Detect and prevent HELLO FLOOD Attack using Centralized technique in WSN

Prabhjot Kaur
Research Scholar
Department of Computer Science And Engineering RIMT University,
Fatehgarh Sahib, Punjab, india
prabhjotkaursehke@gmail.com

Er. Jasmeet Singh Gurm
Assitant Professor
Department of Computer Science And Engineering RIMT University,
Fatehgarh Sahib, Punjab, india
jasmeetsinghgurm@gmail.com

Abstract— In wireless sensor networks, wirelessly nodes communicate with each other. WSN is a very large array of diverse sensor nodes that are interconnected by a communication network . The battery lifetime of nodes in wireless sensor networks have limited, the focus must always be given to conserve their energy so that they can work for longer duration of time. While some of the attacks such as black hole attack or worm hole attack focus on the dropping the data packets which are being transmitted in the network, other attacks such as hello flood attack focus on consuming up the resources of the network like battery power of the nodes etc. These kind of attacks prove to be very harmful to the network. In wireless sensor network, By the use of LEACH protocol nodes are usually clustered in the groups. This technique is applied in most of the cases to conserve the energy of the nodes. Hello flood attack is one common misbehaving activity which targets the cluster head which are formed in the clusters of the wireless sensor network. This study presents the detection and prevention of hello flood attacks by use cenetralized technique in wireless sensor networks.

Keywords- WSN, HELLO Flood Attack , LEACH, Cenetralized technique, clustering,Cluster Head.

I. INTRODUCTION

Recent years have witnessed an increasing interest in using wireless sensor networks (WSNs) in many applications, including environmental monitoring and military field surveillance.In these applications, tiny sensors are deployed and left unattended to continuously report parameters such as temperature, pressure, humidity, light, and chemical activity.

HELLO FLOOD ATTACK

Many protocols which use HELLO packets make the naive assumption that receiving such a packet means the sender is within radio range and is therefore a neighbor. An adversary may use a high-powered transmitter to trick a large area of nodes into believing they are neighbors of that transmitting node. If the adversary falsely broadcasts a superior route to the base station, all of these nodes will attempt transmission to the attacking node, despite many being out of radio range in reality.

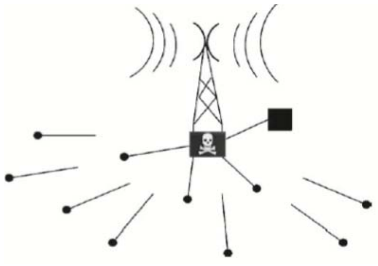

Figure1. HELLO flood attack in WSN

II. LITERATURE SURVEY

In 2007Avinash Srinivasan and jie wu[1] uses metrics with an emphasis on the former and address the Denial-of-Broadcast Message attacks (DoBM) in networks of sensor. A novel treebased model called the k-Parent Flooding Tree Model (k-FTM) and present algorithms for the construction of k-FTM. This model has reliability close to blind flooding and detection rate close to a static tree and also presented various methods with algorithms for constructing k-FTM.

In 2010 Ghossoon M. Waleed[3] used anomaly detection to detect TCP SYN flood attack based on payload and useless area in Hypertext Transfer Protocol (HTTP). The results show that the proposed detection method can save TCP SYN Flood in the network through the payload.

In 2011 Najla Badie Ibraheem Al-Dabagh and Ismael Ali Ali[4] handles the popular DoS attack called TCP-SYN flood attack, and presents the design and implementation of an temporal Immune system for Syn flood Detection, abbreviated by AISD, based on the Dendritic Cell Algorithm (DCA). Results of the experiments showed the precision of intrusion detection process to the ratio of 100%, with a checked response speed.

In 2012 Zhiqiang Chen, Wushau Wen and Da Yu [5] focus in denial of services (DOS) flooding attacks by the use of SIP messages in IMS and provide a detection approach using the non-parameter cumulative sum (CUSUM) algorithm that can efficientienly detect such kind of DOS attacks and also evaluate the performance of proposed algorithm using open IMS core platform.

