ISSN 2347 - 3983
Volume 8. No. 9, September 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter230892020.pdf
https://doi.org/10.30534/ijeter/2020/230892020

Ensemble DOS Attack Detection with IoT Integration Algorithm

Hanumat Prasad Alahari[1] Suresh BabuYalavarthi[2],
[1]Research Scholar, Department of CSE, AcharyaNagarjuna University, Guntur,
hanuma.alahari@gmail.com
[2]Professor, Department of CS, J.K.C. College, Guntur, Andhra Pradesh, India, yalavarthi_s@yahoo.com

ABSTRACT

DDoS attacks integrating with Internet of things (IOT) become very popular in present days. Many researchers attracted by the IOT because of its widespread of applications. The behavior of IOT device is very easy to access and heterogeneous this will connect to various devices that lead to several attacks and threats in the IoT devices. The existing system Constrained Application Protocol (CoAP) is implemented for better efficiency but the few issues are identified. A Distributed Denial of Service (DDoS) attack is a task that developed to attack the web servers, disturbing infrastructure of the network, and all the layers of applications are affected with traffic and heavy files from multiple resources, this will make all the websites and applications to become slow or temporarily unavailable. In this paper, the Enhanced Attack Detection (EAD) is developed to prevent the DOS and DDOS attack of application and 6LoWPAN network layer of IoT. Parameters such as reduced delay, reduced number of packets lost, dynamic routing are calculated. Results show the performance of the proposed system.

Key words: CoAP, DDoS, EAD, 6LoWPAN.

1. INTRODUCTION

From the past few years a rapid growth in the Internet of Things (IOT) field and this innovation is separated as exponential. From the recent years IOT becomes major player. Various new technologies are having more issues when these are at the starting stage for research and development which is more concentrating on providing security for all the new technologies. The infrastructure is developed in the IOT to provide the security from the various DOS attacks.

IOT is the huge network of that are having very compatible and these are connected to each other and internet is used to send data from various sources and provide services without any involvement of human [2]. In the past, it is defined as the all the devices are interconnected and all these are finds differently in the network and these are compatible with communicating each other without having any human involvement [3]. This allows the users to communicate, provide and cooperate to things that are not involved in the process, that are not traditional networks. These networks consider the overall networks that are mainly because of the avoiding, huge scope, and capability features [4].

The structures in IoT help to access the authorized user who requires the usage of IoT devices. This users are called as helpers and these will handles the Sybil, answer, emulate attack [5]. In the different layers the security issues are occur at the different layers. In specific process of IoT security, the proposals are considered [6]. Many smart devices that are having the sensitive data which will be protected with security shield. Further, this should get the security structure and this should have the access control. While sharing the sensitive information security have to give assurance from the attacks. Here there is a need of encryption and decryption to help security. Many of the cryptographic systems are developed to secure the data. Various private and public keys are used to give security to devices related in the IoT network [8].

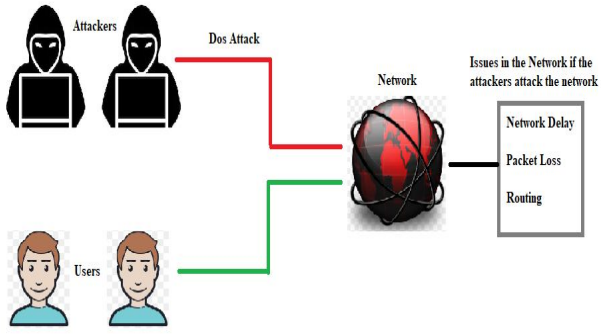

Figure 1: dos attack for the network

2. LITERATURE SURVEY

In the past, many surveys are done on DDos Attacks that are occurred in various networks. Among those most of the attacks are typical DDos and the types are used for the defence mechanisms. Huge data is available in various survey papers that solves the issues with DDoS attacks and these systems effectively help to develop the model to prevent the DDoS attack in IoT. The author Zargar et al. [9] discussed on various types of DDoS flooding attacks are explained that includes the botnet-based DDoS attacks.

Recently many of the DDoS attacks that are new attacking with different malware. It is very important to know about the latest malware attacks that are identified from many references and also it is important to prevent the new malware attacks. To do this, the new powerful prevention mechanism is required. From the various survey, it is understood that the data about the DDoS attacks that should be covered.

