Detection and Prevention Algorithm of DDoS Attack Over the IOT Networks

Mohammed Ridha Nsaif [1], Mohammed Falah Abbood [2], Abbas Fadhil Mahdi [1]

[1] *Computer Science department, faculty of computer science and mathematics, University of Kufa, Iraq*
[2] *Central Library, University of Kufa, Iraq*

Abstract **– One of the most notorious security issues in the IoT is the Distributed Denial of Service (DDoS) attack. Using a large number of agents, DDoS attack floods the host server with a huge number of requests causing interrupting and blocking the legitimate user requests. This paper proposes a detection and prevention algorithm for DDoS attacks. It is divided into two parts, one for detecting the DDoS attack in the IoT end devices and the other for mitigating the impact of the attack placed on the border router. Also, it has the ability to differentiate the High-rate from the Low-rate DDoS attack accurately and defend against these two types of attacks. It is implemented and tested against different scenarios to dissect their efficiency in detecting and mitigating the DDoS attack.**

Keywords **- Internet of things, IEEE, security, 802.15.4,6LoWPAN, DDoS attack defensive mechanism**

1. Introduction

A Denial of Service (DoS) attack is a type of cyber-attack aims to prevent the legitimate users from accessing the network resources, by disrupting or completely eliminates the network's communication. Distributed Denial of Service (DDoS) attack is the most common and widely known type of DoS attacks.

DOI: 10.18421/TEM93-09
https://doi.org/10.18421/TEM93-09

Corresponding author: Abbas Fadhil Mahdi,
Computer Science department, Faculty of computer science and mathematics, University of Kufa, Iraq.
Email: abbassf.wahab@uokufa.edu.iq

Received: 29 January 2020.
Revised: 19 May 2020.
Accepted: 29 May 2020.
Published: 28 August 2020.

DDoS attack uses a number of compromised computers (agents) to form a botnet. The botnet sends a flood of traffic to the target server, causing a denial of service by exhausting computation or communication resources. one of the main challenges is the attack from internal of the (IoT) network, so the attackers can use small devices including tablets, printers, webcams, residential gateways, where these devices form the Internet of Things (IoT) network.
For the IoT, there can be more than remote DDoS attacks. The attacker can use more points for accessing the system either physically or via direct wireless communication. An example of this is producing high-energy radio signals into the air to disrupt the wireless communication around using jammers [1]. The DDoS attack can be initiated in simple ways represented by jamming the physical layer or more sophisticated attack which includes the network and application layers.

Talking about DDoS attack and IoT devices, "mirai" is still remembered as the biggest DDoS attack that occurred in 2016, namely in which the attacker used a powerful malware that caused to infect hundreds of thousands of connected devices all over the world through a dictionary attack, relying upon the fact that these devices use default login credentials and that most of the users never change those credentials. On October 21th, 2016, this massive botnet (the network of infected devices) was used to struck what is currently considered the largest DDoS attack ever seen, reaching a magnitude of about 1.2 Terabits per second [2]. Therefore, DDoS attacks can be considered as an important security issue and must be handled properly in the IoT networks.

1.1. Related Works

There are few researchers been done on the subject of detecting and mitigating of DDoS attack in the IoT. This section reviews the related works carried out in this domain.

S. Misra, P. Venkata Krishna and Mohammad S. Obaidat (2011) based on learning automata proposed an approach detecting and preventing DDoS attack in the IoT networks. Its present Service Oriented

Architecture (SOA) to provide service for the IoT and ensures that the whole framework is free from the DDoS attack. The SOA behaves as a middleware between the IoT gateway and end devices which takes random sampling rates α {α1, α2… αr} at different times as input, and according to these sample rates environment response (β) is stored as output. In the detecting phase, the DDoS prevention component in each device monitors the rate of incoming traffic and whenever it exceeds the threshold attack occurs. It generates DDoS alert (DALERT) message that will be transmitted to all neighbor nodes to inform them that the attack occurred. This method is totally based on automata sampling rates and behavior of the system. Knowing the critical nature of parameters such as energy and computational power in the IoT objects, the LA scheme effectively prevents the objects from a DDoS attack by making the optimal utilization of its resources[3].

