their memory size and processing speed. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as battery, computational speed, memory and transmission range. The major applications of wireless sensor networks are the military applications of sensor nodes include battlefield surveillance and monitoring, guiding systems of intelligent missiles and detection of attack by weapons of mass destruction. Second is The Medical Application and Environmental monitoring, Industrial Applications, Infrastructure Protection Application etc. [2]

This paper is divided in seven sections in 2nd section we tell about different attacks in WSN. In 3RD we define the hello flood attack and its defense schemes is presented in 4th section, upgraded schemes is in 5th section and in 6th section we describe the supporting attack's defense schemes at last we conclude our paper in 7th section.

2. Different Attacks in Sensor Network

There are many attacks have been found time to time by many scholars. In the network there are five layers for communication protocols. These attacks are created by an advisory on the different protocol layers. Such as at physical layer Jamming, Radio interference and Tampering or destruction occurs. At Data Link Layer Continuous Channel Access (Exhaustion), Collision, Unfairness, Interrogation and Sybil Attack occur. At network layer Sinkhole, Hello Flood, Node Capture, Selective Forwarding, Wormhole Attacks, Spoofed, Altered, or Replayed Routing Information, Acknowledgment Spoofing, Misdirection, Internet Smurf Attack and Homing attacks are create. At transport layer flooding and De-synchronization Attacks occur. At application layer Overwhelm attack, Path-based DOS attack and Deluge (reprogram) attack occur. In this paper we discuss about hello flood attack. Besides that we also explain flooding, tempering and node capturing because these attacks are directly related with hello flood attack. [3]

3. Hello Flood Attack

Hello flood attack is the main attack in network layer. The Hello flood attacks can be caused by a node which broadcasts a Hello packet with very high power, so that a large number of nodes even far away in the network choose it as the parent node [4]. All messages now need to be routed multi-hop to this parent, which increases delay. Hello messages are broadcast to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker node is their neighbor, so that all the nodes will respond to the HELLO message and waste their energy. Consequently the network is left in a state of confusion.

The figure 2(a) and 2(b) show about this attack, in this diagram we show the circle as a sensor nodes and in rectangle we show the base station and malicious node like attacker.

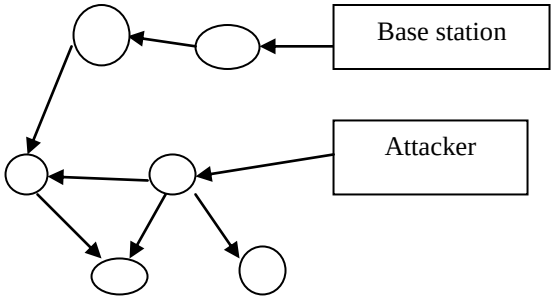

Fig 2(a)

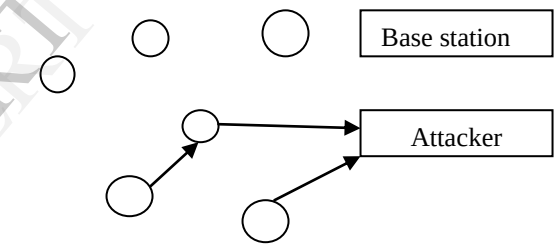

Fig 2(b)

Figure 2(a). shows an attacker broadcasting hello packets with more transmission power than a base station.

Figure 2(b). shows that a legitimate node considers attacker as its neighbor and also as an initiator [5].

In this attack advisory captures a node and broadcast hello massages and declare itself their neighbor. When a node receive this massage and assume that sending node is in communication range, node start communicate to that node and make entry into its routing table as a neighbor. For example in a network all sensor nodes are communicate with base station through its neighbor. When a laptop class attacker captures a legitimate node or creates a false node and broadcast a massage to all nodes so the high power of massage creates a confusion that the massage is come from to its neighbor nodes. So that all nodes assume that the hello massage path is the shortest path from the

base station and assumes that attacker node is a base station and communicates with attacker. So that an attacker can easily control on the network and base station is totally cut from the network. This attack is also affected the routing in WSN. This attack is the main attack at the network layer of the wireless sensors networks [4].

3.1 Hello Packet Properties

There are five main features of hello packet are given below [6]

1) The size of Hello packet is small as compared to data packet.
2) The probability of hello flood reaching to its receiver is higher than data packet especially over weak links.
3) Broadcasting of Hello packet is always done at basic bit rate because Lower bit rate transmission is more reliable.
4) Hello packets are broadcasted without any acknowledgement.
5) There is no guarantee about the bidirectional communication of hello packets.

3.2 Supporting Attacks for Hello Flood Attack

This attack also invites transport layer attack flooding, tempering and node capturing and false node replication. So here we also explain the supporting attacks.

3.2.1 Flooding

In flooding the attacker continuously send new connection request to their neighbor so that these requests capture all the resources. It produces severe resource constraints for legitimate nodes [3].

