Detection and Defense of DDoS Attack for WSN

Prathyusha Reddy Y, Manasa B, Jyothi V, Srikanth V

Abstract: ***Internet of things (IoT) is being widely used in different areas. With the existence of smart and sensing devices at low cost adoption of Internet of Things (IoT) devices has been increased. So they are being used at homes, to predict environmental changes, hospitals, and many more. These IoT devices can be attacked in many ways which results in the great loss of security issues by performing attacks. One of the attacks is Distributed Denial of Service. The Distributed Denial of Services (DDoS) attack is done from a different number of systems which attack one target with large number of requests at a time. So the resources become unavailable to the users. This became our motivation to overcome the issue. To solve this kind of attacks we proposed a framework. In this paper we proposed how the IoT devices can be made secure from the DDoS attack using Wireless Sensor Networks (WSN). The defense mechanism is the one which detects and defense the DDoS attack. In this mechanism the malicious user continuously sends many number of requests to the target, making the resources unavailable to the users. So the wireless sensor detects the attack and defense the attack by using snort rules.***

Index Terms: ***IoT, DDoS, Server, WSN, Malicious User, Attacks, Devices, Snort rules.***

I. INTRODUCTION

The Internet of Things is the system of physical appliances, home devices and different things which are combined with secondary devices like sensors, actuators, hardware and programming which interface the devices for communication. IoT has developed on account of combination of numerous advancements including AI, Deep Learning, Robotics and other related frameworks. IoT can be used extensively for smarter natural disaster management, urban management, health care advancement, monetization and various other industries. It makes human life much easier and also helps the retailers cut unnecessary costs.

IoT comprises of all the web-empowered devices that gather, send and follow up on information they secure from their encompassing surroundings utilizing inserted sensors, processors and correspondence equipment. These devices, are designated "connected" or "smart" devices, can now and then converse with other related gadgets, a procedure called machine-to-machine (M2M) correspondence, and follow up on the data they get from each other.

People can associate with the devices to set them up, give them directions or access the information, however the IOT devices do the greater part of the work alone without human intervention. Their reality has been made conceivable by all the modest portable segments that are accessible now-a-days, just as the constantly online nature of our home and business systems.

The efficiency and profitability that can be picked up by organizations by utilizing IoT are gigantic. Organizations will probably accomplish more through-put in less time. It will assist the business with accomplishing substantially scaled assignments quicker with more prominent precision, checking information investigation and the executives.

The "Internet of Things" (IoT) may sound complex, however in fact, it is a genuinely straightforward idea. Briefly, IOT is the capacity for things that contain inserted innovations to detect, convey, connect, and group up with different things, in this way making a system of physical things which are smart and interact within themselves without any external interference.

Sensors and items with implicit sensors are associated with an Internet of Things stage, which coordinates information from the distinctive gadgets and applies investigation to impart the most significant data to applications worked to address explicit necessities.

Sensors, actuators, register servers, and the correspondence convention and system structure the real establishment of an IoT device. In any case, there are numerous product perspectives that should be considered. To begin with, we need a middleware that can be utilized to interface and deal with these heterogeneous parts. There is no single framework on plan for IoT, which is agreed by. Differing models have been proposed by different researchers and specialists. The most commonly followed architectures are the three and five layer architectures as described below -

The layers in the 3-Layer design are:

(i) **Perception Layer:** The perception layer also called as the physical layer, which has sensors for recognizing and gathering information about the physical amount.

(ii**) Network Layer:** The network layer is responsible for interfacing with other IOT empowered things, organize devices and servers. Its features are in like manner used for transmitting and taking care of sensor data.

(iii) Application Layer: The application layer is accountable for passing on application-unequivocal organizations to the client.

Revised Manuscript Received on May 08, 2019.

Prathyusha Reddy Y, Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India.

Manasa B, Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India.

Jyothi V, Computer Science Engineering, Koneru Lakshmaiah Education Foundation , Guntur, India.

Srikanth V, Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

It describes diverse applications in which the Internet of Things can be passed on, for example, splendid homes, sharp urban networks, and smart prosperity.

The 5-Layer design is only an expansion of the 3-Layer engineering with three included layers barring the system layer. The three layers are:

(i) Transport Layer: The transport layer trades the sensor data gathered from the perception layer to the handling layer and the other path around through frameworks, for instance, 3G, LAN, Bluetooth, RFID, and NFC.

