Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 675 – 682

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Design and Simulation of a Blacklisting Technique for Detection of Hello flood Attack on LEACH Protocol

Madhura Mahajan [a,*] , Dr.KTV Reddy [b] , Manita Rajput [c]

[a,b,c] *Department of Electronics and Telecommunication ,*

FCRIT, Vashi ,Navimumbai , India*

Abstract

Wireless sensor networks consist of number of small, low power nodes with limited computational capabilities. In such networks, data is collected from various low power nodes by nodes with higher energy than others, called cluster heads. These cluster heads then send this data to a major node called sink. However, this aggregation is prone to many attacks. This paper intends to present a study of the algorithms, protocols and techniques for secure data aggregation in sensor networks. The Hello flood attack is explained and a novel algorithm for defense against Hello flood attack is proposed and simulated using Matlab.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: secure data aggregation; hello flood attack; blacklisting.

1. Introduction

Wireless sensor networks are typically characterized by a large area called as sensing field, consisting of a number of standalone entities called the sensor nodes, and a base station or sink, to route the sensed information to the outer world [1]. Each of these nodes is restricted in terms of resources such as battery power, memory, computational efficiency, bandwidth etc. These nodes are assigned the task of sensing a single or various parameters respective to the task. Examples are temperature sensing, battlefield surveillance, bridge health monitoring, health care monitoring etc. The process of data gathering needs to be energy efficient in order to preserve the energy and thus increase the life span of the sensing nodes. For this purpose, several data aggregation protocols have been formulated in the past, to summarize the data and reduce the amount of data transmitted [2]. With more emphasis

* Corresponding author. Tel.:9819667310;
*E-mail address:*maha3.madhu@rediffmail.com, ktvreddy@gmail.com,rajputmanita@yahoo.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.086

being given to deploying sensor networks in remote areas to transmit confidential information, the security related issues need to be given equal importance as energy efficiency. Security protocols are designed to be task specific or attack specific. In cluster based aggregation, a more favorable approach is used wherein the entire network is divided into clusters [3]. A cluster head is elected for each cluster and it performs the task of data aggregation among the cluster. Each cluster head then transmits this aggregated information to the base station. In this approach, the number of hops in transmitting the data is reduced, but energy constraint is a restriction. With increase in intrusion of secure networks, a mechanism to protect the network from external attacks needs to be developed. In this paper we have proposed a novel algorithm to detect a Hello flood attack launched on a wireless sensor network, by an external attacker. The rest of the paper is arranged as follows:

Section 2 discusses the attacks on sensor networks and the security requirements. Section 3 gives a detail account of the Hello flood attack and previously proposed solutions to counter the attack. Section 4 gives details of the proposed algorithm. Section 5 shows the simulation results. The future scope is discussed in section 6 and conclusion in section 7.

2. Security in sensor networks

In this section, we discuss the major possible attacks on sensor networks and the security requirements that should be met, in order to avoid these attacks [4], [5], [6], [7].

2.1 Attacks on sensor networks

2.1.1. Denial of Service attack (DoS): It is a form of attack in which a node captured by an external attacker, denies providing service to the network.

2.1.2 Selective Forwarding Attack: In this type of attack, the infected node refuses to forward a particular message. All neighbours are blocked from forwarding the particular message. Then, a target node is selected and messages are flooded to the target node.

2.1.3. Sinkhole Attack: In sinkhole attack, the attacker node acts as a sinkhole by attracting all the traffic to a certain area of the network by compromising a certain node.

2.1.4. Sybil Attack: In Sybil attack, a node assumes multiple identities to confuse other nodes. Sybil attacks mostly possess threat to geographic routing protocols.

2.1.5. Wormhole attack: Here, an attacker builds a virtual tunnel and routes traffic through it, thus bypassing the rest of the nodes.

2.1.6. Hello flood attack: In this attack, a high energy attacker, causes ordinary nodes to lose energy by making them transmit at a large distance with high energy.

