IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010
ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

Hello Flood Attack and its Countermeasures in Wireless Sensor Networks

Virendra Pal Singh[1], Sweta Jain[2] and Jyoti Singhai[3]

**[1] Department of Computer Science and Engineering, MANIT
Bhopal, M.P., India**

**[2] Department of Computer Science and Engineering, MANIT
Bhopal, M.P., India**

**[3] Department of Electronic and Telecommunication, MANIT
Bhopal, M.P., India**

Abstract

Wireless sensor network have emerged as an important application of the ad-hoc networks paradigm, such as for monitoring physical environment. These sensor networks have limitations of system resources like battery power, communication range and processing capability. Low processing power and wireless connectivity make such networks vulnerable to various types of network attacks. One of them is hello flood attack, in which an adversary, which is not a legal node in the network, can flood hello request to any legitimate node and break the security of WSN. The current solutions for these types of attacks are mainly cryptographic, which suffer from heavy computational complexity. Hence they are less suitable for wireless sensor networks. In this paper a method based on signal strength has been proposed to detect and prevent hello flood attack. 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.

Keywords: *WSN, client puzzles, signal strength.*

1. Introduction

Wireless sensor networks are a particular type of ad hoc network, in which the nodes are 'smart sensors'. Sensors are small devices equipped with advanced sensing functionalities (for monitoring temperature, pressure, acoustics etc.), a small processor, and a short-range wireless transceiver [1]. In this type of network, the sensors exchange information about the environment in order to build a global view of the monitored region. This information is made accessible to the external user through one or more gateway nodes. Sensor networks are expected to bring a breakthrough in the way natural phenomena are observed: the accuracy of the observation will be considerably improved, leading to a better understanding and forecasting of such phenomena. WSN technology enables monitoring of vast and remote geographical region, in such a way that abnormal events can be quickly detected. The cost of sensor nodes varies from hundreds of dollars to a few cents, depending upon their size and complexity. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and transmission range. [1]

2. Attacks on Sensor Networks

Most sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to network attacks as compared to general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories: [2]

2.1 Spoofed, altered, or replayed routing information

One direct attack against a routing protocol is to target the routing information exchanged between nodes by spoofing, altering, or replaying routing information. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency by using this type of attack. [2]

2.2 Selective forwarding

In selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any more. A simple form of this attack is: when a malicious node behaves like a black hole and refuses to forward every packet it receives. However, such an attacker runs the risk that neighboring nodes will conclude that this node has failed and decides to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from few selected nodes can reliably forward the remaining traffic and limit suspicion of its wrongdoing. [2]

2.3 Sinkhole attacks

In a sinkhole attack, the attacker's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a sinkhole with the adversary at the centre like black hole attack in ad hoc networks. Sinkhole attacks typically work by making a compromised node look attractive to surrounding nodes with respect to the routing algorithm. [2]

2.4 The Sybil attack

In Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, multipath routing, and topology maintenance. Replicas, storage partitions and routes believed to be used by disjoint nodes could in actuality be used by one single adversary presenting multiple identities. [2]

2.5 Wormholes

In the wormhole attack, an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part of the network. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. For instance in reactive routing protocols such as AODV or DSR, the attackers can tunnel each route request RREQ packet to another attacker which near to destination node of the RREQ. When the neighbors of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process. [2]

2.6 Hello flood attack

Some routing protocols in WSN require nodes to broadcast hello messages to announce themselves to their neighbors. A node which receives such a message may assume that it is within a radio range of the sender. However in some cases this assumption may be false; sometimes a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every other node in the network that the attacker is its neighbor. For example, an adversary advertising a very high quality route to the base station could cause a large number of nodes in the network to attempt to use this route. But those nodes which are sufficiently far away from the adversary would be sending the packets into oblivion. Hence the network is left in a state of confusion. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are mainly affected by this type of attack. [3]

An attacker does not necessarily need to construct legitimate traffic in order to use the hello flood attack. It can simply re-broadcast overhead packets with enough power to be received by every other node in the network. [3]