The Constrained Application Protocol (CoAP) [10] is the particularly a data transfer protocol which is used in the network that consists of nodes within the IoT. To overcome the energy issues the 6LoWPAN technique that is obtain from the web protocol that will applicable to tiny low power devices with very less processing capabilities which helps in participation of Things.

3. ARCHITECTURE OF IOT

IoT is most widely used by many systems to increase the performance of the applications. Many advantages are there to integrate the IOT to the different types of applications. It is very important to all the devices to operate with the better process for communication [12]. For the IoT infrastructure the protocols such as IPv6, 802.15.4, 6LoWPAN etc are designed [13].

3.1 Delay of Network for Read Request (N1) in 6LowPan Network

- In this case, the server received the request from the client sends a request to the server.
- To find weather the request is started or not, if the request passes the Exinda, the time-clock saves the starting of the request (t1).
- From the exinda, if the final request passed, the time at the clock is (t2)=t2-t1= the time that is taken for client request is passed through Exinda.
- Finally, the complete client request is received by the server.

3.2 Server Delay for Read Request (S)

- Server takes sometime after receiving the request from the client to check this request. Thus it is called as server delay (S).
- Delay of Network for Read Response (N2) 6LowPan Network
- The response to the client is sent by the server and this is in the form of packets.
- To find weather the response is started or not, if the response passes the Exinda, the time-clock saves the starting time of the response (t3).
- From the exinda, if the final request passed, the time at the clock is (t4) = t4-t3= the time that is taken for client request is passed through Exinda.
- Finally, the client receives the data received by the server.

3.3 Total Time for Read Transaction 6LowPan Network

To read the total transaction time is calculated as

$$\text{Transaction time} = N_1 + S + N_2 \text{ where:}$$

$$N_1 = \frac{1}{2}\text{RTTClient} + (t_2 - t_1) + \frac{1}{2}\text{RTTserver} \quad (\text{Equation} - 1)$$

$$S = (t_3 - t_2) - \text{RTTserver} \quad (\text{Equation} - 2)$$

$$N_2 = \tfrac{1}{2}\text{RTTserver} + (t_4 - t_3) + \tfrac{1}{2}\text{RTTClient}$$

(Equation-3_

3.4 Packet Loss in 6LowPan Network

Packet loss is most widely done in every network. This occurs when the data packets one or more transmitted successfully but they fail to reach the destination. Based on the various factors the packet loss is occurs such as congestion in the network, network components that are having faults such as drivers, or corrupted packets within the transmission. If the packet loss occurs in data transmission, the following issues are identified.

- During VoIP communications the gaps occur in audio.
- When the video streaming the performance issues may occur.

To overcome these issues, the transmission of data to the destination to complete requests successfully. The efficiency of the network is based on the packets flow.

$$\text{Efficiency} = 100\% * (\text{transferred} - \text{retransmitted}) / \text{transferred} \text{---------- Equation-4}$$

$$\text{Network Loss} = 100 - \text{Efficiency} \text{------ Equation-5}$$

4. DISTANCE VECTOR ROUTING IN 6LOWPAN NETWORK (DVRN)

In this 6LowPan Network the Distance Vector Algorithm (DVA) is integrated because of various features such as iterative, asynchronous and distributed. This will distribute to every node that receives the data from the neighbors, this makes computation and then transfers the output back to the neighbors.

The process of this algorithm is iterative and this will continuous until the condition satisfies such as data exchange between the neighbors.

- In the lock step, it does not require any of the nodes operations.
- It is dynamic algorithm.
- Distance table is maintained for every router known as Vector.

5. DISTANCE VECTOR ROUTING STEPS

The nodes x and y are present and let dx(y) is the least cost path. This is also called as Bellman-Ford equation,

$$dx(y) = \min v\{c(x,v) + dv(y)\} \text{—Equation (6)}$$

the above Equation (6) is selected for x neighbors.

From the x to v the cost will be c(x,v)+dv(y). Very less cost from x to y is the base of c(x,v)+dv(y) assumed control over all neighbors.

The routing data which the node x contains:

- For each neighbor v, the cost c(x,v) is the route cost from x to clearly associated neighbor, v.
- The detachment vector x, i.e., Dx = [Dx(y) : y in N], containing its cost to all complaints, y, in N.
- The partition vector of all of its neighbors, i.e., Dv = [Dv(y) : y in N] for each neighbor v of x.