V.C. Manju and Kumar M. Sasi (2012) proposed an approach for detecting jamming attack in wireless sensor network (WSN). The proposed solution depends on Received Signal Strength Indicator (RSSI) value. based on Residual Energy, one monitoring node is selected. First, each node in the network calculate its Residual Energy and comparing it with the predefined Residual Energy. If it is less than max Residual Energy, then node is inactive; else the node is active and is selected as monitoring node. Then, based on RSSI and Packet Deliver Ratio (PDR) values from all other node, they make metric weight of each node. When these values reach out of threshold limit, DoS attack occurs and that node is identified as a malicious jammer node and will be isolated from network to let the network work normally. The proposed approach periodically checks RSSI of node which is good but not suitable for the IoT as it continuously asks for RSSI[4].

Luís M. L. Oliveira, Joel J. P. C. Rodrigues, Amaro F. de Sousa and Jaime Lloret (2013) introduced an approach based on address registration process defined in the Neighbor Discovery Protocol proposed for 6LoWPAN to mitigate DoS attacks initiated from the Internet, without adding additional overhead on the 6LoWPAN sensor devices. destination node address must be registered and the node must declare willingness to accept data from the internet to ensures that the traffic is not forward to non-existing nodes. Information about the supported transport layer protocol at the node must be registered with the edge router to ensure that only traffic of such protocol will be forwarded. Also, node should previously inform the edge router about the accepted traffic rate limit where in most sensor cases, data measurements are generated at a slow rate (for example, air temperature monitoring) to set a limit for acceptable request rates to prevent flooding attacks. In this case, the edge router only forwards the Internet traffic into the smart objects network if the traffic meets predefined conditions [5].

C. Zhang and R. Green (2015) proposed a lightweight algorithm for preventive measuring and avoiding DDoS attack in the IoT end network. The proposed algorithm designed to work on the IoT end devices to detect and prevent malicious packet streams[6].

K. Sonar and H. Upadhyay (2016) Proposed an approach to detect and prevent the DDoS attack traffic from reaching the IoT devices by identifying the attack traffic a priori at border gateways. The proposed mechanism puts an agent that is software-based managers between the IoT network and gateway or border router, which identify the DDoS attack depending on router threshold and take appropriate action under such situation. The agent maintains traditional grey list and black list, which are special access control list to block access either temporary or parentally on detecting attacks [7].

2. Problem Statements

One of the most important security challenges in the IoT systems is the increasing number of the DDoS attacks. In many cases, people and companies use IoT devices but do not know about the dangers of exploited DDoS attacks. With the rapid increase in the use of IoT devices, the potential power of a DDoS attack when using IoT devices could increase dramatically. This made researchers proposing and finding new solutions for IoT systems to make it more secure as possible.

3. Research Contribution

This paper aims to propose and implement an approach for detection and mitigation of DDoS attack in IoT networks. The main goal of the thesis can be described in the following points:

- Proposing an algorithm to detect the DDoS attack. The proposed detection algorithm is distributed over the IoT end devices and it has the ability to distinguish between the low-rate and the high-rate DDoS attack.
- Proposing an algorithm to mitigate the impact of DDoS attack. The mitigation algorithm works on the monitor agent (always placed at the gateway or the border router).
- Implementing the algorithms and comparing the result of our approach with the existing techniques that used to detect and mitigate the DDoS attack in IoT networks.