(ii) Processing Layer: The handling layer is generally called the middleware layer. It stores, looks at, and frames enormous proportions of data that begins from the transport layer. It can administer and give a contrasting arrangement of organizations to the lower layers. It uses various developments, for instance, databases, dispersed processing, and tremendous data getting ready modules.

(iii) Business Layer: The business layer manages the whole IoT structure, including applications, business and advantage models, and clients assurance.

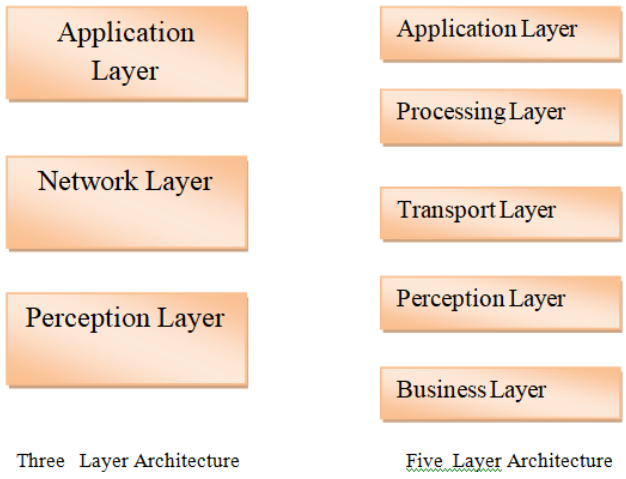


Figure 1: Architecture of IoT

The different kinds of attacks are possible in IoT layers. The different layers where the attacks possible are physical layer, network layer and application layer.

PHYSICAL LAYER ATTACKS:

Physical attacks are focused on equipment devices in the framework.

(i) Node Tampering: In this attack attacker physically modifies the traded off node and can acquire delicate data, for example, encryption key.

(ii) RF Interference on RFIDs: The attacker performs Denial of service attack o radio recurrence signals by sending noise signals. These signs are utilized for RFID's correspondence.

(iii) Node Jamming in WSNs: By utilizing jammer the attacker can bother the remote correspondence. It causes Denial of service attack.

(iv) Malicious Node Injection: In this attack, attacker physically infuses another noxious node between at least two nodes. It at that point alters the information the passes the wrong data to different nodes.

(v) Physical Damage: The attacker physically hurts segments of IoT framework and it results in Denial of service attack.

(vi) Social Engineering: The attacker physically communicates and controls clients of an IoT framework. The attacker gets touchy data to accomplish his objectives.

(vii) Sleep Deprivation Attack: The point of the attacker is to utilize more power that outcomes in closing down of nodes.

(viii) Malicious Code Injection: The foe physically brings a vindictive code into the node of IoT framework. The attacker can deal with IoT framework.

NETWORK LAYER ATTACKS :

These attacks are centered around the system of IoT framework.

(i) Traffic Analysis Attacks: The attacker captures and inspects messages to acquire arrange data.

(ii) RFID Spoofing: A foe parodies RFID signals. At that point it catches the data which is transmitted from a RFID tag. Parodying attacks give wrong data which is by all accounts right and that the framework acknowledges.

(iii) RFID Cloning: In this attack, enemy duplicating information from prior RFID tag to another RFID tag. It doesn't duplicate unique ID of RFID tag. The attacker can embed wrong information or control the information passing through the cloned node.

(iv) RFID Unauthorized Access : If the right validation isn't given in the RFID frameworks, at that point the foe can watch, modify or expel data on nodes.

(v) Sinkhole Attack: In a sinkhole attack a foe bargains a node inside the system and plays out the attack by utilizing this node. The traded off node sends the phony steering data to its neighboring nodes that it has the base separation way to the base station and afterward draws in the rush hour gridlock. It would then be able to modify the information and furthermore drop the parcels.

(vi) Man in the Middle Attack: The attacker over the web catches the correspondence between the two nodes. They acquire the delicate data by listening in.

(vii) Denial of Service: An attacker floods the system with huge traffic so benefits are inaccessible to its proposed clients.