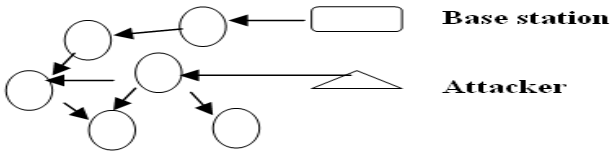

Figure 1(a)

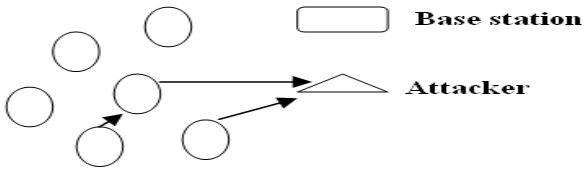

Figure 1(b)

Figure 1(a) shows an attacker broadcasting hello packets with more transmission power than a base station. Figure 1(b) shows that a legitimate node considers attacker as its neighbor and also as an initiator. [3]

3. Countermeasures against Hello Flood Attack

Multi-path multi-base station data forwarding technique is proposed in [3], in which a sensor node maintains number of different secrets (keys) in a multiple tree. Sensor node can forward its sensed data to multiple routes by using these secrets. There are multiple base stations in the network that have control over specific number of nodes and also, there are common means of communication among base stations. Each base station has all the secrets that are shared by all the sensor nodes, covered by it, according to the key assignment protocol. Given the shared secret and the generated new key between two sensor nodes, the process of route setup requires much processing hence is inefficient.

In [4] author suggests that hello flood attack can be counteracted by using "identity verification protocol". This protocol verifies the bi-directionality of a link with encrypted echo-back mechanism, before taking meaningful action based on a message received over that link. This defense mechanism becomes in effective when an attacker has a highly sensitive receiver and a powerful transmitter. If an attacker compromises a node before the feedback message, it can block all its downstream nodes by simply dropping feedback messages. Thus, such an attacker can easily create a wormhole to every node within range. Since the links between these nodes and attacker are bidirectional, the above approach will unlikely be able to locally detect or prevent a "hello flood".

Considering the scarcity of energy resources of sensor nodes, the authors have proposed in [5] a probabilistic based approach, which forces few randomly selected nodes to report to base station about hello requests. The base station then further analyzes the request authenticity.

In [2] a cryptographic technique is used to prevent the hello flood attack. Any two sensors share the same secret key. Every new encryption key is generated on fly during the communication. This phenomenon ensures that only reachable nodes can decrypt and verify the message and hence prevent the adversary from attacking the network. But the main drawback of this approach is that any attacker can spoof its identity and then generate attacks.

In [6] the authors have proposed a security solution framework tailored to the base station for defending against DoS attack. After initial DoS detection, base station challenges clients with cryptographic puzzles to protect itself from different types of attacks. Compared with traditional puzzle schemes, they introduce a novel reputation based client puzzles, which applies a dynamic policy to adjust the puzzle difficulty for each node in terms of node's reputation value. Hence the punishment for malicious nodes becomes more and more pressing without introducing extra unnecessary burden to most normal nodes.

A security mechanism based on signal strength and geographical information is proposed in [7] for detecting malicious nodes that launching hello flood and wormhole attack. The idea is to compare the signal strength of a reception with its expected value, calculated using geographical information and the pre-defined transceiver specification. The detection rate of the solution depends on different parameters such as network density, transmission power multiplier of the malicious node, message checking probability etc.

In [8] a compromised network scenario, when the adversary with sensitive receiver, broadcasts a request like Hello with noticeable power, many nodes hear it at the same time, the nodes try to reply using two way or more way handshake protocol, to this message in order to announce their presence. However the healthy nodes have small transmission and carrier sense ranges. So those located farther than the carrier sense range of each other will try to send the messages back simultaneously. The core idea is to tune 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. This way the adversary will not be able to hear the victims' replies and is obliged to reduce his power and act just like a normal node in the ideal form. This is like a well-known hidden node effect in wireless ad hoc networks.
In fig. 2, node "A" represents the attacker with high transmission range equipped with sensitive receiver while "B", "C" and "D" stand for healthy nodes whose carrier sense ranges are shown by dark circles around them. "b", is a healthy node whose transmission is blocked and backed off due to the transmission of other nodes[8].