2.2 Security requirements of sensor networks [8],[9],[10]

2.2.1. Data confidentiality: Data confidentiality ensures that secrecy of sensed data is never disclosed to unauthorized entities. The standard approach for keeping important data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality.

2.2.2. Data integrity and freshness: Data integrity guarantees that a message being transferred is never corrupted. Data freshness protects data aggregation schemes against replay attacks by ensuring that the transmitted data is recent.

2.2.3. Source authentication: Source authentication enables a sensor node to ensure the identity of the peer node it is communicating with. An adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

2.2.4. Availability: Availability guarantees the survivability of network services against Denial-of-Service (DoS) attacks. Since data aggregators collect the data of a number of sensor nodes and sends the aggregated data to the base station, availability of data aggregators is more important than regular sensor nodes.

3. The Hello Flood attack

3.1 The concept of Hello message

The Hello flood attack is a network layer attack [2]. It targets the routing protocols that require nodes to broadcast the Hello packets to announce their presence to their neighbors. A node that receives such a packet, from a node, assumes that this node is in its own vicinity. A high energy outsider attacker may send Hello packets to the nodes in the field, creating an impression that it is within the radio range of the nodes. Thus, these ordinary nodes make attempts to communicate to the attacker assuming that it is its neighbor, and lose a significantly high amount of energy. The network is left in a state of confusion and chaos. It is hence, necessary to detect the presence of such a high energy attacker and isolate it [11],[12].

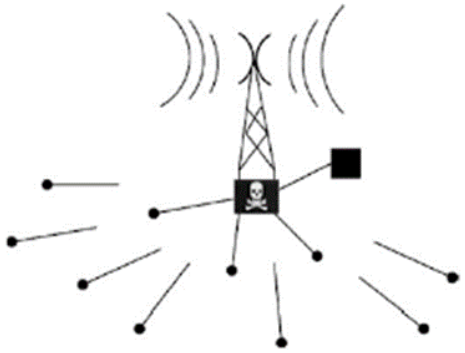

Fig. 1. Hello flood attack in WSN [2]

3.2 Defence against hello flood attack

An extensive survey on protocols and techniques used to detect the hello flood attack has been presented in [9]. The authors have classified these techniques in cryptographic and non-cryptographic approaches. However, due to high energy, time, and memory requirements of the cryptographic methods, we have preferred to discuss the non-cryptographic methods prominently. These are given below:

- In [13], Waldir et al. had proposed a signal strength based detection of Hello flood attack. The mechanism was such that, if a node was suspected to be an adversary, all the surrounding nodes, within its radio range would test the received signal strength (RSS) from that node and, vote for it either as suspicious or non-suspicious. If the suspicious count for a particular node was full, it was marked as suspicious.
- In [14], Virendra et al. have proposed the signal strength based approach for detection of malicious node. However, the disadvantage of this approach is the transmission of test packet if any node is suspected to be malicious. This increases the bit overhead extensively.
- In [15], Magotra et al. have improvised this approach and based the decision of detection of malicious on signal strength as well as distance between the nodes. However, if both these parameters cross a certain threshold, the test packet scenario again comes into picture, thus increasing the overhead.

3.3 The Leach protocol

Since the attack simulation presented in this report, is based on Leach protocol, a brief account of basics of this protocol is being presented. Heinzelman, et.al [1] introduced a hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH arranges the nodes in the network into small clusters and chooses one of them as the cluster-head. Node first senses its target and then sends the relevant information to its cluster-head. Then the cluster head aggregates and compresses the information received from all the nodes and sends it to the base station.

LEACH operations can be divided into two phases:-

1. Setup phase: - During the setup phase, a predetermined fraction of nodes, p, choose themselves as cluster-heads. This is done according to a threshold value, T(n). The threshold value depends upon the desired percentage to become a cluster-head- p, the current round r, and the set of nodes that have not become the cluster-head in the last 1/p rounds, which is denoted by G. The formula is as follows:

$$T(n) = \begin{cases} \frac{p}{1-p*\left(rmod\frac{1}{p}\right)} & \text{if } n \in G \\ 0 & \text{else} \end{cases} \quad (1)$$

2. Steady phase :-During the steady phase, the sensor nodes i.e. the non-cluster head nodes starts sensing data and sends it to their cluster-head according to the TDMA schedule. The cluster-head node, after receiving data from all the member nodes, aggregates it and then sends it to the base-station.

