Rupinder Singh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.4 Issue. 5, May- 2016, pg. 1-9 **ISSN: 2321-8363**
Impact Factor: 4.123

HELLO FLOOD ATTACK COUNTERMEASURES IN WIRELESS SENSOR NETWORKS

Rupinder Singh[1], Dr. Jatinder Singh[2], Dr. Ravinder Singh[2]

[1]Research Scholar, IKG PTU, Kapurthala, Punjab, rupi_singh76@yahoo.com
[2]IKG PTU, Kapurthala, Punjab, bal_jatinder@rediffmail.com

Abstract

Wireless sensor network (WSN) is a collection of dispersed and dedicated sensors nodes for monitoring, recording the physical conditions of the environment, and organizing the collected data at a central location. WSN are playing a great role in the controlling and managing environments in different situations and has become important part of research area. WSN research is usually classified into three categories i.e. hardware & software of the sensors nodes, application area and communication & security. Due to limited resources of computation power, battery, communication range, WSN are vulnerable to different types of attacks and hello flood attack is one of them. This attack is performed by malicious node by flooding the hello request to the legitimate node continuously in order to break the security. In this paper we first describe the working of hello flood attack and then we discuss various countermeasures proposed in the literature for tackling with hello flood attack. A detailed study of these countermeasures with their limitations is the need of the time so that new and improved one can be proposed in the future for more robust security against hello flood attack.

Keywords: Wireless Sensor Networks, Sensor, Hello flood attack, Malicious, legitimate node.

1. INTRODUCTION

Wireless sensor network (WSN) is a collection of dispersed and dedicated sensors nodes for monitoring, recording the physical conditions of the environment, and organizing the collected data at a central location. WSNs usually measure environmental conditions like temperature, sound, pressure, pollution levels, humidity, wind speed and direction, etc.

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. The security concerns of the sensor network should be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of wireless sensor networks. Every node in the WSN must be designed to provide the set of primitives that are necessary to synthesize The challenges of security in WSN are totally different from traditional network security due to inherent resource and computing constraints. WSNs use interconnected topology as it is deployed for meeting strict requirements of power consumption, size, and cost. Security for group

communication applications that require packet delivery from one or more senders to multiple receivers is more critical and challenging goal. Figure 1 shows the structure of a typical WSN.

Sensor nodes are often deployed in large accessible areas that present the added risk of physical attack. Sensor networks also poses new security problems as they interact closely with their physical environments and with people. Most of the early proposed network techniques in the past assumed that all nodes are cooperative and trustworthy. However, this is not the case for many sensor network applications today, that require a certain amount of trust in the application. This is required in order to maintain proper network functionality. Consequently, the existing security mechanisms are inadequate resulting in new research directions and new ideas for properly addressing sensor network security.

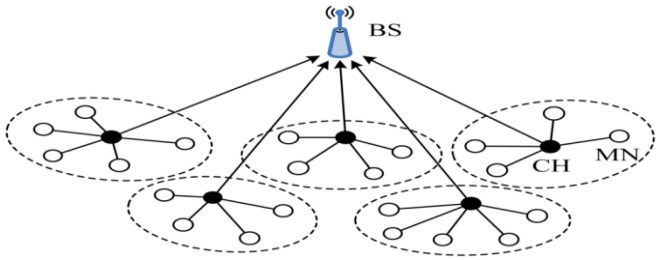

Figure 1: A typical WSN

.
A variety of attacks are possible in WSN including Jamming, tampering, collision, exhausting, hello flood, wormhole, sybil, sinkhole, flooding, denial-of-service, cloning etc. Hello flood attack is one of the main attack in network layer of WSNs. Hello flood attack is caused when an attacker with high transmission power can send or replay hello packets which are used for neighbour discovery. In this way, attacker creates an illusion of being a neighbour to other nodes and underlying routing protocol can be disrupted, which facilitate further types of attacks. The attacker broadcast packets with such a high power that a large number of nodes in the network choose it as the parent node. In this paper we first describe the working of hello flood attack and then we discuss various countermeasures proposed in the literature for tackling with hello flood attack. A detailed study of these countermeasures is required along with their limitations so that new and improved can be proposed for more robust security against hello flood attack.