DVR is an unconventional computation where hub x sends the copy of its detachment vector to all of its neighbors. Exactly when center point x gets the new division vector from one of its neighboring vector, v, it saves the partition vector of v and from one of its neighboring vector, v, it spares the separation vector of v and utilizations the Bellman-Ford condition to refresh its own separation vector. The condition is given underneath:

dx(y) = minv{ c(x,v) + dv(y)} for every hub y in N

6. ENHANCED ATTACK DETECTION (EAD)

EAD is the proposed algorithm which is used to detect the attacks and improves the performance of the network stability and efficiency. Various parameters are calculated by using this Equations 1-6.

Step-1 Initialize network.

Step-2 Nodes N_1, N_2, N_3……N_N.

Step-3 Start transmission.

Initial time to start transmission t=5 sec.

If (t>5)

Message (“Start Transmission”);

Else

Message (“Attack Detected”);

Step-3 Calculate the network delay by using equ.1, 2, 3

Step4 Calculate the network efficiency by using equ-4

Step-5 Calculate the packet loss by using equ-5

Step-6 Calculate the dynamic routing with attacks if occurs.

Step-7 Show results.

7. EXPERIMENTAL RESULTS:

The implementation is done in NS-3 simulator with the 10, 30, 60 nodes in each iteration. The system requires 8 GB Ram and 1 TB hard disk. The network is integrated with 6LoWPAN network and dynamic network that can increase the nodes based on requirement.

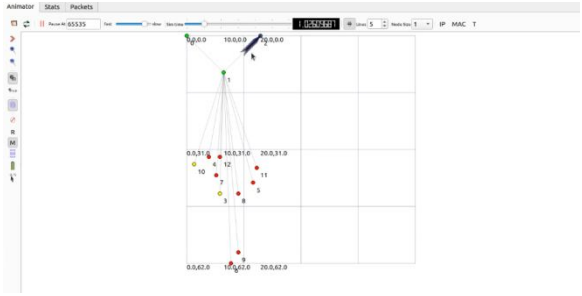

Figure 2: showing network delay (nodes are represented with red-attackers, yellow-normal nodes and green-IoT devices).

Figure 2 shows the existing methodology which transmission of packets 1.31 kb data.

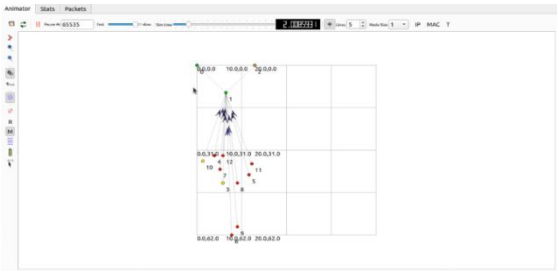

Figure 3: showing network (nodes are represented with red-attackers, yellow-normal nodes and green-IoT devices).

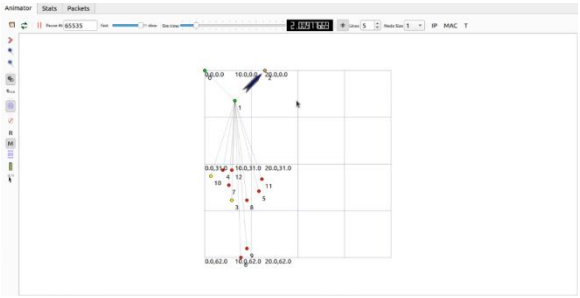

Figure 4: Showing no network delay (nodes are represented with red-attackers, yellow-normal nodes and green-IoT devices).

The maximum data transmission that can be done with the proposed mythology is 1.56 MB.