3.2.2 Tempering and Node Capturing

The term tampering is well accepted in the research community to designate attacks on components that involve modification of the internal structure of a single chip. So that advisory can easily capture on it and use for hello flood attack.

And node capture attacks which give the attacker full control over a sensor node. It is not so easy. To do this attacker requires expert knowledge, costly equipment and other resources, and, most important work is removal of nodes from the network for high amount of time [7].

3.2.3 False Node Replication

In this attack an attacker implant a new sensor node in the network, this is using the ID of a legitimate user. Mainly attacker first remove the legitimate node and at the place of it attacker deployed false node with genuine node id. This attacker node replication can cause a big destruction in network and support the hello flood attack [3].

In this section we know about the hello flood attack this attack create interruption in two manner first is by creating the confusion and flooding in the network so that attacker is succeed in interruption of the data packet sending in whole network and secondly is by implanting a false node so it create hello massage so all nodes communicate it by knowing that it is a base station. But truly they communicate with attacker. So attacker can control on overall network most of the time. So the damage occur from this attack is very high.

4. Defense Strategies against Hello Flood Attack

In the large deployed network there are many unattended energy crucial sensor nodes, which are cooperate each other but also vulnerable to many kind of network attacks like Hello flood. In this section I present the review about all security schemes against hello flood proposed by different scholars both cryptographic and upgraded schemes.

In [8] authors define the cryptographic security scheme to defend the hello flood attack. In this scheme any two nodes share the same secret key. In every new communication new encryption key is generated. So according to this scheme only legitimate nodes can decrypt and verify the message and receiver node only accept the data packet from which node that is in its routing table. The main drawback of this scheme is that if any attacker can spoof the identity then he makes the attack on network. And this scheme has also heavy computational complexity not suitable for wireless sensor network.

In [9] scholars suggest identity verification protocol technique. It is a bi directional verifying protocol of a link in which receiver check the identity of data packet sender and after verifying correct it send the feed back to the sender, so it is a encrypted reflect-back mechanism. This scheme is more effective when receiver is highly sensitive. The main problem in this scheme is if attacker compromise with sender node before receiving the feed back then he can drop the feedback and block all its sender nodes. Thus, such an attacker can easily create a wormhole to every node within its range. If this done the above approach will not likely be able to locally detect or prevent a hello flood attack.

A Hamid and S Hong proposed Multi-path multi-base station data forwarding technique for multiple base stations in [10]. In this scheme every node has a number of secret keys. When it sends its sensing data to the multiple routs then use its keys. In the multi base system every base has some certain numbers of nodes and all base stations communicate with this scheme. In this scheme node generate multiple keys in the very short time so this create extra work load on the processor of the node. This may cause the crashing of the node and likewise the cryptographic schemes it has high computational complexity.

In [6] authors have given the probabilistic based approach. This approach is concerned with energy, so in this first authors proposed energy saving routing by Network Modeling and second node selection by Turn-Rolling technique, in this we Consider that the energy taken either to send one packet to neighboring node or compute eight hundred or one thousand lines of instructions by sensor node is same, it is not feasible that on each time nodes belonging to sensor field receives a hello packet will report to base station. Considering energy constraint in mind, probabilistically chosen random set of nodes will correspond with base station to validate the legitimacy of data sending request, so there are three types of node in this scheme. Due the fix routing if attacker cut the link then data packet may lost or if an attacker compromise with corresponded node then he easily make hello flood attack in one part of the network.

In [11] authors proposed the cryptographic puzzle scheme, it is based on reputation client puzzle. In this scheme first we define the reputation of the node by the formula

$$RPi = log \frac{1+ncp}{1+npk} \qquad \text{..... (1)}$$

Where *ncp* represents the number of puzzles solved by node *i*, *npk* denotes the number of packets sent by node *i* to base station. RPi is the reputation of the node i. Through this a legitimate node solve the more puzzle with honesty and send limited data packet so the reputation is high and attacker node not solve the puzzle as easily and it is always flooding the base station, so it has low reputation. So according to the reputation client puzzle node define the secret keys for the routing and then calculate the reputation of the node and design the puzzle. Hence the difficulty of cryptographic puzzles for attackers will increase according to low reputation value, whereas as for honest nodes, who honestly solve puzzles giving rise to larger n_{cp}, will get high reputations mapping to easier cryptographic puzzles. But likewise cryptographic and multipath scheme it has very high computational complexity.

In [12] authors proposed an idea is to tune the timing of the channel access and transmission parameters so that the responses of these nodes collide with each other due to the high density in arrival time and prevent the adversary from decoding the messages correctly. So the adversary will not be able to hear the victim's replies and is compelled to reduce his power and act just like a normal node in the ideal form.

5. Other Advance Security Schemes

In the last section we present many security schemes which based on cryptography and also narrate the drawbacks of these schemes. In this section we present some other upgraded security schemes.

