© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 14 Issue: 03 | April - June 2023
Paper is available at http://www.jrps.in | Email : info@jrps.in
Refereed & Peer Reviewed

Special Edition
NCASIT 2023, 29th April 2023
Department of Computer Engineering,
St. Vincent Pallotti College of Engineering & Technology, Nagpur,

Trust Based Mechanism for the Isolation of Hello Flood Attack in Internet of Things

Kirti1 Anil Sangwan2 Dr. shailender kumar3
1Ph.D Scholar, 2Asst. prof.,3 Associate Professor (CSE), 1Electronics and communication engineering (ECE)
1UIET, Maharshi Dayanand University, Rohtak, Haryana, India. 2ECE, UIET MDU Rohtak, Haryana, 3Delhi Technological University, New Delhi

Abstract

The Internet of Things systems are prone to the attacks as they have ad-hoc and finite resource structure. Internet of Things-based mechanisms can be utilized for managing a large volume of information and assist in services related to industrial and medical applications. Due to this, the IoT attains vulnerability against huge number of attackers and adversaries namely cybercriminals, government, etc. The major goal of PA is to steal the sensitive information such as numbers of credit card numbers, state of data, credential of commercial account and information related to health, by hacking the Internet of Things devices. The hello flood attack is one of malicious activity of IoT which affect network performance to great extent. This attack is triggered by the malicious nodes which can flood unlimited hello packets in the network. The hello flood attack raised situation of denial of service within the network. This research work suggests a trust-based system in which every node obtains a trust value based on their activities. The note that is least trusted will be marked as malicious and get isolated from the network. Network Simulator-2 is applied to deploy the suggested scheme and various metrics such as throughput, packet loss, energy consumption and delay are considered to analyse the results.

Keywords

IoT, Trust Calculation, Hello Flood, ICMP

1. Introduction

IoT is a network that offered diverse services across the conventional Internet to allow efficient communications. In IoT, heterogeneous entities are linked with one another at which the term entity is a kind of a sensor or potentially anything using a service can be obtained. The IoT paradigm has been emerged rapidly as the most spectacular phenomena over previous years. A number of communication protocols are constructed along with the miniaturization of transceivers assists in offering the opportunity of converting an isolated device into a communicating thing. In addition, the mitigation of sizes of computing energy, battery and storage potentials of sensing devices lead to enhance them in considerable manner. Due to these technological developments in the electronics and computer science, various sensing and computing devices based on Internet are maximized which are useful for offering services. Consequently, several potential and possible attacks, that affect the safety of a thing or an individual, are also increased. However, these security requirements are not organized properly [1]. Therefore, it is essential to analyze and tackle these security attacks and privacy issues in comprehensive way. Various secure smart devices are introduced which facilitates numerous services for human beings such to develop automation and monitor the health using diverse things such as temperature sensor, light and clinical sensors that are capable of communicating one another or with a human having a smart device, such as a smart phone. RPL protocol is of a dynamical nature, distance - vector protocol and focuses on discovering the paths among the nodes on the network with the deployment of routing algorithms [2]. The basic function of this protocol is that the data traffic must be directed with least energy utilization and lower loss of packets. Furthermore, the P2P, MP2P and P2MP topology types make the deployment of this protocol. The tree-based topology is utilized in which the data flow is transmitted amid roots and motes. The Rank is a point at which every device is placed within the topology. The motes are located on the basis of their levels whose computation is done using an ‘objective function [3]. Diverse algorithms are utilized in this function for quantifying the route concerning parameters. The quality of life is enhanced and the employment prospects are enlarged using the interaction of objects which are responsible for communicating and transferring the data and are associated with the network through 6LoWPAN. The Internet of Things systems are prone to the attacks as they have ad-hoc and finite resource structure. Internet of Thing-based models have utilized for managing a large volume of information and assist in services related to industrial and medical applications. Due to this, the IoT is attracted by a number of attackers and adversaries namely occasional hackers, cybercriminals, government, etc. The major goal of attacker is to steal the sensitive information such as credential of commercial account and information regarding health, by hacking the Internet of Things devices. In addition, they attempt on compromising the elements of Internet of Things such as edge nodes for activating the intrusion against a third-party entity [4]. An intelligence agency is considered which has affected millions of IoT-based systems and smart devices. The affected systems and devices are utilized by attacker for spying on the interest of an individual or launching an assault extensively. Moreover, the attackers have major goal to attack the smart devices for launching protests against an organization. An attack on the IoT device employs authentication details regarding credentials of user. An attacker is capable of infecting the device with the help of a brute-force technique and controlling it. In general, attacks emphasize on the usability and energy consumed through a node which is associated with a serious data stream. Attack detection systems are employed as safety techniques and play a significant role in an Internet of Things ecosystem. The attacks which are occurred on IoT networks based on RPL concentrated on routing the messages among nodes. In the source-side attacks, the attacker node that harms the sensitive network structure leads to generate energy utilization, and extreme recall density for disturbing the stability of the QoS of the network. Flood attacks lead to damage the network topology through the malicious node so that the nodes can dysfunction. For this, the DIS (DODAG Information Solicitation) messages are transmitted. The DODAG contains some devices which are associated with each other in accordance with a particular topology that consists of tree and mesh topologies [5]. It is an advance kind of DAG at which every node attempt on reaching at a single destination. HF is attack of the Routing Protocol for Low-Power and Lossy Networks. This attack is occurred on a Layer 2 and affected the device while transmitting the data. The Figure 2 represents the attack diagram.