4. The Proposed DDoS Defense Architecture

The main goal of any DDoS defense mechanism is the detection of DDoS attacks as soon as possible to stop them as near as possible to their sources. DDoS defense mechanisms are divided into four classes based on the locality of deployment: source-end, victim- end, intermediate network, and Hybrid defense mechanisms. The hybrid defense mechanisms are deployed at multiple locations such as victim or intermediate networks. Attack detection and mitigation using Hybrid mechanism can be considered the best strategy against DDoS attacks where, the intermediate network is the best to rate-limit all kinds of attack traffic whereas, the victim-end can accurately detect the attack traffic in a combination of legitimate and attack packets. Therefore, distribution of methods of detection and mitigation at different ends of the network can be more beneficial [4].

The proposed DDoS defense works based on Hybrid defense mechanisms. The two algorithms cooperate with each other to achieve best defense strategy where the detection algorithm is distributed over the End-nodes (victims) to detect the attack and distinguish attack type. Then, it will send a warning to the mitigation algorithm which is found on the monitor agent to mitigate the impact of the DDoS attack. The monitor agent represents the intermediate network; it is a software-based agent usually placed at the border router or the gateway of the IoT network.

4.1. The Proposed DDoS Detection Algorithm

Logically, the first phase of the proposed approach is the attack detection phase that will be done at the End-Nodes of the IoT network. The Proposed DDoS Detection Algorithm (PDDA) checks the incoming traffic to the IoT devices, whether it is DDoS traffic or normal traffic. In case it senses a DDoS traffic, PDDA will specify the type of the attack, whether it is High-rate or Low-rate attack then it will send warning message containing the address of the attacker, port number and the type of the attack to monitor agent.

PDDA maintains a table for counting the received packets from each client during a fixed time called detection time. Each record in the table maintains the following fields: IP address of the requester, port number, number of received packets during the detection time, and time difference between the first and last packet during this time. Figure 1. shows PDDA table format.

IP address	port number	Packet counter	time difference

Figure 1. shows PDDA table format

PDDA is designed to be very lightweight and efficient to work in terms of time consumption and storage usage to meet the requirement of constraint environments such as the IoT network, where the devices have low processing capabilities with power and storage restrictions.

The Proposed DDoS Detection Algorithm is as follows:

Algorithm 1. PDDA

```
Set:   Threshold value = th_value
 Packet counter =Pc
        Detection time = td
       Detection factor=β
If (detection time(td) not expired) then
If packet received then
Pc++;
    If (pc > th_value) then
If (Δ (Rp) < β*td) then
        Send High-rate attack warning to monitor
node;
        else
        Send Low-rate attack warning to monitor
node;
        end if
    end if
end if
else
Reset timer;
Pc=0;
end if
```

where β assumed to be the detection factor that PDDA uses to check the type of attack depending on the time difference between the received packets $\Delta t(Rp)$.

4.1.1. PDDA Description

To achieve the desired results accurately, the PDDA follows few steps in the detection process as described below:

Step 1. During a fixed time (detection time), the PDDA counts the incoming packets from each sender. It allocates record for each sender to save its IP address, port number, packet counter and the time difference between the received packets.

Step 2. On receiving a packet, the algorithm will compare the Packet counter (Pc) of the sender record with the predefined threshold value (th_value). If (Pc > th_value) is satisfied, this means that the DDoS attack occurred and the algorithm goes to step3,

otherwise, the PDDA will wait for the next packet to check it.

Step 3. After the detection of the attack, the PDDA will specify the type of the DDoS attack, whether it is High-rate or Low-rate attack. The algorithm depends on the predefined detection factor (β) to distinguish the attack type. The type of attack will be a High-rate attack if the following equation is satisfied:

$$\Delta t(Rp) < \beta * td \qquad (1)$$

Where, $(\Delta t(Rp))$ is the time difference between the first and the last received packets during the fixed detection time (td), and β is a small positive number: $0 < \beta < 1$. Otherwise, the algorithm considers the attack type as a Low-rate attack.

Step 4. Finally, warning message containing the address of the attacker, port number and the type of attack will be sent to the monitor agent to start the mitigation process.