(viii) Routing Information Attack: In this attack, the attacker can make the system complex by mocking, altering or sending directing data. It brings about permitting or dropping bundles, sending incorrectly information or dividing the system.

(ix) Sybil Attack: In this attack, pernicious node that takes the identities of different nodes and goes about as them.

APPLICATION LAYER ATTACKS:

The attacker plays out the attack by utilizing infection, worm, spyware, adware and so forth to take information, deny the services, and so forth.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(i) Phishing Attacks: The attacker acquires the private data like username, passwords by email parodying and by utilizing counterfeit sites.

(ii) Virus, Worms, Trojan steed, Spyware and Aware: A foe can harm the framework by utilizing vindictive code. These codes are spreads through email connections, downloading records from the Internet. The worm can recreate itself with no human activity. We can utilize worm identifier, hostile to infection, firewalls, interruption recognition framework to recognize the infection.

(iii) Malicious Scripts: By infusing pernicious content the attacker can access the framework.

(iv) Denial of Service: The attacker obstructs the clients from the application layer by refusing any assistance.

The presence of IoT worldview over the most recent couple of years has released such huge numbers of dangers and doable attacks against security and protection of IoT articles and people. These dangers lead to hamper the acknowledgment of this worldview on the off chance that they have been left without appropriate countermeasures. Regardless of extraordinary number of security attacks produced on IoT space, there is an absence of standard technique to distinguish and address such attacks.

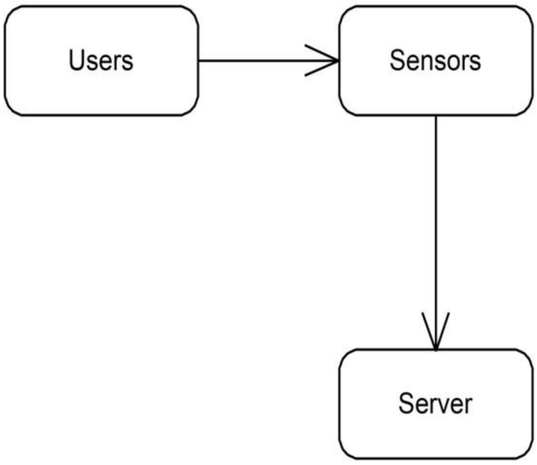


Figure 2: Interface of Proposed Model

In denial of service attack, the attacker will try to make a machine or data inaccessible to its users by interfering with services of a server. DOS is achieved by requesting the machine with many number of requests which in turn overload the server.

In a distributed denial of service attack, the large number of requests target the server from a different targets. It is not just about blocking a single source.

II. LITERATURE REVIEW

The paper "Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning ", presented by Umar Sa'ad,Trung V. Phan, Joongheon Kim, Nhu-Ngoc Dao, Sungrae Cho and Thomas Bauschert introduced a MEC shield Framework for heterogeneous IOT systems which detects DDoS attack by behaviour learning [1]. The paper "A Denial of Service Attack Method for an IoT System", presented by Lulu Liang, Kai Zheng, Qiankun Sheng, Xin Huang introduced a Kali Linux which is used to detect the DDoS attack by connecting the sensor node to the router via LAN.The terminal of Kali Linux is use to launch DoS attack [2]. The paper "Real-time DDoS attack detection based on Complex Event Processing for IoT", presented by Adeilson M. da S. Cardoso, Rafael Fernandes Lopes, Ariel Soares Teles and Fernando B. Veras Magalhaes introduced a DDo detection system and evaluated the performance by running the system on a raspberry PI. It is used to lessen the computational power [3]. The paper "Analysis of IoT Bots against DDOS attack using Machine learning algorithm", presented by K.Gurulakshmi and A.Nesarani introduced an algorithm which is used to classify the traffic against normal and abnormal flow .This algorithm is called support vector machine which is used to identify the DDoS attack based on the flow [4]. The paper "An NTP-based Detection Module for DDoS Attacks on IoT", presented by Tamotsu KAWAMURA, Yasushi HIRANO, Masaru FUKUSHI, Yoshihiko HAMAMOTO and Yusuke FUJITA introduced an algorithm which focus on the system behaviour under DDoS attack and detects it using the information obtained from NTP. This algorithm achieves precision values and it is useful in real time detection on IOT [5]. The paper "An Adaptive Intrusion Detection for the Internet of Things", presented by Eirini Anthi, Lowri Williams and Pete Burnap introduced an Intrusion Detection System (IDS) which is used to monitor the IoT devices. IDS will be able to adapt the environment and detect the malicious activity on the network [6]. The paper "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework", presented by AND KUN ,YANG DA YIN and LIANMING ZHANG, introduced an framework for software-defined Internet of Things and then proposed an algorithm for detecting and mitigate DDoS attacks using the SD-IoT framework.This proposed algorithm detects DDoS attack by using SD-IOT framework [7]. The paper "Lightweight Bloom-filter based DDoS Mitigation for Information-Centric IoT", presented by Gang Liu, Bohao Feng, Wei Quan , Shen Hongke Zhang Nan Cheng, and Xuemin introduced BLAM mechanism to decrease the detecting memory cost. They implemented BLAM in a realistic network tested to analyze its performance [8]. The paper "Mitigating IoT-based Cyberattacks on the Smart Grid" ,presented by Suleyman Uludagpropose , Yasin Yilmaz proposed a scalable mitigation approach called Minimally Invasive Attack Mitigation via Detection Isolation and Localization , under a hierarchical infrastructure of data [9]. The paper "Dynamic Attack Detection and Mitigation in IoT using SDN", presented by Suman Sankar Bhunia, Mohan Gurusamy proposed Software Defined Networking (SDN) framework to detect attacks and abnormal behaviors as quick as possible and defense as appropriate. Machine Learning algorithm is implemented at the SDN controller to learn and monitor the nature of IoT devices over time.