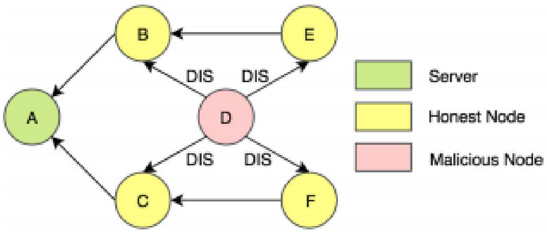

Figure 2. Hello flooding

A node transmits DIS messages to all its neighbours while joining a network. Afterward, their neighbour nodes revert back using DIO messages. Under this attack, several DIS messages are transmitted by a malicious node that often leads to jam the network. The figure represents the transmission of hello packets from a malicious node to nodes in the network. Every node has generated a neighbourhood list for which a packet is transmitted with a Hello message to their neighbours. Any attacker mote available within the network ecosystem focuses on striking network traffic with the transmission of Hello messages to diverse motes and imposing itself to other motes, transmitting the messages which will undergo the server and performing the transmission process [6]. The DODAG has an attacker mote is responsible for maximizing the internet traffic and sending the messages to the motes which are present closer. At the initialization of Hello Flooding attack, the resource usage is maximized for which the data traffic is directed on the neighbouring nodes through itself. The nodes of network ecosystem which contains heavy data traffic consume more power and data losses are occurred. The repair mechanism utilizes to correct the RPL's data flow assists in dealing with this issue. However, the motes available nearer to the attacker are continually affected due to the occurrence of this attack [7]. The attacks occurred on Wireless Sensor Network which is based on Internet of Things and they have different infrastructures of algorithms. Thus, diverse ways are required to prevent or alleviate the intrusions. Moreover, the techniques implemented to tackle one kind of attack are not suitable for others. Various anomaly-based, techniques, ML, DL and NN techniques and classifiers can be adopted to detect and prevent the IoT attacks.

2. Literature Review

Xu Chen, et.al (2021) modelled the communication between an LFA assailant and the network controller like a two people Bayesian game for classifying the conduct of both ends in a precise way [8]. To reveal the logical behaviours of the assailant and the most effective plans of the defender, this work derived the Bayesian Nash Equilibrium (BNE). BNE was a low-cost decision model motivated by the achieved BNEs. The objective of BNE was to enable the protector for security decision making. In addition, this work basically deterred the attack objectives by statistically analyzing the implant of all relevant aspects and existing possible solutions. The results of tests depicted that the introduced approach constantly performed better than the state-of-the art techniques in the context of protectors' services under different level of assaults as well as proved strong to the variations in crucial metrics such as the authentic traffic rate and the traffic cleaning delay.

Apeksha Gajbhiye, et.al (2020) presented a DPLPLN (Detection and Prevention Low Power and Lossy Network) system for securing the message sharing in IoT [9]. To offer defense, this system identified the flooding nature or spam packets of Denial of Service (DoS) assailant in the network. A performance-based comparison was conducted between DPLPLN the RMDD approaches and the DPLPLN outperformed the former approach in the context of overhead and throughput, which were selected as performance parameters. The new system not only detected the spiteful activities of the assailant but also the stopped the assailant to do so. This approach performed routing between the nodes using the RPL routing protocol. After the evaluation of every node's performance, it was observed that new approach showed less percent of loss than the RMDD. In the context of DPLPLsystem, Standard Deviation, Variance and round trip performed remarkably well.