4.2. The Proposed DDoS Mitigation Algorithm

The second phase of the proposed approach is the attack mitigation phase. This phase will be done at the monitor agent. The main purpose of the Proposed DDoS Mitigation Algorithm (PDMA) is to reduce the impact of the DDoS attack on the IoT network. The PDMA maintains three tables: WhiteList, GreyList and BlackList tables as described below:

- **WhiteList:** this list is used for trusted and high priority clients. The monitor agent will forward all packets from the sources listed in the WhiteList without checking the other lists. It is possible to add or remove addresses manually to/from the WhiteList.
- **GreyList:** PDMA uses the GreyList for temporary blocking of the suspected addresses. GreyList is an important resource to check whether the incoming traffic is an attack traffic or normal traffic. The main function of the GreyList is to block the traffic from the suspected addresses temporally to check whether the attack is real attack or flash crowed from the legitimate clients. GreyList record consists of six columns as illustrated in Figure 2.
- **BlackList:** this list is used to block the attacker address permanently. Components in BlackList are always considered as an attack in the highest priority.

Suspected IP address	Port number	Victim IP address	Low-rate flag (L-active)	High-rate flag (h-active)	Expiration Time (False-Positive Flag)

Figure 2. PDMA GreyList Table Format.

The proposed DDoS mitigation algorithm is as follows:

Algorithm 2. PDMA

```
If warning packet then
        If in GreyList then
Add to Blacklist;
else
if high-rate attack warning then
Add to grey list;
H_active=true (timer for temporary blocking);
else
Add to grey list;
L_active= true (timer for temporary blocking);
end if
      Set expiration time to delete record (false
Positive);
end if
else                                    // for
Data Packets
if in white list then
forward packet;
else if in grey list and (dest_addr=victim_addr) and
(H_active or
 L_active) =true then
drop packet;
else if in black list then
drop packet;
else
forward Packet (new flow);
end if
end if
```

4.3. PDMA Description

The proposed mitigation algorithm goes through some steps to reduce the impact of the DDoS attack as described below:

Step 1. For each received packet, the PDMA checks whether it is a warning or data packet.

Step 2. On receiving a warning packet, the algorithm will check whether the address of the attacker is in GreyList or not, if it is found in the GreyList then, the address of the attacker will be moved to the BlackList.

Step 3. If the address of the attacker received with warning packet is not found in the GreyList, the PDMA will add the attacker address, port number, type of attack and the victim address to the GreyList for temporary blocking with some assumptions that will be explained in Step4.

Step 4. Depending on the attack type received with the warning packet, the PDMA takes the appropriate action for each type of attack. For the High-rate attack, it blocks the connections from the attacker for a long period (10 seconds) as compared with the Low-rate attack type period (5 seconds). The PDMA adjusts the corresponding flag for each type of attack to be true during these periods.

Step 5. The PDMA also uses another type of flags in the GreyList called False Positive flag. This flag is used for False Positive warning where, in some cases the legitimate users may be flagged as attackers. The False Positive flag will be set to true for each new record and remains for a fixed predefined time (30 seconds). If during this time PDMA did not receive another warning for the suspected address, then the record will be removed at the end of this time and the warning will be considered as a False Positive warning, otherwise the warning will be considered as True Positive warning.

Step 6. On receiving data packet, the PDMA goes to the filter mode. In this mode firstly, the PDMA checks the source address in WhiteList, if the record is found then the packet will be forwarded directly to the destination without checking the other lists.

Step 7. After that, the algorithm checks the GreyList, If the address is found in the GreyList and the destination address is equal to the victim address and the High-rate or Low-rate flags set to be true, then the packet will be dropped.

Step 8. The next step in filtering mode is to check the source address in the BlackList, if the record is found in this list then the packet will be dropped.

Step 9. Finally, if the source address is not archived in all lists, then the packet will be forwarded to the destination (new flow).

5. Implementation

In a typical IoT network involved with DDoS attack scenario, four different types of nodes can be present in the simulation environment, including working nodes (IoT end devices), monitor agent node, legitimate user nodes, and the attacker nodes. Figure 3. shows the network topology for the proposed work containing the four types of the nodes explained above.