4. The proposed algorithm

We consider that in a wireless sensor network that follows a clustering approach, the non-Cluster Head (CH) nodes along with comparing the RSS of receiving HELLO packet also compare the distance between the non-CH node and elected CH node with the Distance threshold [10]. Thus, only those nodes whose RSS as well as distance are within threshold limits are considered for joining CH. For this, we assume that every node has its location information and during the Setup phase of LEACH protocol, when advertisement of "HELLO" packets is done by CH, it sends its location coordinates also. Now, the nodes receiving HELLO packets from CH calculates the distance between as shown in (2).

Dist = sqrt[sq(xch-x1) + sq(ych-y1)] *(2)*

Here, (x1,y1) are location coordinates of node receiving packet and (xch,ych) are location coordinates of CH sent through advertising HELLO packet. Receiving Node also calculates threshold value for RSS (Rthresh) which corresponds to the radio range of each node in the network and threshold value for distance (Dthresh) which corresponds to the distance covered through radio range. After this, each node decides to join a CH based on RSS of receiving packet & distance calculated. For each non-CH node, If RSS < Rthresh & Dist < Dthresh, then CH Node ='Friend' otherwise the node is classified as suspicious. If all the nodes that are within the radio range of the CH , classify it as suspicious, a variable called 'blacklist' is incremented. Further the node 'blacklisted' as suspicious is then isolated and no more packets are received from that particular node by any other node. Let N be a normal node that receives an advertisement from Cluster head Cl. Here, ! indicates unicast i.e node N decides to join Cl.

Algorithm for simulation is given below:

1. N< = Cl : id (Cl) , join Adv, (xch, ych)
2. N: Dist= sqrt[sq(xch-x1) + sq(ych-y1)]
3. If RSS < Rthresh && if Dist<Dthresh,
   then N(i) ! Cl (j): id (N (i)), id (Cl (j)), join req
4. Else add Cl into suspicious list.
5. If all nodes in radio range of Cl mark it as suspicious, increment variable blacklist.
6. Isolate location of Cl i.e. node at location (xch, ych).

5. Simulations and results

Assumptions: All nodes have complete knowledge of their location. Matlab (version 7.8) simulator has been used for simulation purpose. A square area of 100m × 100m is considered for simulation experiments. The network topology consists of 100 nodes. Initially, the nodes are randomly placed in fixed position. 10% of total number of nodes may have high transmission, receiving and carrier sensing power; one node is a base station. Various parameters taken for simulation and their values are given in Table below

Table 1: Parameters used for simulation

Parameter Used	**Values**
Field Dimensions	100x100 (metres)
No. of nodes in the field	100
Optimal election probability	0.1
ETX & ERX	50 nJ
No. of rounds	100-5000
Message size	4000 bits
Initial energy of each node	0.5 J

5.1. LEACH protocol after simulation:

Figure 2 shows the simulation of basic Leach protocol. The network consists of hundred nodes spread around in 100mx100m area. Depending on Received Signal Strength (RSS), clusters are formed. Each cluster has its own cluster head.