2. HELLO FLOOD ATTACK

Hello flood attack is one of the main attack in network layer of WSN. Hello flood attack is caused when an attacker with high transmission power can send or replay hello packets which are used for neighbour discovery. In this way, attacker creates an illusion of being a neighbour to other nodes and underlying routing protocol can be disrupted, which facilitate further types of attacks. The attacker broadcast packets with such a high power that a large number of nodes in the network choose it as the parent node. Figure 2 shows the scenario of hello flood attack.

All messages to be broadcasted in the WSN are routed through this parent, that increases delay. The attacker broadcast these hello messages to a large number of nodes in a wide area of the WSN. These nodes are then forced to be convinced that the attacker node in the network is their neighbour. All the nodes are going to respond to this HELLO message from the attacker and are going to waste their energy. This results in a confusion state in the

WSN. Figure 3 and 4 show hello flood attack in the network. In this diagram circles, rectangle, and triangle represents sensor nodes, base station, and attacker respectively.

In Hello flood attack advisory captures a sensor node and broadcast hello massages in the network and declare itself their neighbour. When any node in the network receives this hello message, it assumes that sender node is in communication range and start communicating that node and make entry in its routing table as a neighbour. All sensor nodes communicate with base station through their neighbours. When an attacker captures a legitimate node in the network or creates a fake node, it broadcast hello message to all nodes in the network with the high power, it creates a confusion that the message is come from its neighbour nodes. So that all the nodes in the network assume that the hello message path is the shortest path from the base station by assuming that attacker node (malicious) is a base station and starts communicates with attacker. In this way an attacker can control the network as base station is totally cut from the WSN and also affect its routing. Hello flood attack is the one of the main attack at the network layer in WSN.

Figure 2: Hello Flood Attack

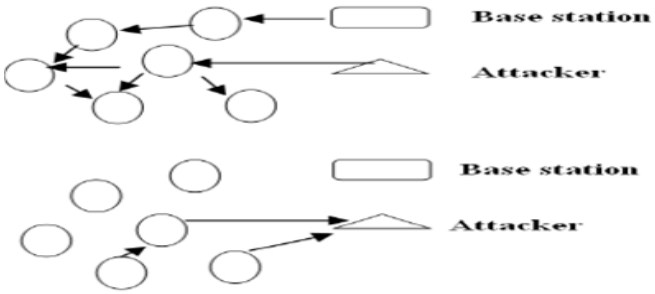

Figure 3: Shows broadcasting of hello packets by attacker with more transmission power than a base station.
Figure 4 shows legitimate nodes considering attacker as their neighbours.

2.1 Properties of hello packet

Hello packet has five main features as given below [17]:

1) The size of the Hello packet is smaller as compared to data packet.
2) The probability of hello packet reaching to its receiver is usually higher than data packet especially in weak links in the network.

3) Broadcasting of the hello packet is done at basic bit rate since lower bit rate transmission is more reliable as compare to others.
4) Hello packets do not require any acknowledgement for broadcasting.
5) Bidirectional communication of hello packets is not guaranteed.

2.2 Hello flood attack supporting attacks

A large number of attacks are supported by hello flood attack including flooding, tempering and node capturing, false node replication etc. These supporting attacks are explained below:

1) Flooding

In flooding attack, the attacker continuously send new connection request to their neighbour in order to capture the resources. This results in severe resource constraints for legitimate nodes.

2) Tempering and node capturing

Tampering is concern with attacks on components that involve modification of the internal structure of a single chip. An advisory can easily capture it and can be used for hello flood attack. Node capture attacks give the attacker full control over a sensor node, but node capturing is not easy. To do node capturing, attacker requires expert knowledge along with costly equipment and other resources. The difficult is the removal of nodes from the network for large amount of time.

3) False node replication

In false node replication attack, a new sensor node is implanted by an attacker in the WSN by using the ID of a legitimate user. Attacker first removes the legitimate node from the network and at that place deploy false one. This false node replication can cause a huge destruction in WSN by supporting the hello flood attack. Attacker can have control on overall network for most of the time and therefore the damage occur from this attack is very high.

3. HELLO FLOOD ATTACK COUNTERMEASURES

This section of the paper provides various countermeasures proposed in the literature to tackle with the hello flood attack in WSNs. Although a number of countermeasures are proposed but design of efficient and robust security mechanisms is still a great challenge.