For this purpose used Cooja Simulator is a network simulator specifically designed for wireless sensor networks, it is a highly useful tool by which developers can test their applications on fully emulated devices before running it on real hardware.

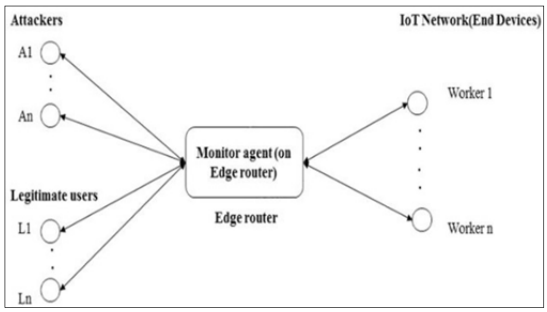

Figure 3. Network topology for the proposed approach

The working node in the proposed topology represents the IoT end device (sensor) that collects information and executing simple tasks in an IoT environment. The major behavior of the proposed working node is serving requests and detecting DDoS attacks using the proposed detection algorithm explained above.

The monitor agent is a software-based agent that can be placed on the gateway or the border router of the IoT network. To implement this type of node in simulation environments, the proposed mitigation algorithm which is presented in Chapter 3 will be placed on the node that acts as border router in our proposed topology.

As we explained before, there are two types of the attacker nodes in the proposed approach, Low-rate attackers and High-rate attackers. To implement these two types of the attacker nodes in the simulation, we designed the High-rate attacker node to send requests in high frequency where it sends one request every one second as compared with the Low-rate attacker node which sends one request every three seconds. The last type of the proposed nodes is the legitimate user node; this type of nodes sends requests at a normal rate where it is designed to send one request every four seconds.

Simulation Parameters and Performance Metrics

Table 1. For our simulation, we have chosen parameters as shown in table

Parameter	***Value***
Simulation time	*60 s*
Number of legitimate clients:	*5*
Number of attackers:	*5*
Transmission range:	*50 m*
Packet type:	UDP
Low-rate attacker packet rate:	1 packet per 3 seconds
High-rate attacker packet rate:	1 packet per second
Legitimate client packet rate:	1 packet per 4 second

The simulation starts with normal traffic for the first 5 seconds, then the attackers will send the attack traffic with the next 15 seconds (5s < t < 20 s), at the end of this period (t=20) the attack will be detected at the worker nodes and the warning for the attack will be sent to the monitor node with the address of the attacker, port number, and the type of attack (High-rate or Low-rate) to start the mitigation process. The mitigation process will take about 30 seconds to check whether the warning is True Positive or False Positive warning, finally, the attack ends with the last 10 seconds where the system recovered from the attack.

The performance metrics that are used to measure the impact of the DDoS attack in our simulation are as follow:

1. **Packet Delivery Ratio (PDR):** It is the ratio of the number of packets successfully delivered to the destination to the total number of packets received from all sources in the monitor agent.

$$PDR = \frac{PS}{PS + PD} * 100\ \% \qquad (2)$$

Where, PS is the number of delivered packets to the destination, and PD is the number of dropped packets in the monitor agent.

2. **True Positive/ False Positive:** Due to the accuracy and precision at the proposed algorithm's rules which focused on the cooperation between the end nodes (sensors) and the monitor node (on the edge router) which are defined to specifically detect the volumetric flooding attack on the network layer, the experiments show no False Negatives attacks during the experiments. The victim node could detect all attacks and produce five True Positive (true attacks) out of five in all five attacks during the experiments. Table 1 shows the True Positive and False Negative results of proposed approach
3. **Power consumption:** It is the approximated amount of energy that is consumed in a specified time for each node. This metric gives us clear view of the power consumption for each node in milliwatts (mW). In our simulation we will measure the power consumption for the victim nodes (IoT devices) due to the constraint nature of these devices which require reducing the power consumption to improve the life of such devices.