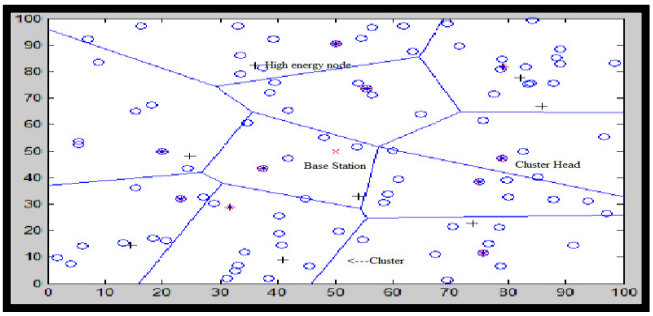

Fig.2. Initial scenario after setup phase

5.2 With one external attacker launching Hello flood attack:

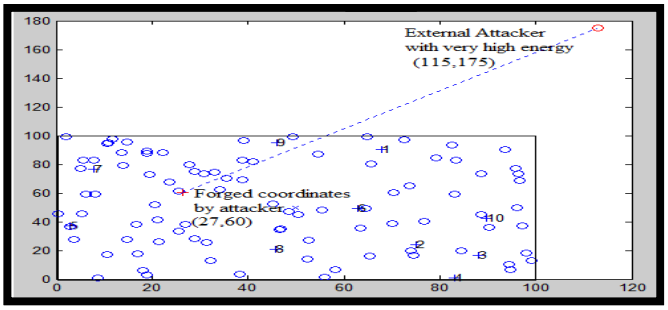

Fig. 3. Single external attacker launching a Hello flood attack

Figure 3 shows how an external attacker at location (115,175) launches a Hello flood attack on the 100x100 m^2 WSN. The red '+' sign indicated the fake co-ordinates that the attacker creates in the WSN to confuse the adjacent nodes. The above mentioned algorithm is followed and the result is: i) the value of the variable 'blacklist' is 1 indicating presence of 1 malicious node. ii) The original co-ordinates of the fake location are displayed correctly.

5.3 Varying the location of external attacker [15]:

Initially, the location co-ordinates of external attacker were chosen such that it was far away from the sensor field (115,175), at a diagonal distance of nearly 95 m. A further analysis by reducing the diagonal distance is performed and the results are tabulated in table 2. From Table 2, it is clear that as the attacker node moves closer to the fields, the nodes lose high amount of energy due to high energy reception .The nodes die out faster. 1000 rounds were simulated for each position.

Table 2. Analysis of dead nodes according to proximity of attacker (single attacker)

Approximate diagonal distance of attacker from the field (meters)	First node dead at round number
95	545
60	443
43	417

5.4 With 2 external attackers launching Hello flood attack:

Figure 4 shows two attackers launching hello flood attack on the WSN.
The results of software simulation were:
i) The value of the variable 'blacklist' is 2 indicating presence of 2 malicious nodes.
ii) The original co-ordinates of the fake location are displayed correctly.

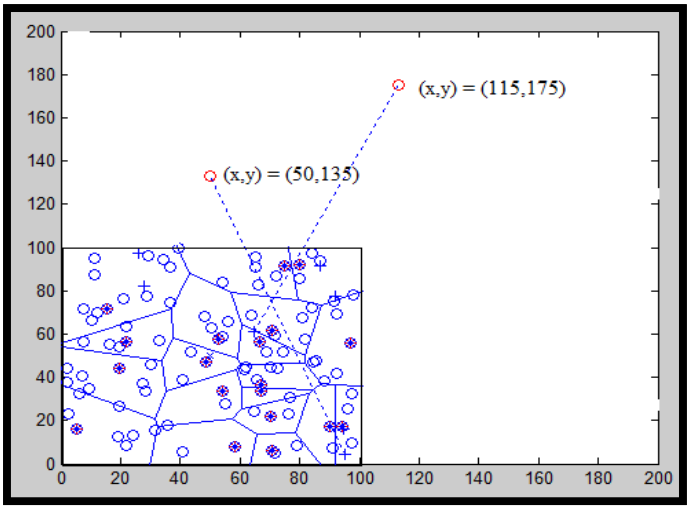

Fig. 4. Two external attackers launching a Hello flood attack

With increase in number of attackers, the total number of packets forwarded and ultimately, the total energy spent in the network increases and thus the statistics of dead nodes changes as per the table shown below:

Table 3. With single external attacker

No. of rounds	First node dead at round no:	Total no. of dead nodes	Simulation time (seconds)
100	-	-	12
200	-	-	24
300	-	-	36
400	-	-	48
500	-	-	60
600	545	43	72
700	551	78	84
800	553	95	96

Table 4. With two external attackers

No. of rounds	First node dead at round no:	Total no. of dead nodes	Simulation time (seconds)
100	-	-	15
200	-	-	30
300	-	-	45
400	-	-	60
500	413	63	75
600	421	79	90
700	428	95	105
800		95	120

6. Future Scope

The proposed algorithm was successful in isolating the external attacker. However, a more detailed analysis of the algorithm needs to be performed. Comparison of the execution time of the algorithm, with the test packet time approach can be conducted and a further estimation of energy efficiency needs to be made.