In [5] authors proposed the signal strength and client puzzle based scheme the signal strength can be calculated as

$$Pr= (Pt*Gt*Gr*Ht^2*Hr^2)/ (d^4*L) \qquad \text{..... (2)}$$

In this eq. Pr is received signal power (in watts), Pt is transmission power (in watts), Gt is the transmission antenna gain, Gr is the receiver antenna gain, Ht is the transmitter antenna height (in meter) and Hr 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). So according to this authentication puzzle identification algorithm first set the input signal strength according above formula if an intermediate node receives hello message from the source node. If signal strength of received hello message is equal to fixed signal strength in radio range than source node is classified as a true node accepts hello message and perform necessary function. If not than check another condition. If Signal strength of received hello message is nearly equal to fixed signal strength in radio range then nodes request an authentication identity and send a puzzle to source node according to its reputation, If authentication identity is correct and reply message of correct answers comes in fixed time threshold then Node is classified as a true node and accepts the request and performs function. If not than check signal strength of received message is greater than fixed signal strength in radio range then source node is classified as stranger and rejects the further requests from it. This scheme reduce the computational complexity of the processor but there are some limitations of this schemes like we assume that

communication is within fixed radio range, all sensor nodes in a fixed radio range have same transmitting and receiving signal strength and all sensor nodes have same hardware and software, battery power etc.

One other scheme is counter based in this scheme a legitimate node keep a count list in which node checks the number of hello message received in a fixed time interval with the help of a counter. Node accepts the request of that node first that has minimum count in the count list.

Another scheme is based on time, if the reply massage is not received in a predefined time threshold by a node then it treats the sender to be an attacker and send this information to other nodes.

One proposed scheme is based on packet size, according to the property of the hello packet the size of packet is very small than data packet size so we design an algorithm which drop those small size packet that has high signal strength.

6. Defense Schemes for Supporting Attacks

6.1 Defense Schemes for Flooding

Flooding can be stooped by asking a puzzle during the connection establishment between the nodes.
Another method is that we can fix a limit above sending the packets on the node [3].

6.2 Defense Scheme for Tempering and Node Capturing

In order to design a WSN secure against tempering and node capture attacks, the following steps should be applied:
1) Take standard precautions for protecting microcontrollers from unauthorized access
2) Choose a hardware platform appropriate for the desired security level, and keep up-to-date with new developments in embedded systems security
3) Monitor sensor nodes for periods of long inactivity
4) Allow for revocation of the authentication tokens of suspicious nodes [7].

6.3 Defense Scheme for False Node Replication

This type of attack is can be defend by monitoring and encrypted authentication techniques.
Another scheme for detecting malicious nodes that launching hello flood attack is signal strength and geographical information is proposed in [13]. In this scheme first calculate the signal strength of a node according to its geographical information and then compare the packet signal strength with the actual signal strength if there found any inequalities between them the we can say that sending node is a malicious node.

7. Conclusion

Wireless sensor network plays an important role in military operations and at the time of natural disaster. Hello flood attack is the main attack on wireless sensor network, so it is necessary to defend this attack with light and powerful defense schemes. So in this paper we present the hello flood attack, hello packet and different defense schemes proposed by many scholars time to time, drawbacks of cryptographic schemes, signal and puzzle based security scheme and defense schemes of supporting attacks. In future we implement these security schemes on network simulator to check effectiveness of the upgraded security schemes.

8. Acknowledgement

We all of us would like thanks our college guide prof. rajnesh singh and our head of the department, computer science and engineering.

9. References

[1] Dr. Yudhvir Singh, Dheer Dhwaj Barak, Vikas Siwach, Prabha Rani,"Attacks on Wireless Sensor Network: A Survey ", IJCSMS International Journal of Computer Science and Management Studies, Vol. 12, Issue 03, Sept 2012 ISSN (Online): 2231-5268
[2] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010
[3] Chaudhari H.C. and Kadam L.U."Wireless Sensor Networks: Security, Attacks and Challenges" International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16 Available online at: http://www.bioinfo.in/contents.php?id=108
[4] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks", Commun.ACM,47(6):53-57.
[5] 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 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814
[6] Mohamed Osama Khozium, "Hello Flood Counter Measure for Wireless Sensor Networks", IJCSS: International Journal of Computer Science and Security, " Volume 2, Issue 3"57-65, May/June 2008
[7] Alexander Becher, Zinaida Benenson, and Maximillian Dornseif" Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks" RWTH Aachen, Department of Computer Science 52056 Aachen, Germany
[8] Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.

[9] Venkata C. Giruka, Mukesh Singhal, James Royalty, Srilekha Varanasi, (2006), Security in wireless networks, Wiley Inter Science
[10] A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT
[11] Zhen Cao, Xia Zhou, Maoxing Xu, Zhong Chen, Jianbin Hu,Liyong Tang , (2006), Enhancing Base Station Securityagainst DoS Attacks in Wireless Sensor Networks, IEEE
[12] Mohammad Sayad Haghighi , Kamal Mohamedpour, (2008), Securing Wireless Sensor Networks against Broadcast Attacks, IEEE
[13] Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, (2004), MaliciousNode Detection in Wireless Sensor Networks, IEEE