They conducted this experiment on Mininet emulator. This framework is capable to detect attacks in 98% cases [10]. Sensor systems are exceedingly dispersed systems of little, lightweight remote nodes, conveyed in extensive numbers to screen the condition or framework by the estimation of physical parameters, for example, temperature, weight, or relative dampness. The sensors likewise can transmit and advance detecting information to the base station. Most present day WSNs are bi-directional, empowering two-way correspondence, which could gather detecting information from sensors to the base station just as exchange directions from base station to end sensors.

They are many possible attacks on this WSN. They are:

- Attacks on network availability
- Attacks on secrecy and authentication
- Silent attack on service integrity

Attacks on network availability:

Modifying the customary encryption calculations to fit inside the remote sensor organize is not free, and will present some additional expenses. A few methodologies alter the code to reuse however much code as could reasonably be expected. A few methodologies attempt to make utilization of extra correspondence to accomplish a similar objective. Furthermore, a few methodologies constrain severe impediments on the information get to, or propose an inadmissible plan, (for example, an essential issue conspire) so as to disentangle the calculation. In any case, every one of these methodologies debilitate the accessibility of a sensor and sensor arrange for the accompanying reasons :
• Additional calculation expends extra vitality. On the off chance that no more vitality exists, the information will never again be accessible.
• Additional correspondence likewise expends more vitality. Furthermore, as correspondence increments so too does the opportunity of bringing about a correspondence struggle.
• A solitary point disappointment will be presented if utilizing the main issue conspire. This extraordinarily compromises the accessibility of the system. The necessity of security influences the activity of the system, yet in addition is profoundly essential in keeping up the accessibility of the entire system. The attacks on accessibility of WSN are regularly alluded to as DoS attack. DoS go under this attack which influences distinctive layers of WSNs.

III. EXISTING ALGORITHMS

From the past systems, implementation and analysis of a DDOS mechanism is not integrated with snort rules. In DDOS attack, many number of packets are forwarded. The attacker sends the malicious packets to the server making its resources unavailable to the users. The disadvantage with the existing system is that the defense cannot be done resulting in the resource unavailability.

IV. PROPOSED WORK

In this paper, the network undergoes an attack and we are unable to access the resources. So, in order to make the resources available to the users, we proposed a system which defense the attack. Whenever the user sends large number of request to the server it stops working and does not respond back. With the help of proposed system even when more number of requests are sent to the server it responds to each and every genuine request which makes the resources available to the user. In this framework we considered 5 user nodes, 10 server nodes, 8 sensor nodes. The user node continuously sends request to server node. The server node takes the requests of the user and responds. The sensor node is used to detect the attack happened at server side.