7. Conclusion

In data aggregation, the general approach is to jointly process the data generated by different sensor nodes while being forwarded toward the base station. This report provides an introduction of the concept of data aggregation and its classification in brief. This is followed by the review of secure data aggregation concept in wireless sensor networks. To give the motivation behind secure data aggregation, first, the security requirements of wireless sensor networks are presented and several techniques and protocols for secure data aggregation are explained in brief. Second, a simulation of Hello flood attack is performed with one and two external attackers and the blacklisting technique to detect the presence of malicious node is analyzed and found to be successful in detection.

References

1. Anjali, Shikha, Mohit Sharma, "Wireless Sensor Networks: Routing Protocols and Security Issues", *Network Security and Systems (JNS2)*, 2012 pp.60-68.
2. S. Ozdemir, Y. Xiao. "Secure data aggregation in wireless sensor networks: A comprehensive overview", Computer Networks, Elsevier 53 (2009) pp. 2022-2037.
3. Aly Mohamed El-Semary and Mohamed Mostafa Abdel-Azim, "New Trends in Secure Routing Protocols for Wireless Sensor Networks", International Journal of Distributed Sensor Networks Volume 2013 (2013), Article ID 802526, 16 pages
4. Rahayu, T.M.; Sang-Gon Lee; Hoon-Jae Lee, "Security analysis of secure data aggregation protocols in wireless sensor networks" 16th International Conference on Advanced Communication Technology (ICACT), 2014 pp.471-474.
5. Priyanka K. Shah and Kajal V. Shukla, "Secure Data aggregation Issues in Wireless Sensor Network: A Survey",Journal of information and communication technologies, volume 2, issue 1, January 2012 pp.10-19
6. Blilat, A, Bouayad, A, El Houda Chaoui, N.; Ghazi, " Wireless sensor network: Security challenges", Network Security and Systems (JNS2), 2012 pp.68-72
7. H. Cam, S. Ozdemir, D. Muthuavinashiappan, and Prashant Nair, "Energy-Efficient security protocol for Wireless Sensor Networks", IEEE VTC Fall 2003 Conf., October 2003, pp. 2981-2984.
8. Satwinder Kaur Saini, Mansi Gupta, "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,Volume 3, May 2014.
9. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:attacks and countermeasures", Ad Hoc Networks, vol. 1, 2003, pp. 293-315
10. Wendi Rabiner Heinzelman, Anantha Ch, and Hari Balakrishnan. "Energy-effcient communication protocol for wireless microsensor networks." pp. 3005-3010.
11. Yaya Shen, Sanyang Liu, Zhaohui Zhang, " 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, March 2015.
12. H. O. Sanli, S. Ozdemir, H. Cam. "SRDA: secure reference-based data aggregation protocol for wireless sensor networks" , in: Proceedings of the IEEE VTC Fall Conference, Los Angeles, CA, 26-29 September 2004, pp. 4650-4654.
13. Waldir Ribeiro Pires Junior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro, "Malicious Node Detection in Wireless Sensor Networks," 18th International Parallel Distributed ProcessingSymposium(IPDPS'04) Vol. 1, pp. 24, 2004.
14. Virendra Pal Aishwarya S. Sweta Jain, "Signal Strength based HELLO Flood Attack Detection and Prevention in Wireless Sensor Networks,"International Journal of Computer Applications (0975 – 8887), Vol. 62,January 2013
15. Shikha Magotra, Krishan Kumar, "Detection of HELLO flood Attack on LEACH Protocol", Advance Computing Conference (IACC), 2014 IEEE International pp:193-198.