Lucas R. B. Brasilino, et.al (2019) studied the mitigation of DDoS flooding assaults that made IoT gadgets its prey [10]. This work presented a potential framework architecture that used the advantages of a CoAP Accelerator for improving the flexibility of gadgets effectively. The CoAP Accelerator worked collaboratively with CPU of the gadget that had a fundamental part in the processing of CoAP message. System-on-Chip (SoC) Field Programmable Gate Array (FPGA) was used in tis work for the prototyping of the framework. The evaluation depicted the non-exhaustion of the computing assets of the gadget, hence enabled it to work properly when an attack was launched. The future endeavor will discover the pertinency of CoAPAccelerator in other IoT security factors, like identifying both high-pitchedboost of demands and assault signs.

Xu Chen, et.al (2020) stated that classic techniques were not capable enough in the detection and prevention of link flooding attacks [11]. This project modeled the communication between the LFA attacker and the protector as a wide-rangingmethod game with partialknowledge. This work applied space reduction and the split and conquer approach to examine the Nash equilibrium of the subgame on every connection. The main objective here was to unveil thecoherentactions of assailants and the most effective approaches of protectors. In addition, this work soundly expoundedthe way of implementing the local optimal approaches in the web-wide environment. The outcomes of tests demonstrated the efficiency and strength of the introduced decision-making technique to make the LFA defensiveconditions understandable.

S. Ratan Kumar, et.al (2021) proposed a Multi-Core Parallel Processing method for preparing the time series data so that the DDoS flooding assaults could be detected in time [12]. For the early-stage detection of the assault, this work recommended many time series analysis strategies. Generating time series data by means of parallel processing not only saved time but also escalated the assault discovery. To implement the presented strategy, this work used a standard dataset CICDDoS2019 that produced four types of time sequences to identify TCP-based flooding assaults. These sequences were called TCP-SYN, TCP-SYN-ACK, TCP-ACK, and TCP-RST. After enforcement, the results demonstrated that the new approach had the potential to boost the speed by 2.3 times in order to process assault traffic in comparison to successive processing.

Abhishek Verma, et.al (2019) proposed an Ensemble Learning assisted NIDS namely ELNIDS in order to detect routing attacks against RPL network systems [13]. The fourdissimilar ensemble ML classification models namely Boosted Trees, Bagged Trees, Subspace Discriminant and RUS Boosted Trees were enforced in this work. This work used RPL-NIDDS17 dataset containing packet traces of many assaults for the evaluation of the presented ID framework. According to the simulation outcomes, the devised framework was effective. It was noticed that Boosted Trees and Subspace Discriminant approach respectively obtained maximal and minimal accuracy counted as 94.5% and 77.8 %. Likewise, RUS Boosted Trees and ensemble of Subspace Discriminant respectively obtained maximum and minimum Area under ROC rate counted as 98% and 87% amidst of all classification authentication techniques.

Tasnuva Mahjabin, et.al (2020) not only analyzed the DNS flood assaults but also presented two mitigation schemes [14]. This work presented a load dispersedmitigation methodthat served as a rapid escape path of the genuine traffic from the assault domain. This approach basically involved service level modifications which were possible to apply cooperatively between service suppliers. Moreover, this new strategy was pocket friendly than the downtime cost of the domain names due to a DNS flood assault. In addition, this work presented a benign-bot mitigation approach and a business design for the strategy. The benign-bot mitigation method deployed a bot program in DNS local servers of the clients to permit IP addresses of a catalogue of remuneratedcompany websites to keep up in the caches in order to get the easy access to websites even under the downtime of the DNS servers.