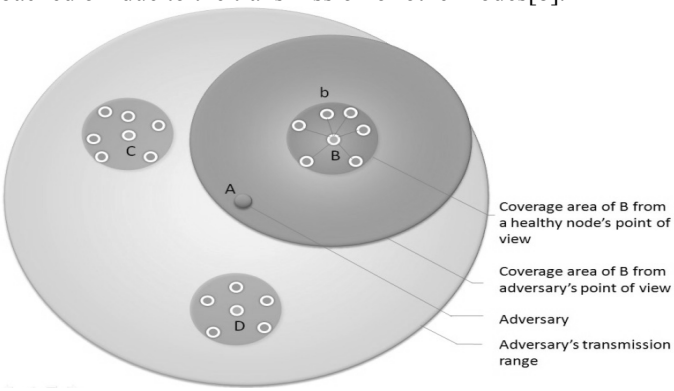

Figure (2)

A threshold based solution is proposed in [9] to defend against flooding attacks in MANET. The mobile nodes use a threshold value to check whether its neighbors are intruders or not. When the number of route request packets broadcasted by a node exceeds the predefined threshold value, it is treated as an intruder and the node stops providing its services to the intruder.

4. Proposed Scheme

In this paper we have proposed a solution for detection of hello flood attack which is based on signal strength and client puzzles method. Signal strength of all sensor nodes is assumed to be same in a radio range. Each node checks the signal strength of the received hello messages with respect to known radio range strength; if they are same then sender node is classified as a "friend" else sender is classified as a "stranger". When any node is classified as a stranger, we try to check its validity using some client puzzles. Dynamic policy technique is used to adjust the difficulty of puzzle level for each node in terms of number of hello messages sent. The more the number of hello message sent by a node, more will be the difficulty of the puzzles it has to solve.

Some primary assumption are-

(1) Communication is within fixed radio range.
(2) All sensor nodes in a fixed radio range have same transmitting and receiving signal strength.
(3) All sensor nodes are homogeneous (same hardware and software, battery power etc.).
(4) Every sensor node knows the fixed signal strength used in its communication range.
(5) A time threshold is used, which denotes the expected time of reply message.
(6) A hello message counter has been used by all sensors to keep the record of number of hello requests received in an allotted time.
Initially signal strength is calculated as two ray propagation model [10]

$$P_r = (P_t * G_t * G_r * H_t^2 * H_r^2)/(d^4 * L) \quad (1)$$

In eq. 1 P_r is received signal power (in watts), P_t is transmission power (in watts), G_t is the transmission antenna gain , G_r is the receiver antenna gain, H_t is the transmitter antenna height(in meter) and H_r 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). A signal is only detected by a receiving node if the received signal power P_r is equal or greater than the received signal power threshold P_{thres}.

When any laptop class attacker sends hello message to a legitimate node in a fixed radio range then the receiving node checks its hello message signal strength, if it is same then requesting node is a legal node of the network; if it differs, it categorizes the sender node as stranger.

Signal strength = Fixed signal strength in radio range=friend
Signal strength > Fixed signal strength in radio range=stranger

If signal strength of received hello message is approximately same but not equal to fixed signal strength then it may be a stranger or a friend. To distinguish between a friend and a stranger we apply a technique based on client puzzles. The puzzles used take less memory and computation power. The node sends some puzzles to the requesting node; if the correct reply comes in allotted time threshold then the node is considered as a friend, if not then it is treated as stranger.

4.1 Algorithm for hello flood prevention

Begin
INPUT: Signal Strength
1: If a node receives hello message from a node S then
2: if Signal strength of received hello message = fixed signal strength in radio range
3: then node s is classified as a friend
4: Node accepts hello message and perform necessary function
5: Else
6: if Signal strength of received hello message ≈ fixed signal strength in radio range
7: then nodes sends puzzle to node S
8: If reply message of correct answers comes in fixed time threshold
9: then Node is classified as friend and accepts the request and performs function
10: Else Signal strength of received message > fixed signal strength in radio range
11: then Node S is classified as stranger and rejects the further requests from S.
12: End

4.2 Client Puzzle Method

Puzzle is basically a number that is used to check the validity of node. The difficulty level of Unicode is based on the left bit. Changes in left bits increase or decrease the

difficulty of puzzles. 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.