6. Simulation Results

The two algorithms are designed to be very lightweight and efficient to work in terms of time consuming and memory usage to meet the requirement of the IoT network. We have tried as much as possible to minimize the consumption of time and memory in the implementation phase by maintaining the record list short as possible and reduce the execution time for the two algorithms.

Table 2. shows the average time needed to execute the algorithms (for one time) during the simulation.

Table 2. Average Time Consumption for PDDA and PDMA in millisecond.

Algorithm	***Time Consumption***
PDDA	0.013 ms
PDMA	0.095 ms

The experiments were done on a Lenovo laptop with intel CORE i5 Processor, (4 CPUs) 2.4 GHz, 6 GB of RAM, using Windows 10 Operation System. Contiki OS has been run as a guest OS (Virtual Machine) on the host operation system.

Three simulation scenarios will be studied in our implementation to analyze how the proposed algorithms can effectively detect and mitigate the DDoS attacks in the IoT networks.

Case 1. In this case, the interaction between the Low-rate attackers with the legitimate clients. The number of the Low-rate attackers (LA(n) =5) and the number of legitimate clients (L(n) =5).

Table 3. illustrates the simulation results for Case 1 during the attack warning phase. It shows the PDR, the number of False Negative and the number of True Positives. In this case, the victim node could detect all the five attackers accurately and generate five True Positive out of five.

Table 3. Simulation results for Case 1.

	No. of Received Packets	***No. of Forwarded Packets***	***Packet Delivery Ratio***	***No. of True Positive Alerts***	***No. of False Negative Alerts***
L(n)=5 LA(n)=5	79	63	79.7 %	5	0

Case 2. In this case, the interaction between the High-rate attackers with the legitimate clients where, the number of the High-rate attackers (HA(n)=5) and the number of the legitimate clients (L(n)=5).

Table 4. shows the simulation results for this scenario during the attack warning phase. It can be noticed from the results that the PDR value has decreased in this case because of the nature of the High-rate attackers as they send packets with a high frequency, which leads to increase in the number of the dropped packets and results in reducing the PDR.

Table 4. Simulation results for Case 2.

	No. of Received Packets	***No. of Forwarded Packets***	***Packet Delivery Ratio***	***No. of True Positive Alerts***	***No. of False Negative Alerts***
L(n)=5 HA(n)=5	*178*	112	62.9 %	5	0

Case 3. This scenario explains the interaction between the two types of the attackers with the legitimate clients, where (LA(n)=3, HA(n)=2 and L(n)=5)**.** The purpose of this scenario is to examine whether the worker node can accurately detect the two type of attacks at the same time and distinguish between them or not**.** The simulation results are as shown in Table 5.

Table 5. Simulation results for Case 3.

	No. of Received Packets	***No. of Forwarded Packets***	***Packet Delivery Ratio***	***No. of True Positive Alerts***	***No. of False Negative Alerts***
L(n)=5 HA(n)=5	117	82	70 %	5	0

It can be noticed from the results in Table 4.-5. that the victim node could detect the two types of attacks accurately in this case. Also, the PDR is greater than the PDR in Case 2 because the number of High-rate attackers reduced to be two attackers in this case.

Figure 4. shows a comparison between the power consumption in the case of using the proposed algorithm and without using the algorithm in Case 1. The comparison is measured during the attack warning phase in the victim node (IoT device), due to the constraint nature of this type of nodes which makes the power consumption very critical issue in such devices. It can be noticed that the power consumption is reduced by 2 milliwatts approximately during the period (0s<t<5s) in the attack warning phase where the algorithm at the monitor agent blocks the traffic from the suspected nodes. In the next 15 seconds, the power consumption will be increased where the algorithm in this period allows the packets from the suspected nodes to be forwarded to the victim node again to check whether the warning is True Positive or False Positive warning. At the time (t=20), the attack is confirmed and the power consumption is reduced again, and it will continue to the end of the simulation.