3. Research Methodology

This research work suggests a method that is capable of find and isolated spiteful modes from the system. The suggested method is planned on the basis of the monitoring system mode and the rating of nodes. This project makes the deployment of the system and discusses the source and destination nodes placed in the network. The node at the source is responsible of flooding RREQ in the system. The nodes near to the destination have to reply to the source node using the RREP. The hop count and series number are considered for the selection of best path between two ends. The suggested method executes diverse stages in order to isolate the node in the network, which are defined as:

1. The selection of finest route done between two ends of source and destination in accordance to the hop count and sequence number.
2. The route generated will be scrutinized for isolating the spiteful nodes. To test built route, the ICMP messages are flooded in the system through the source node. The nodes after getting ICMP messages move to the observation mode for watching its nearby motes.
3. The adjacent nodes are watched by the motes, the motes that are found spiteful given lowest rating.
4. The motes having lower rating in the system are detected as the malicious nodes. Different colors such as red, green and yellow are assigned to nodes in accordance with their rating values.
5. The Delphi method is utilized to provide location to every node and it makes the deployment of location of node having least rating to isolate it from the network.

Special Edition
NCASIT 2023, 29th April 2023
Department of Computer Engineering,
St. Vincent Pallotti College of Engineering & Technology, Nagpur,

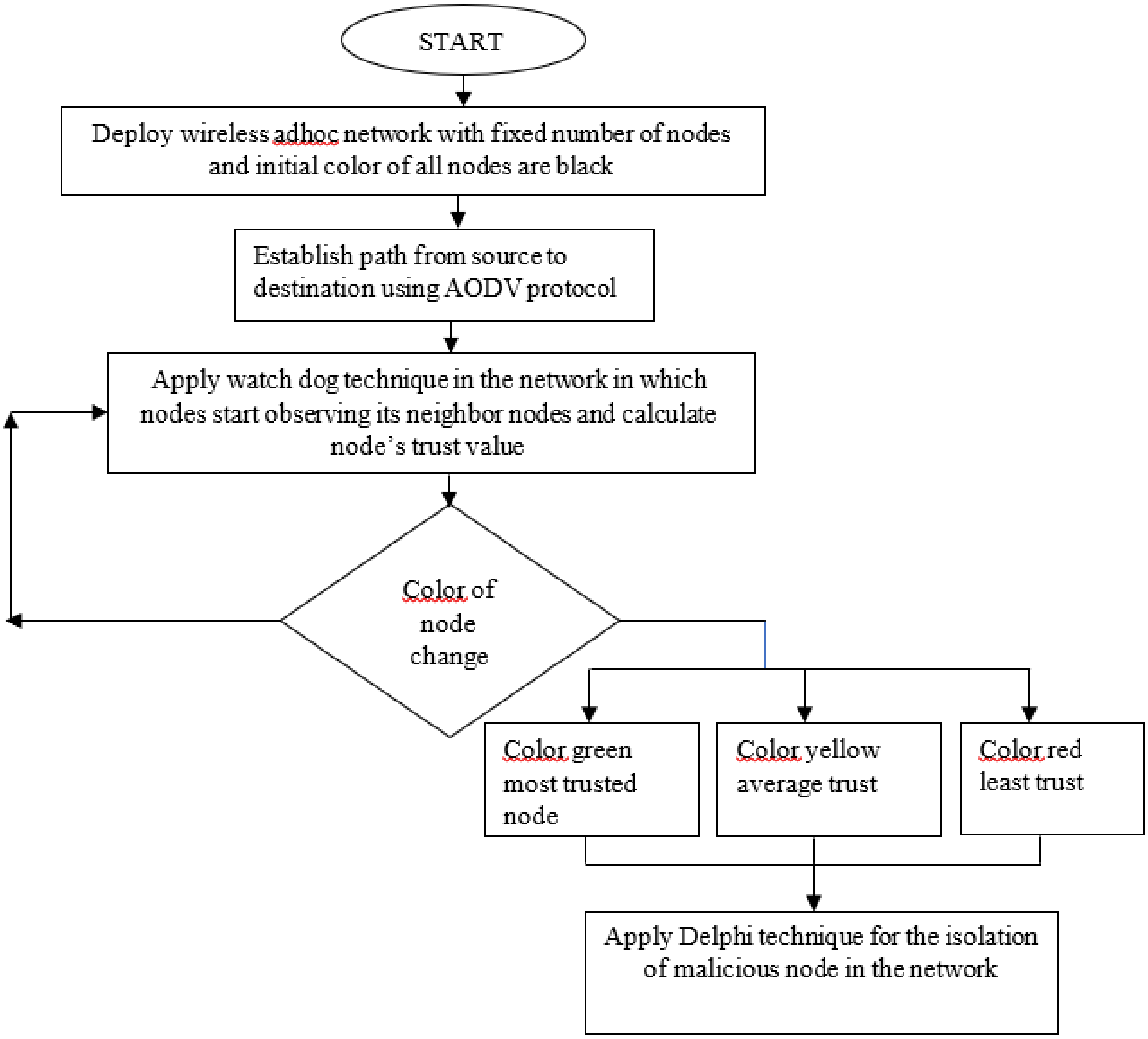
START
Deploy wireless adhoc network with fixed number of nodes and initial color of all nodes are black
Establish path from source to destination using AODV protocol
Apply watch dog technique in the network in which nodes start observing its neighbor nodes and calculate node's trust value
Color of node change
Color green most trusted node
Color yellow average trust
Color red least trust
Apply Delphi technique for the isolation of malicious node in the network