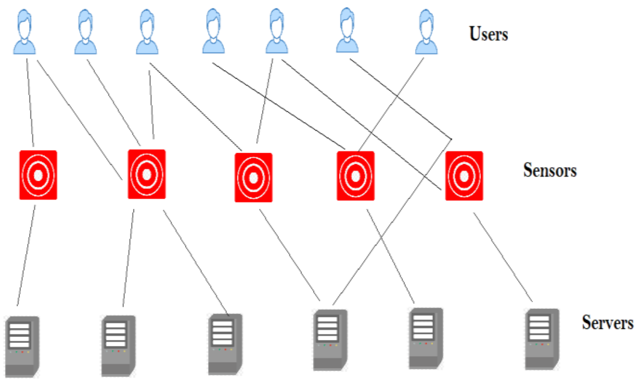


Figure 3: Network Setup

Step-1: Start
Step-2: Server started successfully.
Step-3: Running and listening on port: 11111
Step-4: Deploy Network
Step-5: No of users are activated
Step-6: According to Snort rule-1, Initialize all the IP address and port numbers.
Step-7: Launch all the servers.
Step-8: Launch all the Users.
Step-9: Perform the device actions by the user.
Step-10: Consider the threshold value. It is calculated based on the number of requests sent per sec. If the number of requests sent per sec to the server is greater than 10, it is considered as low attack.
Step-11: If the number of requests sent per sec is greater than 20, it is considered as high attack.
Step-12: Based on the rules, whenever the attack happens the proposed system recovers from it and respond back to the server.
Step-13: Display the attack and defense time.
Step-14: Exit.

V. RESULTS

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

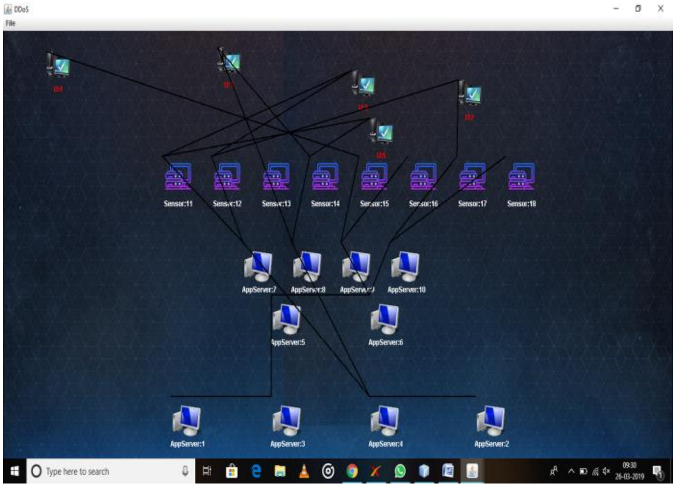
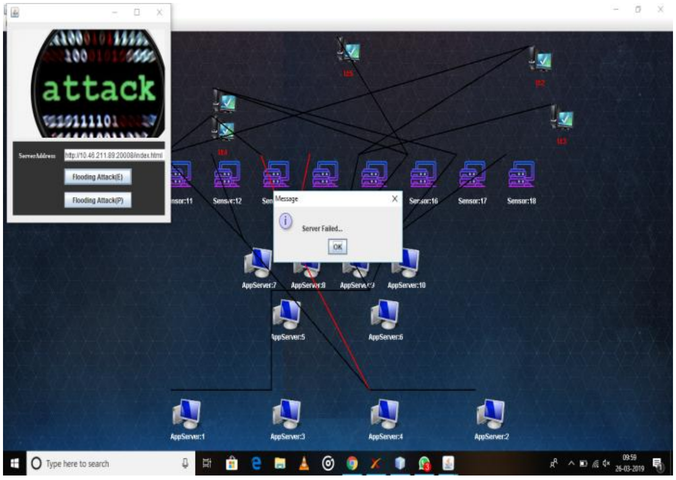