3.1 CHMD Algorithm

The characteristics of clustering of Low Energy Adaptive Clustering Hierarchy (LEACH) could effectively reduce energy consumption of wireless sensor network. In [1] according to authors, cluster heads are so vulnerable to various malicious attacks, which will greatly affect the performance of the whole network. The paper begins with setting of a reasonable threshold for the members of the cluster that each cluster head belongs to so as to initiate the detection mechanism, then an algorithm for detection of Hello flood attack caused by malicious cluster head on LEACH protocol is improved according to the voting mechanism. This algorithm just detects those cluster heads whose numbers of cluster members are beyond the threshold, and then it confirms the malicious node by the voting mechanism of guide nodes based on the received signal strength (RSSI) and the distance. According to authors, the algorithm proposed in this paper can effectively reduce the energy consumption of the network and the false positive rate, which will prolong the network lifetime.

3.2 BAP Technique

In [2] authors consider Wireless Sensor Network security and focus attention to tolerate harm caused by an adversary who has compromised deployed sensor node to change, block, or inject packets. Authors analytically show that their defence mechanisms against Hello flood attack using BAP Method. In this paper authors present the hello flood attack, hello packet and cryptographic schemes, signal and puzzle based security scheme, and defence schemes of supporting attacks. The proposed security framework for hello flood detection via a signal strength and cryptographic puzzle method is more secure and hence it is quite suitable for sensor networks. Authors implement these security schemes on programming to check result and effectiveness in securing sensor networks. According to authors in future implementation of the proposed scheme in ns-2 can be done to check its effectiveness in securing sensor networks with other puzzle method.

3.3 LDK Scheme

Based on non-cryptographic and cryptographic, solution for detection Hello flood attack is proposed in [3]. In this paper both RSS and distance calculation is used and by comparing both, test packet approach is used. According to authors, the number of times the test packet is transmitted is greatly reduced by providing security using location dependent key (LDK) management scheme where it involves loading random set of keys to the nodes prior to deployment. Furthermore, LDK doesn't require any knowledge of node deployment, eventually provides better connectivity and containment of node compromise.

3.4 Location Verification Scheme

An IDS based on nodes location verification algorithm for WSNs to detect the locations of malicious nodes is proposed in [4]. In addition, this IDS detects hello flood attack and report the attack and goal nodes. Authors implemented an intrusion detection system in MATLAB to detect the hello flood attacks on WSNs based on using the greedy filtering by matrix location verification scheme. According to authors system has achieved high detection rate which in average 9.0643, the false positive rate became lower and false negative rate became higher with increasing the anomaly degree, but, both in general were low as required with average false positive rate 0.3263 and average false negative rate 0.1362.

3.5 Energy Level Based Scheme

In [5] according to authors, existing solutions for detection of HELLO flood attack are either cryptographic which are less suitable in terms of memory and battery power, or non-cryptographic which involves sending the test packet for detection. This increases communication overhead as the energy required for transmission of the packet is far more than the energy required for processing/calculation. Based on these facts, a non-cryptographic solution for Hello flood attack detection is proposed in this paper, in which the no. of times the test packet is transmitted is greatly reduced. In the proposed scheme authors aim to detect the malicious cluster head on the basis of energy remaining with it. When the malicious cluster head broadcasts Hello message to the large part of the network its energy tends to become lower than the other nodes present in the network. The proposed scheme by authors is divided into two phases.

Phase 1: The nodes which are located far away from the cluster head will compare their distance from the attacker and received signal strength value of the signal with the threshold value. If the received RSSI value is less than the threshold value and the distance is more than threshold value then the nodes will not join the malicious cluster head.

Phase 2: If the nodes are located closer to the attacker cluster head then the cluster head will first send its remaining energy level to the nodes. The nodes will compare their remaining energy level with that of the malicious attacker. If the energy level is low then they will not join the malicious cluster head. The simulation results showed

detection of adversary nodes with minimal communication overhead as the number of test packets sent for detection is reduced from 20-35 to 10-14.