Figure 3: Proposed Flowchart

4. Result and Discussion

IoT network is not controlled by any central entity. In other words, no central controller is present in IoT which results in threats related to the network security. The Hello Flood is the attack which can influence the network productivity in the context of many factors. The various simulation parameters are considered which are described in table 1

Table 1: Simulation Metrics

Simulation Parameter	Value
Number of Nodes	38
Antenna Type	Omi-Directional
Area	800*800 meters
Queue Type	Priority Queue
Queue Size	50
Propagation Model	Two Ray

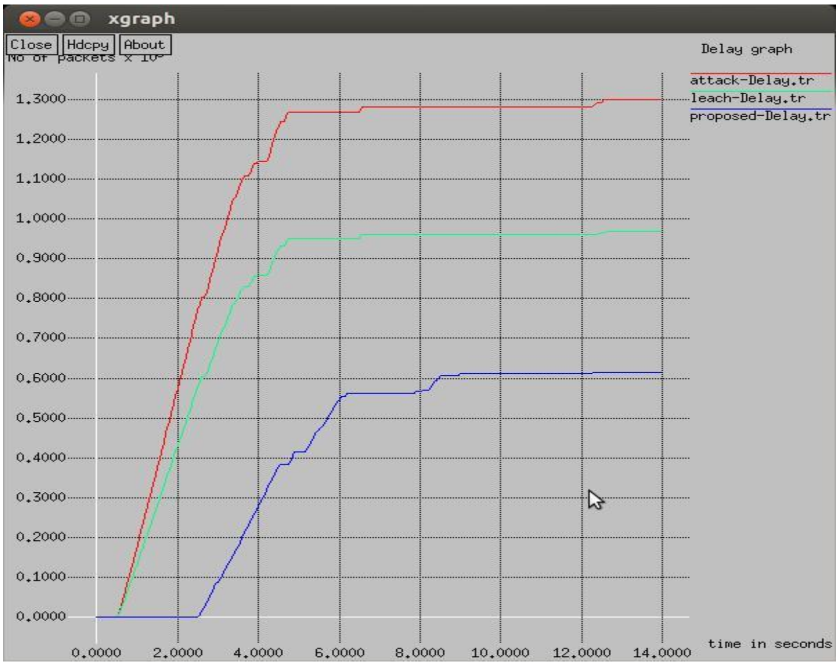

Figure 3: Delay Analysis

Figure 3 displays that the delay in the attack scenario, existing scheme and proposed scheme is compared for the performance analysis. It is noticed that when attack is triggered in the network delay surges at the constant rate. When the developed strategy is implemented for the detection of malicious node delay is reduced at its least level.