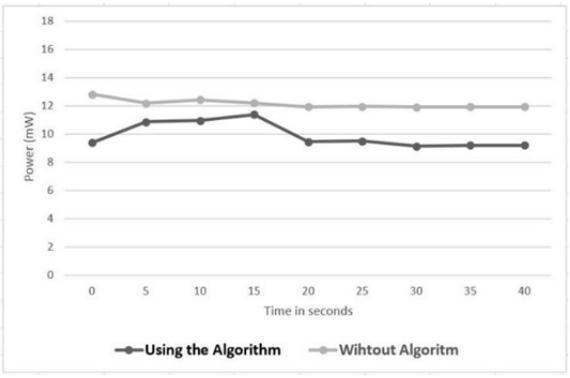

Figure 4. Power consumption in Case 1.

A comparison between the power consumption in the case of using the proposed algorithm and without using the algorithm in Case 2 is shown in Figure 5. It can be noticed that the power consumption is reduced by 4 milliwatts approximately after the confirmation of the attack by using the proposed algorithm.

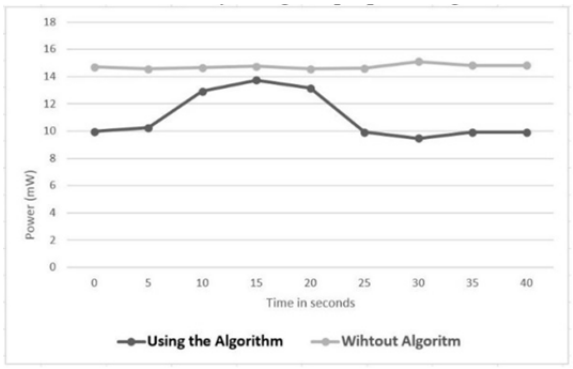

Figure 5. Power Consumption in Case 2

Figure 6. shows a power consumption comparison in Case3. The comparison indicates that the power consumption is reduced by 3 milliwatts approximately by using the proposed algorithm in this case.

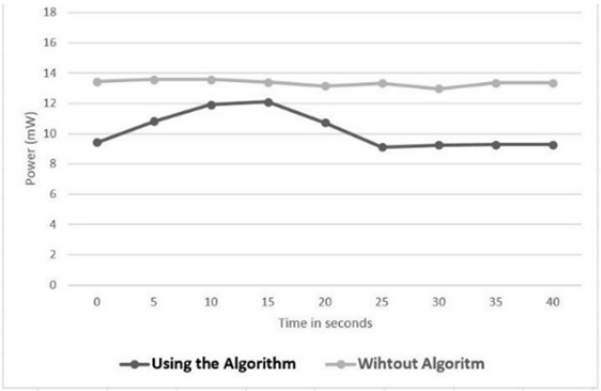

Figure 6. Power Consumption in Case 3.

Figure 7. shows PDR comparison between the proposed approach and paper [8]. The comparison illustrates the simulation results for the three cases of the proposed approach with the results of paper [8] for the same number of attackers and legitimate clients. It can be noticed that the PDR value in Case 1 of our approach is higher than the PDR value of paper [8]. Also, due to the nature of the High-rate attackers which send packets in high frequency, the PDR values decreased in Case 2 and Case 3 of our approach, this indicates the accuracy and effectivity of our approach in detecting and mitigating the DDoS attacks. Furthermore, our approach has the ability to distinguish between the Low-rate and the High-rate attacks. The proposed algorithm depends on the worker nodes thresholds not on the router threshold to detect the attacks, this cooperation between the worker nodes and the monitor agent

increase the detection sensitivity and lower the total cost on extra hardware.