In 2013 Meenakshi Patel, Sanjey Sharma and Divya Sharma [9] proposed a new method based on AODV behavioral metrics save and check MANET flooding attacks. In this method they used the PDER, CO and PMIR as metrics to prediction of flooding attacks. This method will be implementing on NS-3 test bed and also discuss flood attack and their attack of the network.Used a solution for finding and prevention of Flooding attacks.

In 2014 Shikha Magotra and Krishan Kumar [11] proposed a non-cryptographic solution for HELLO flood attack detection ,in which the no. of times the test packet is transmitted is greatly reduced. 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 (approx.). A new security framework for HELLO Flood detection is implemented and the results are analyzed which proves that it requires less computational power, hence is suitable for sensor networks.In 2015 N. Dharini, Ranjith Balakrishnan and A. Pravin Renold [15] use Conventional hierarchical routing protocols were not created considering security, they are helpless against Denial of Service (DoS) attacks. This scheme will increase the detection ratio thereby achieving energy saving. By effectively detecting and isolating the intruders from the network, the network's lifetime is also enhanced.In 2015 Thenmozhi Ra,KarthikeyanPa,Vijayakumar V b ,Keerthana M a and Amudhavel J c [16] use a technique that are useful in preventing the server from shutdown. The paper focuses on the protection of server and reduces the loss to the organization and also provide the parameters such as Reliability, Fault tolerance, Minimized Response time, Throughput.

In 2015 Pham Thi Ngoc Diep and Chai Kiat Yeo [17] propose a detection scheme for flooding attack that piggybacks on an existing encounter record (ER)-based scheme of detecting blackhole attack. Result shows that flooding adversaries who send too many messages or replicas can be detected. The piggyback is also used to incorporate two schemes into a single robust misbehavior detection system that can detect multiple attacks (blackhole, greyhole and flooding) with little additional overhead.

In 2015 Faouzi Hidoussi, Homero Toral-Cruz proposed a scheme in which a new centralized intrusion detection system is proposed by the authors to detect selective forwarding and black hole attacks in cluster-based wireless sensors networks. The main idea is the use of a centralized detection approach, where the base station decides on potential intrusions based on control packets sent from the cluster heads. The proposed intrusion detection technique is simple and energy efficient, it is thus suitable for sensor nodes with resource constrained. The simulation results have confirmed the expected performance of the proposed IDS in terms of security and energy efficiency.

In 2015 Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos [18] uses an intrusion detection system, called INTI (Intrusion detection of SiNkhole attacks on 6LoWPAN for InterneT of ThIngs), to find sinkhole attacks on the routing services in IoT. Results show the INTI performance and its effectiveness in terms of attack detection rate, number of false positives and negatives and also shows that INTI achives a sinkhole detection rate up to 92% on fixed scenario and 75% in mobile scenario.

III. Existing Scheme

In hello flood attack , the adversary node which is the malicious cluster head has the higher transmission range than the other cluster heads or nodes in the network. The first phase of the clustering protocol begins with the transmission of Hello messages by the cluster heads to the nodes which are in their communication range. The nodes which receive such messages join the cluster head and forms the cluster. If the malicious cluster head transmits Hello messages to the larger portion of the network (since the transmission range is higher) , the normal nodes tend to join it after receiving the messages. Thus a larger sized cluster is formed in such kind of scenario. When the nodes have to send data to the cluster head, their transmission range is less so the data sent by them does not reaches the cluster head and also their radio transmitters have to expend extra amount of energy to send the data packets to the cluster head over a larger distance. This results in the extra consumption of the energy as well as the loss of data packets in the network. Thus Hello flood attack turns out to be very dangerous to the network. The emphasis must be given to detect such kind of attacks so as to conserve the resources of the network.