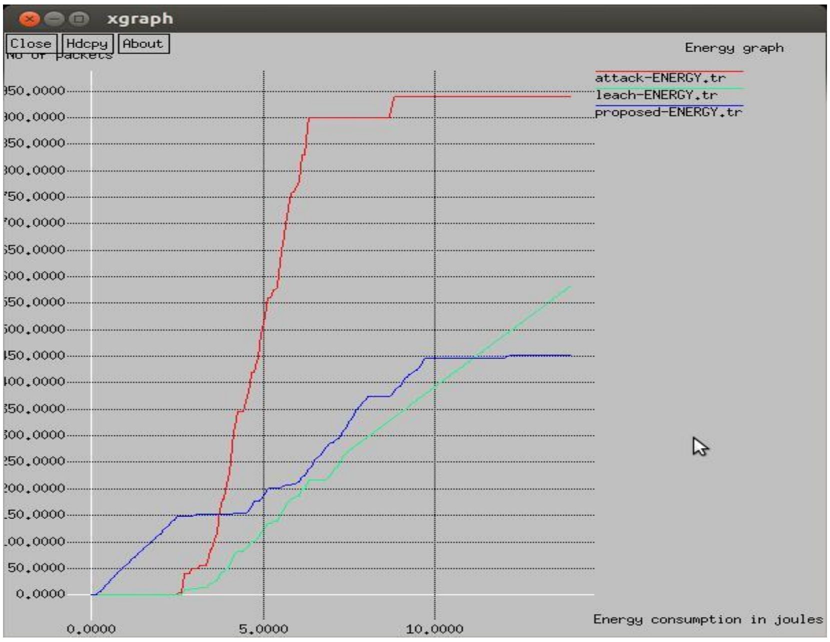

Figure 4:Energy Consumption Analysis

Figure 4 outlines the energy consumption-based comparison between the presented scheme, attack case and existing scheme. As per the analysis, when the attack is eliminated and malicious node is detected from the network, energy consumption is reduced to least level

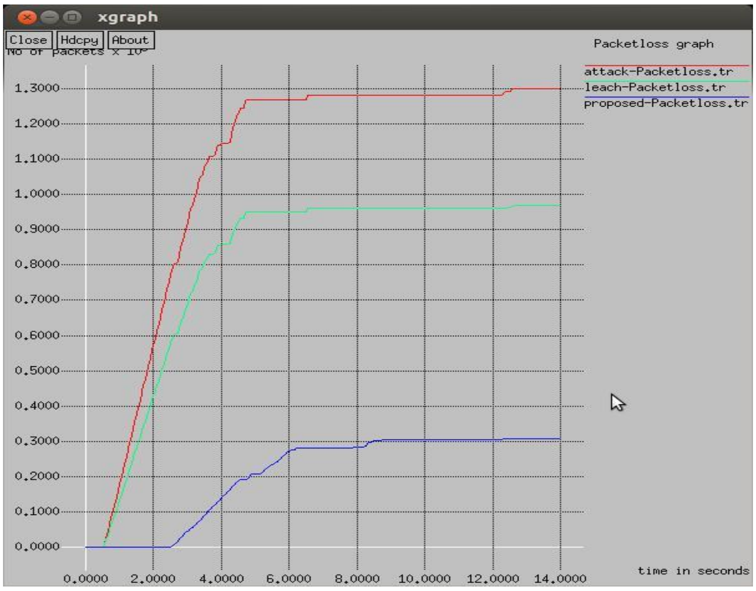

Figure 5: Packet loss Analysis

Figure 5 outlines the packet loss-based comparison between the presented scheme, attack case and existing scheme. The packet loss of proposed scheme is least as compared to other schemes because hello flood attack is detected from the network. In the hello flood attack malicious node flood, the network with unlimited number of hello packets.

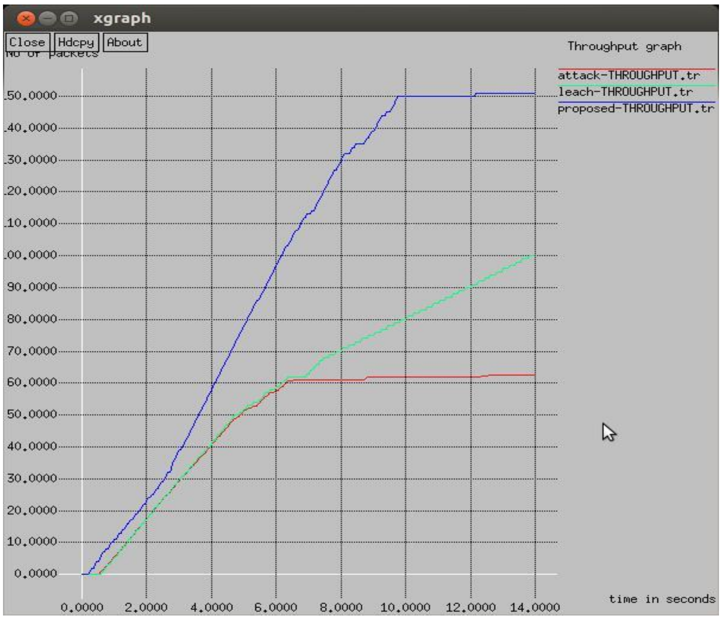

Figure 6: Throughput Analysis

Figure 6 outlines the throughput-based comparison between the presented scheme, attack case and existing scheme. As per the analysis, when the malicious node is detected, the throughput of the network raises at a constant rate.