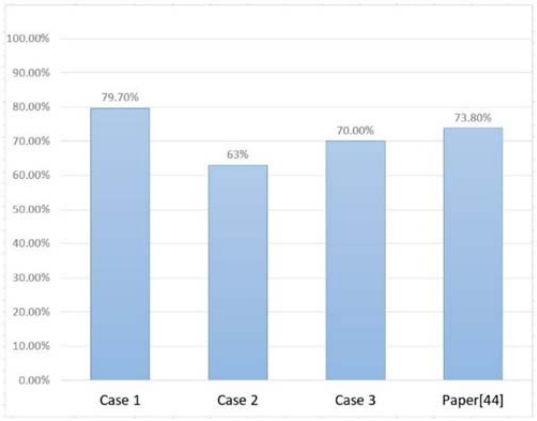

Figure 7. Packet Delivery Ratio (PDR).

The experiments show no False Negatives where, the detection was based on predefined rules, which are defined to specifically detect the volumetric flooding attack on the network layer. The victim node could detect all attacks and produce five True Positive out of five in all cases. Figure 8. shows the True Positive and False Negative results of our approach and paper [8].

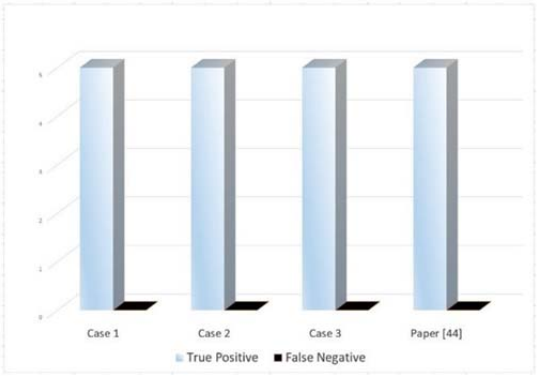

Figure 8. True Positive and False Negative.

7. Conclusion

In this thesis, an approach to detect and mitigate DDoS attack have been proposed. The proposed approach includes two algorithms, one for detection of the attack which is distributed over the end devices of the IoT network, and the other is to mitigate the impact of DDoS attack which is placed on the border router/ gateway of the IoT network. Our approach depends on IoT End devices threshold in detecting the DDoS attack to increase the detection accuracy and sensitivity. The two algorithms designed to be very lightweight to meet the IoT requirements in terms of time, power and memory consumption. The proposed algorithms also, can distinguish between Low-Rate and High-rate DDoS attacks accurately.

According to the results, the proposed approach could effectively help the IoT network environment in detecting DDoS attacks and defense against it. We can say that our approach can be applied in many IoT areas, especially when the number of users is relatively small such as smart home, smart building and smart hospital so it can easily identify and protect the IoT network from the DDoS attackers.

References

[1]. Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2011). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys and Tutorials*, *13*(2), 245-257.

[2]. Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*.

[3]. Misra, S., Krishna, P. V., Agarwal, H., Saxena, A., & Obaidat, M. S. (2011, October). A learning automata based solution for preventing distributed denial of service in internet of things. In *2011 international conference on internet of things and 4th international conference on cyber, physical and social computing* (pp. 114-122). IEEE.

[4]. Manju, V. C., & Sasi, K. M. (2012, December). Detection of jamming style DoS attack in Wireless Sensor Network. In *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing* (pp. 563-567). IEEE.

[5]. Adhianto, L., Banerjee, S., Fagan, M., Krentel, M., Marin, G., Mellor-Crummey, J., & Tallent, N. R. (2010). HPCToolkit: Tools for performance analysis of optimized parallel programs. *Concurrency and Computation: Practice and Experience*, *22*(6), 685-701.

[6]. Zhang, C., & Green, R. (2015, April). Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In *Proceedings of the 18th Symposium on Communications & Networking* (pp. 8-15).

[7]. Sonar, K., & Upadhyay, H. (2016). An approach to secure internet of things against DDoS. In *Proceedings of international conference on ICT for sustainable development* (pp. 367-376). Springer, Singapore.

[8]. P. N. Aote, T. Belsare, S. Giri, S. Giradkar, and S. Mohekar.(2018). Smart Digital Door Lock System. I*nternational Journal of Recent Engineering Research and Development*, *3*(4), 41-45.