3.6 EBDS Scheme

In [6] according to authors cryptographic approaches used are found not to be very suitable as the complexity found in handling the keys. So non cryptographic approaches are introduces which are based on RSS (received signal strength), finding distance between nodes, test packet approach and LDK(Location dependent key) scheme are suitable up to some extent. In this paper authors present the new non cryptographic approach EBDS (Energy based detection scheme) which detect the attacker by calculating the energy of nodes as when attacker starts dropping the packets its energy starts decreasing and it becomes the low energy node when compare with other nodes. According to authors, EBDS is efficient to save the data of node that lies near to base station as in this approach detection is carried out on the basis of energy of nodes as attacker node starts flooding as it enters in network. So its energy level will be low as compare to other nodes.

3.7 RSS and Distance Based Scheme

A new security framework for Hello flood detection is implemented in [7] and the results are analyzed which proves that it requires less computational power, hence is suitable for sensor networks. The new algorithm is implemented in Matlab by modifying LEACH protocol. Hello flood attack is generated by making selected adversary nodes send Hello message using high transmission power as compared to regular nodes. The performance of the proposed approach has been compared with existing technique of received signal strength based approach. The simulation results show that the proposed approach is effective in improving the performance of the network. It results in lesser detection time & energy for detection as compare to existing one and also results in smooth functioning of LEACH Protocol even under hello flood attack with minimal communication overhead. The proposed work on LEACH under hello flood attack detects the adversary node successfully but does not result in isolation of adversary nodes.

3.8 RSS and Geographical Information Based Scheme

According to authors in [9], LEACH protocol is difficult for an adversary to attack except the case when the adversary node become a Cluster Head, it makes it easy for the attacker to launch a HELLO flood attack by simply broadcasting a powerful advertisement to all the nodes deployed in the sensing field. In this paper, a new non-cryptographic approach to detect and prevent HELLO Flood attack in LEACH protocol in WSN is proposed. The results of the proposed approach have been compared with the existing approaches and the comparison proves that the proposed approach is more effective with less detection time, energy and computational overhead. The proposed approach improves the network performance by early detection of adversary and preventing the nodes from associating with such a malicious Cluster Head.

3.9 Signal Strength Based Scheme

According to authors in [11], the current solutions for hello flood 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 by authors 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.

3.10 An Analytical Approach

An analytical approach for stochastic modelling of the challenge-broadcasting scenarios in networks using slotted carrier sense multiple access with collision avoidance (CSMA/CA) protocols is proposed in [14]. Authors model the non stationary channel right after issuance of the request by a recursive method and then put forward an approach to find the broadcaster's approximate payoff. The model also supports the cases where the broadcaster is a malicious node with an abnormally high transmission and reception range, which is found in severe flooding attacks. Authors investigate the applications of the model in finding the optimal attack range for the flooding adversaries and deriving a flood-resilient medium access control (MAC) protocol design framework to increase the security of challenge-response protocols. The latter one is especially relevant to mobile networks as it provides a low-cost solution. This paper describes the detailed analysis of the proposed theoretical framework as well as the comprehensive evaluations that have been carried out via simulations.

3.11 MBCP Scheme

A method based on signal strength has been proposed to detect and prevent hello flood attack in [15]. Nodes have been classified as friend and stranger based on the signal strength. Short client puzzles that require less computational power and battery power have been used to check the validity of suspicious nodes. The core idea of hello message based client puzzles scheme (MBCP) is that the larger the number of hello messages sent, the sender will have to solve more difficult puzzles. Hence the difficulty of puzzles for stranger will increase according to number of hello messages sent. Each node has a counter to count the hello message in allotted time and a puzzle generating capability. If any node sends x hello message then it has to solve p^{th} level difficult puzzles.

4. CONCLUSION

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. The security concerns of the sensor network should be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of wireless sensor networks. Hello flood attack is one of the common type of attack in WSNs in which an attacker can control the network as base station is totally cut from the WSN and also affect its routing. In this paper different countermeasures proposed for tackling with hello flood attack are discussed. Novel, efficient, and robust techniques for dealing with hello flood attack is still a great challenge and need of the time.

REFERENCES

[1] Yaya Shen, Sanyang Liu, Zhaohui Zhang, March 2015, Detection of Hello Flood Attack Caused by Malicious Cluster Heads on LEACH Protocol, International Journal of Advancements in Computing Technology (IJACT), Volume 7, Number 2.