Conclusion

The internet of things is a distributed network. In this work, spiteful nodes after joining the network activate a variety of active and passive assaults. This research work is based on the detection of hello flood assault from

IOT. In the hello flood attack malicious node flood unlimited amount of hello packets in the set up. Due to flooding of unlimited number of packets it raised situation of denial of service in the network. The trust-based strategy is recommended in this paper for the detection of malicious nodes. In this strategy, all nodes are provided with some trust value based on their activities. The node which maximum trusted is marked with green color, medium level trusted node is marked with yellow color and least trusted node will be marked as red color. The nodes which are marked as red will be declared as the spiteful nodes. The simulation is conducted in NS 2 and outcomes are evaluated in view of delay, energy consumption, packet loss and throughput. The functionality of the proposed scheme is greater as compared to existing strategy for finding spiteful nodes.

References

[1] Kamaldeep, Manisha Malik, Maitreyee Dutta, “Contiki-based mitigation of UDP flooding attacks in the Internet of things”, 2017, International Conference on Computing, Communication and Automation (ICCCA)

[2] BuğraKepçeoğlu, AzharMurzaeva, SercanDemirci, “Performing energy consuming attacks on IoT devices”, 2019, 27th Telecommunications Forum (TELFOR)

[3] LadislavHuraj, Marek Simon, Tibor Horák, “IoT Measuring of UDP-Based Distributed Reflective DoS Attack”, 2018, IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)

[4] Yumeng Cui, Qianli Liu, Kai Zheng, Xin Huang, “Evaluation of Several Denial-of-Service Attack Methods for IoT System”, 2018, 9th International Conference on Information Technology in Medicine and Education (ITME)

[5] S. Santhosh Kumar, K. Kulothungan, “An Anomaly Behavior based Detection and Prevention of DoS Attack in IoT Environment”, 2017, Ninth International Conference on Advanced Computing (ICoAC)

[6] Lucas R. B. Brasilino, Martin Swany, “Mitigating DDoS Flooding Attacks against IoT using Custom Hardware Modules”, 2019, Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)

[7] AkshitGuleria, Evneet Kalra, Kunal Gupta, “Detection and Prevention of DoS Attacks on Network Systems”, 2019, International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)

[8] Xu Chen, Wei Feng, Yantian Luo, Meng Shen, Ning Ge, Xianbin Wang, “Defending Against Link Flooding Attacks in Internet of Things: A Bayesian Game Approach”, 2021, IEEE Internet of Things Journal

[9] ApekshaGajbhiye, Devkant Sen, Abhishek Bhatt, Gaurav Soni, “DPLPLN: Detection and Prevention from Flooding Attack in IoT”, 2020 International Conference on Smart Electronics and Communication (ICOSEC)

[10] Lucas R. B. Brasilino, Martin Swany, “Mitigating DDoS Flooding Attacks against IoT using Custom Hardware Modules”, 2019, Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)

[11] Xu Chen, Wei Feng, Ning Ge, Xianbin Wang, “Defending Link Flooding Attacks under Incomplete Information: A Bayesian Game Approach”, ICC 2020 - 2020 IEEE International Conference on Communications (ICC)

[12] S. Ratan Kumar, V. Valli Kumari, K. V. S. V. N. Raju, “Multi-Core Parallel Processing Technique to Prepare the Time Series Data for the Early Detection of DDoS Flooding Attacks”, 2021, 8th International Conference on Computing for Sustainable Global Development (INDIACom)

[13] Abhishek Verma, Virender Ranga, “ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things”, 2019, 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)

[14] TasnuvaMahjabin, Yang Xiao, Tieshan Li, C. L. Philip Chen, “Load Distributed and Benign-Bot Mitigation Methods for IoT DNS Flood Attacks”, 2020, IEEE Internet of Things Journal, Volume: 7, Issue: 2