For example A, B, C are three nodes that send x1, x2, x3(x1<x2<x3) hello message respectively to node N. N counts the number of hello messages sent and sends puzzles p1, p2, p3 according to increasing order of difficulty level (p1<p2<p3). This means C has to solve more difficult puzzles than B and B has to solve more difficult puzzle than A. So, when any node sends X hello requests then it has to solve p^{th} level difficult puzzles.

$$X \alpha p \quad (2)$$

Equation (2) shows that if the number of hello message increases, then difficulty of puzzles also increases.

4.3 Other solutions for preventing hello flood attacks

Each node checks the number of hello message received in a fixed time interval with the help of a counter. The node then tries to solve these requests in inverse proportionality of the number of incoming hello requests. This means a node which sends less number of hello messages, its request will be solved first and a node which sends more number of hello messages, its request will be solved later.

Another solution for preventing hello flood attacks is based on time threshold. When a node does not receive reply message in a predefined time threshold then it treats the sender to be an attacker and this information is broadcasted to other nodes in the network which contains the attacker node id and the related path.

5. Conclusions

Security plays a crucial role in the proper functioning of wireless sensor networks. Our proposed security framework for hello flood detection via a signal strength and client puzzle method requires less computational power and energy, and hence it is quite suitable for sensor networks. In future we will be implementing the proposed scheme in ns-2 to check its effectiveness in securing sensor networks.

References

[1] Luis E. Palafox, J. Antonio Garcia-Macias,(2008) Security in Wireless Sensor Networks, IGI Global, Chapter 34.

[2] Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.

[3] A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT

[4] Venkata C. Giruka, Mukesh Singhal, James Royalty, Srilekha Varanasi, (2006), Security in wireless networks, Wiley Inter Science

[5] Dr. Moh. Osama K., (2007),Hello flood counter measure for wireless sensor network, International Journal of Computer Science and Security, volume (2) issue (3)

[6] Zhen Cao, Xia Zhou, Maoxing Xu, Zhong Chen, Jianbin Hu, Liyong Tang , (2006), Enhancing Base Station Security against DoS Attacks in Wireless Sensor Networks, IEEE

[7] Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, (2004), Malicious Node Detection in Wireless Sensor Networks, IEEE

[8] Mohammad Sayad Haghighi , Kamal Mohamedpour, (2008), Securing Wireless Sensor Networks against Broadcast Attacks, IEEE

[9] Bo-Cang Peng, Chiu-Kuo Liang, (2006), Prevention Techniques for Flooding Attacks in Ad Hoc Networks, IEEE

[10]T.S.Rappaport,(200), Wireless communication: Principles and practice, Prentice hall 2nd edition.

Virendra Pal Singh. I have completed my B. Tech. degree from Uttar Pradesh Technical University, Lucknow, Uttar Pradesh (India) in Information Technology in the year 2005. Presently I am pursuing M. Tech. (Information Security) from Computer Science Department, Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh, India. My current research interests include Wireless Sensor Network, Network Security and computer networks.

Sweta Jain. I have done B.Tech.(CSE) and M.Tech. (CSE) from Computer Science and Engg. Department of Maulana Azad National Institute of Technology, Bhopal, Madhya Pradesh, India in the year 2004 and 2009 respectively. Presently I am pursuing PhD from the same institute. I am working as an Assisstant Professor in Computer Science & Engineering Department of MANIT, Bhopal, India. My current research interests include Mobile Ad hoc Networks, specifically clustering and security issues in MANETs.

Jyoti Singhai. I have completed B.Tech. (ET&C) from Maulana Azad National Institute of Technolgy, Bhopal in the year 1991. Also completed my M.Tech.(Digital communications) and PhD from the same institute in the year 1997 and 2005 respectively. I am working as an Associate Professor in Electronics and Telecommunications deptt. Of MANIT, Bhopal. My research interests include Mobile Ad hoc Networks and Image processing.