Table: 1 Results showing the performance of the ES at various nodes in the network

No of Nodes	Network Delay (MS)	Packet Loss (%)	Efficiency (%)
10	**120**	**23**	**76.4**
20	**145**	**34**	**75.4**
30	**175**	**38**	**76.5**
40	**189**	**45**	**77.4**
50	**210**	**55**	**76.3**
60	**230**	**65**	**77.4**
70	**260**	**76**	**76.5**

Table 2: Results showing the performance of the EAD at various nodes in the network

No of Nodes	Network Delay (MS)	Packet Loss (%)	Efficiency (%)
10	**45**	**9**	**90.5**
20	**55**	**13**	**91.2**
30	**75**	**19**	**90**
40	**80**	**22**	**93.1**
50	**85**	**26**	**92.4**
60	**90**	**29**	**92.4**
70	**97**	**31**	**92.3**

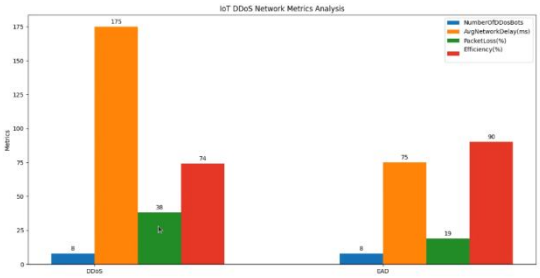

Figure 2: the performance of the EAD and ES at 30 Nodes in 6LoWPAN network

8. CONCLUSION

In this paper, the Enhanced attack detection algorithm (EAD) is introduced to solve the DDOS attack issues in network. With the integration of IOT, security is improved to the devices and nodes. The EAD is the algorithm prevents the network crashes, preventing packet loss and dynamic routing. Every node in the network connected to the server with the help of IOT device and this device monitors the ddos attacks and prevents the network loosing.

REFERENCES

1. Al Hinai, S., & Singh, A. V. (2017, December). **Internet of things: Architecture, security challenges and solutions.** In 2017 International Conference on Infocom Technologies and Unmanned Systems(Trends and Future Directions)(ICTUS) (pp. 1-4). IEEE.

2. Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., et al.(2018). **Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. Journal of Hardware and Systems Security**, 2(2), 97–110.

3. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). **The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved.** IEEE Internet of Things Journal, 6(2), 1606–1616.

4. Roman, R., Zhou, J., & Lopez, J. (2013). **On the features and challenges of security and privacy in distributed internet of things.** Computer Networks, 57(10), 2266–2279.

5. Kamble, A.; Bhutad, S.: **Survey on Internet of Things (IoT) security issues and solutions.** In: 2018 2nd International Conference.on Inventive Systems and Control (ICISC) IEEE, pp. 307–312(2018).

6. Ammar, M.; Russello, G.; Crispo, B.: **Internet of Things: a survey on the security of IoT frameworks.** J. Inf. Secur. Appl. 38, 8–27 (2018).

7. Hassan, W.H.: **Current research on Internet of Things (IoT) security: a survey.** Comput. Netw. 148, 283–294 (2019)

8. Al Salami, S.; Baek, J.; Salah, K.; Damiani, E.: **Lightweight encryption for smart home.** In: 2016

11th International Conference on Availability, Reliability and Security (ARES) IEEE, pp. 382–388 (2016).

9. Zargar, S. T., Joshi, J., & Tipper, D. (2013). **A survey of defence mechanisms against distributed denial of service (DDoS) flooding attacks.** IEEE Communications Surveys & Tutorials, 15(4),2046–2069.

10. Hanumat Prasad Alahari, Suresh Babu Yalavarthi, **"Integrating and Interfacing the Reference Protocol Stack of IoT in 6LoWPAN Network"**, Jour of Adv Research in Dynamical & Control Systems, Vol. 12, Issue-06, 2020.

11. H. P. Alahari and S. B. Yelavarthi, **"Performance Analysis of Denial of Service DoS and Distributed DoS Attack of Application and Network Layer of IoT,"** 2019 Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2019, pp. 72-81, doi: 10.1109/ICISC44355.2019.9036403.

12. Chen, Y. K. (2012, January). **Challenges and opportunities of internet of things.** In 17th Asia and South Pacific design automation conference (pp. 383-388). IEEE.

13. Deep, S., Zheng, X., & Hamey, L. (2019). **A survey of security and privacy issues in the Internet of Things from the layered context**. arXiv preprint arXiv:1903.00846.

14. Daud, M., Rasiah, R., George, M., Asirvatham, D., Rahman, A. F. A.,& Ab Halim, A. (2018, May). **Denial of service:(DoS) Impact on sensors.** In 2018 4th International Conference on Information Management (ICIM) (pp. 270-274). IEEE.