[2] Gayatri Devi, Rajeeb Sankar Bal, Nibedita Sahoo, Jan. 2015, Hello Flood Attack Using BAP in Wireless Sensor Network, International Journal of Advanced Engineering Research and Science, Vol. 2, Issue 1, ISSN: 2349-6495.

[3] Mayur S, Ranjith H. D., March 2015, Security Enhancement on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, ISSN (Online): 2319 – 8753, ISSN (Print): 2347 – 6710.

[4] Rawan S. Hassoubah, Suhare M. Solaiman, Manal A. Abdullah, May 2015, Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme, International Journal of Computer and Communication Engineering, Volume 4, Number 3.

[5] Dilpreet Kaur, Rupinderpal Singh, July 2015, Energy level based Hello Flood attack Mitigation on WSN, International Journal of Embedded Systems and Computer Engineering, ISSN 2321 3361.

[6] Jyoti, Ashu Bansal, September 2015, Detection of Hello Flood Attack on Leach Protocol Based on Energy of Attacker Node, International Journal of Innovations & Advancement in Computer Science, Volume 4, ISSN 2347 – 8616.

[7] Shikha Magotra, Krishan Kumar, 2014, Detection of HELLO flood Attack on LEACH Protocol, 2014, IEEE International Advance Computing Conference (IACC).

[8] J. Steffi Agino Priyanka, S. Tephillah and A. M. Balamurugan , January 2014, Attacks and countermeasures in WSN, International Journal of Electronics & Communication, Volume 2, Issue 1, ISSN 23215984.

[9] Satwinder Kaur Saini, Mansi Gupta, May 2014, Detection of Malicious Cluster Head causing Hello Flood Attack in LEACH Protocol in Wireless Sensor Networks, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 5, ISSN 2319 – 4847.

[10] Akhil Dubey, Deepak Meena, Shaili Gaur, January 2014, A Survey in Hello Flood Attack in Wireless Sensor Networks, International Journal of Engineering Research & Technology (IJERT), Vol. 3, Issue 1, ISSN: 2278-0181.

[11] Virendra Pal Singh, Aishwarya S. Anand Ukey, Sweta Jain, January 2013, Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks, International Journal of Computer Applications (0975 – 8887), Volume 62, No.15.

[12] Nusrat Fatema, Remus Brad, December 2013, Attacks and counterattacks on wireless sensor networks, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol. 4, No. 6.

[13] Anup A. Wanjari, Vidya Dhamdhere, December 2014, Evading Flooding Attack in MANET Using Node Authentication, International Journal of Science and Research (IJSR), Volume 3, Issue 12, ISSN (Online): 2319-7064.

[14] Mohammad Sayad Haghighi, Kamal Mohamedpour, Vijay Varadharajan, and Barry G. Quinn, December 2011, Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks, IEEE transactions on information forensics and security, vol. 6, no. 4.

[15] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, May 2010, Hello Flood Attack and its Countermeasures in Wireless Sensor Networks, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, ISSN (Online): 1694-0784, ISSN (Print): 1694-0814.

[16] Venkata C. Giruka, Mukesh Singhal, James Royalty and Srilekha Varanasi, 12 September 2006, Security in wireless sensor networks, Wireless communications and mobile computing 2008, Published online in Wiley Inter Science.

[17] Mohamed Osama Khozium, May 2008, Hello Flood Counter Measure for Wireless Sensor Network, IJCSS: International Journal of Computer Science and Security, Volume 2, Issue 3.

[18] Hamid, A ., Mamun Rashid, Choong Seon Hong, 20-22 Feb. 2006, Defense against lap-top class attacker in wireless sensor network, The 8th International Conference Advanced Communication Technology, Print ISBN: 89-5519-129-4, IEEE.

[19] Waldir Ribeiro Pires J´ unior Thiago H. de Paula Figueiredo Hao Chi Wong, 2004, Malicious Node Detection in Wireless Sensor Networks, 18th International Parallel and Distributed Processing Symposium, Print ISBN: 0-7695-2132-0, Publisher: IEEE.

[20] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, 2010, A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN, International Journal of Computer Science and Information Security, Vol. 7, No. 1.

[21] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, May 2012, A Cross-Layer Based Intrusion Detection Technique for Wireless Networks, The International Arab Journal of Information Technology, Vol. 9, No. 3.