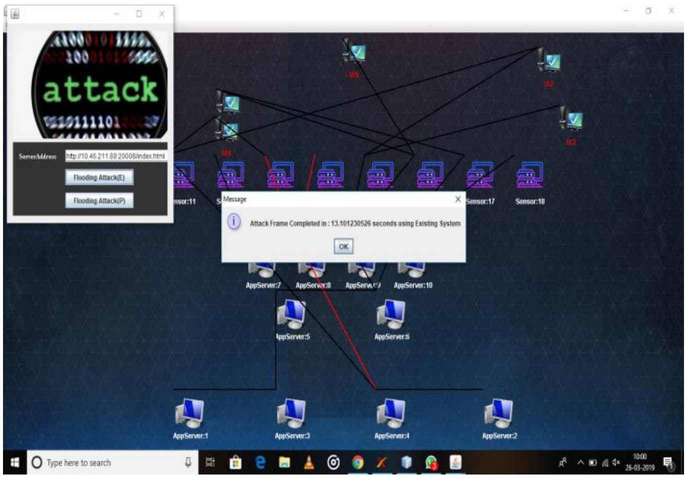
Figure 4: Network Setup



http://10.46.211.89:20008/index.html

Server Failed...

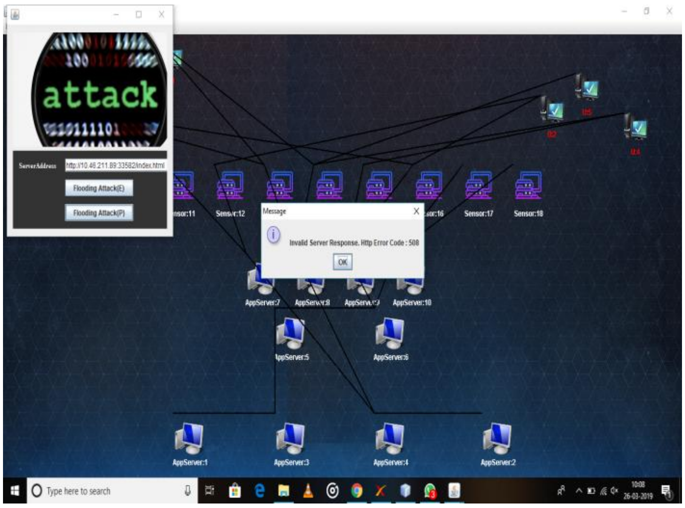
Figure 5: DDoS Attack using Existing System



http://10.46.211.89:20008/index.html

Attack Frame Completed in : 13.101230526 seconds using Existing System

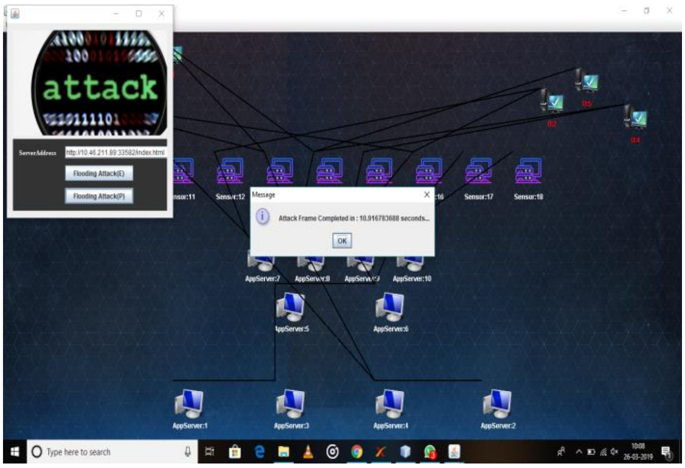
Figure 6: Time taken for Attack using Existing System



http://10.46.211.89:33582/index.html

Invalid Server Response. Http Error Code : 508

Figure 7: DDoS Attack using Proposed System



http://10.46.211.89:33582/index.html

Attack Frame Completed in : 10.916783688 seconds...

Figure 8: DDoS Attack prevention using Snort Rules

This project is implemented by using java, jdk 1.8 and all the simulations are shows by using java. The comparative results shown based on the time for attack and defense.
The comparison is done between the attack and defense for the existing and proposed system.