IV. Proposed Model

In the proposed work we tend to modify the centralized IDS scheme which is based on the misuse detection to detect the malicious cluster head which has the intention of causing the Hello Flood attack in the wireless sensor network.Initially the nodes will be deployed in the network. The cluster head will be selected among the nodes on the basis of the residual energy. This is the remaining amount of the energy in the nodes. The node with highest energy will be selected as the cluster head and then cluster heads will send the Hello messages to the nodes in their communication range. The nodes receiving the messages will join the respective cluster heads then cluster heads will send the control packet to the Base Station using single hop communication. the control packet will contain the ID of the cluster head as well as the ID of its members then Base Station will detect the malicious cluster head on the basis of the number of member nodes present in the cluster. BS will check on the size of the cluster by counting on the number of members a cluster has. If any cluster has members more than average number of the members in the other clusters, then the cluster formation will be cancelled by the base station. The Base Station will detect the cluster head with abnormal cluster size as malicious. It will inform the other cluster heads to not receive any messages from the malicious cluster head. It will inform to restart the clustering process again. The malicious cluster head cannot take part in the clustering process. Once the new cluster has been formed the new cluster head must send the control packet again to the base station informing about its member nodes. The Base Station will again compare the size of the new cluster with the average size. If the condition satisfies then the nodes can start the data aggregation process with the cluster head. At the start of every new round, the newly elected cluster head will send the control packet and the data transmission will start only after Base Station checks the cluster size condition.

V. Conclusion

In the proposed work ,to detect the malicious cluster head which has the intention of causing the Hello Flood attack we have presented the modified centralized IDS scheme in the wireless sensor network. The proposed scheme will be implemented in NS2.35 in future and performance of the network will be analysed against hello flood attacks.

References

[1] Faouzi Hidoussi, Homero Toral-Cruz, “Centralized IDS Based on Misuse Detection for Cluster- Based Wireless Sensors Networks” Springer Science+Business Media New York 2015

[2] Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos, “Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things”,2015

[3] Pham Thi Ngoc Diep and Chai Kiat Yeo, “Detecting Flooding Attack in Delay Tolerant Networks by Piggybacking Encounter Records”,2015

[4] Thenmozhi Ra ,Karthikeyan Pa,Vijayakumar V b ,Keerthana M a and Amudhavel J c , “Backtracking Performance Analysis of Internet Protocol for DDoS Flooding Detection” International Conference on Circuit, Power and Computing Technologies [ICCPCT] , 2015

[5] N. Dharini, Ranjith Balakrishnan and A. Pravin Renold, “Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network” 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 6-8 MAY,2015

[6] Reihaneh Haji Mahdizdeh Zargar, Mohammad Hossein Yaghmaee Moghaddam, “An Entropy-based VoIP Flooding Attacks Detection and Prevention System” 4th international conference on computer and knowledge engeneering(ICCKE)

[7] Shikha Magotra and Krishan Kumar, “Detection of HELLO flood Attack on LEACH Protocol”,2014

[8] Meenakshi Patel, Sanjey Sharma and Divya Sharma, “Detection and Prevention of Flooding Attack Using SVM” International Conference on Communication Systems and Network Technologies,2013

[9] Zhiqiang Chen, Wushau Wen and Da Yu , “Detection SIP Flooding Attacks on IP multimedia subsystem(IMS),,workshoponcomputing,networking and communications,2012

[10] Najla Badie Ibraheem Al-Dabagh and Ismael Ali Ali, “Design and Implementation of Artificial Immune System for Detecting Flooding Attack”,2011

[11] Ghossoon M. Waleed, “TCP SYN Flood Detection based on Payload Analysis” IEEE Student Conference on Research and Development,13-14 DEC,2010

[12] Avinash Srinivasan and jie wu, “A Novel k-Parent Flooding Tree for Secure and Reliable Broadcasting in Sensor Networks” IEEE Communications Society subject matter experts for publication in the ICC,,2007