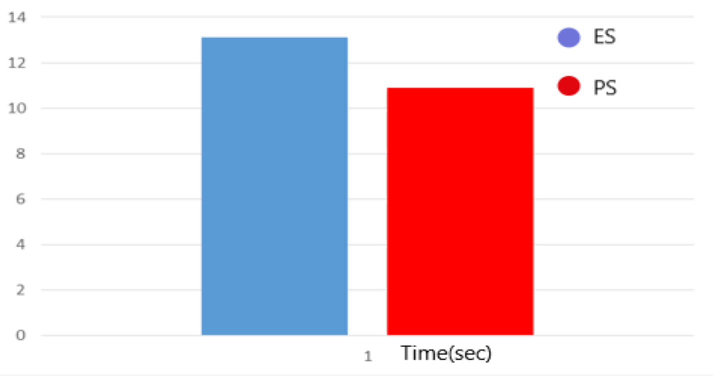


Figure 9: Time comparison between Existing System and Proposed System

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

VI. CONCLUSION

In this paper, the proposed system detected and defended DDoS attack using the IoT wireless sensors and the performance of the proposed system is shown. The proposed system performs well by comparing the attacks time frames with the existing system. The proposed system reduces the attack time frame by using the snort rules. The future scope of the proposed system it can be implemented in real time network.

REFERENCES

1. Securing Heterogeneous IoT with Intelligent DDoS Attack Behavior Learning Nhu-Ngoc Dao, Trung V. Phan, Umar Sa'ad, Joongheon Kim, Thomas Bauschert, and Sungrae Cho.
2. Liang, L., Zheng, K., Sheng, Q., & Huang, X. (2016). A Denial of Service Attack Method for an IoT System. 2016 8th International Conference on Information Technology in Medicine and Education (ITME).doi:10.1109/itme.2016.0087.
3. Marques da Silva Cardoso, A., Fernandes Lopes, R., Soares Teles, A., & Benedito Veras Magalhaes, F. (2018). Poster Abstract: Real-Time DDoS Detection Based on Complex Event Processing for IoT. 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI).doi:10.1109/iotdi.2018.00036.
4. Gurulakshmi, K., & Nesarani, A. (2018). Analysis of IoT Bots Against DDOS Attack Using Machine Learning Algorithm. 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI).doi:10.1109/icoei.2018.8553896.
5. Kawamura, T., Fukushi, M., Hirano, Y., Fujita, Y., & Hamamoto, Y. (2017). An NTP-based detection module for DDoS attacks on IoT. 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW). doi:10.1109/icce-china.2017.7990972.
6. Anthi, E., Williams, L., & Burnap, P. (2018). Pulse: an adaptive intrusion detection for the internet of things. Living in the Internet of Things: Cybersecurity of the IoT - 2018 .doi:10.1049/cp.2018.0035.
7. Yin, D., Zhang, L., & Yang, K. (2018). A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework. IEEE Access, 6, 24694–24705.doi:10.1109/access.2018.2831284.
8. Lightweight Bloom-filter based DDoS Mitigation for Information-Centric IoT Gang Liu , Wei Quan , Nan Cheng , Bohao Feng , Hongke Zhang , Xuemin (Sherman) Shen, School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China School of Telecommunication Engineering, Xidian University, Xi'an, China.
9. Yilmaz, Y., & Uludag, S. (2017). Mitigating IoT-based Cyberattacks on the Smart Grid. 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). doi:10.1109/icmla.2017.0-109.
10. Bhunia, S. S., & Gurusamy, M. (2017). Dynamic attack detection and mitigation in IoT using SDN. 2017 27th International Telecommunication Networks and Applications Conference (ITNAC).doi:10.1109/atnac.2017.8215418.
11. Sonar K. and Upadhyay H., "An Approach to Secure Internet of Things Against DDoS." Proceedings of International Conference on ICT for Sustainable Development. Springer Singapore, 2016.
12. Hsiao-Chung LIN, and WANG Ping, "Implementation of an SDN-based Security Defense Mechanism Against DDoS Attacks". DEStech Transactions on Economics and Management, 2016.
13. O. Depren, M. Topallar, E. Anarim, M. K. Ciliz,"An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks", Expert Systems with Applications, vol. 29, pp. 713–722, 2005.
14. M. De Donno, N. Dragoni, A. Giaretta, and A.Spognardi, "A Taxonomy of Distributed Denial of Service
15. Attacks," in Proceedings of the International Conference on Information Society (i-Society'17). IEEE, 2017.
16. O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," 29th IEEE WAINA Conference, pp. 688–693, 2015.