Global Journal of Engineering and Technology Review

Journal homepage: www.gjetr.org

Global J. Eng. Tec. Review 4 (2) 26 – 34 (2019)

Development of Denial of Service (DoS) Mitigation for Internet of Things (IoT) Sensor Node

Abdul Fuad Abdul Rahman[1]*, Azni Ab Halim[2], Nurul Syazwani[3], Maslina Daud[4]
Madihah Zulfa Mohamad[5], Muhamad Izzat Yahood[6]

[136] IoT Security Lab, CyberSecurity Malaysia, 63000, Cyberjaya, Malaysia
[2]Universiti Sains Islam Malaysia (USIM), 71800, Nilai, Malaysia
[4]CSPS, CyberSecurity Malaysia, 63000, Cyberjaya, Malaysia
[5]CIEC, CyberSecurity Malaysia, 63000, Cyberjaya, Malaysia

ABSTRACT

Objective – The objective of this paper is to proposed a lightweight IDS algorithm to secure IoT Sensor Node.

Methodology/Technique –The proposed IDS algorithm for IoT Sensor Node shall prevents the abnormal energy consumption by monitoring, calculating and evaluating energy drop from each cluster nodes based on few condition.

Findings –The DoS attack is considered as one of security threat that may affected the quality service of IoT network and also reduce the lifespan of IoT Sensor Nodes

Novelty – The approach is using data from previous experiments and translated it to develop a mitigation to secure IoT Sensor Node, thus increased the lifespan of IoT Sensor Nodes.

Type of Paper: Other.

Keywords: Internet of Things (IoT); Intrusion Detection System (IDS); Denial of Service (DoS); Smart Water; Sensor;

1. Introduction

The Internet of Things (IoT), also called the Internet of Everything or the Industrial Internet, is a new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other.

However, IoT is generally characterized as small miniature things, widely distributed with limited storage and processing capacity, which involve concerns regarding reliability, performance, security,

*Paper Info: Revised: June 16, 2019
Accepted: July 10, 2019

* Corresponding author: Abdul Fuad Abdul Rahman
E-mail:
Affiliation: IoT Security Lab, CyberSecurity Malaysia, 63000, Cyberjaya, Malaysia

and privacy. Most current available research on IoT focus on wireless networks and wireless protocol as IoT preferred medium of communication. Wireless appears to be the most suitable choice for the IoT as it has the potential to address all the IoT challenges and requirements. However, wireless networks are susceptible to DoS attacks.

2. Intrusion Detection System

Many researchers have already discovered numerous strategies for mitigating DoS attack. Most common approach on developing a mitigation for a DoS attack is to block the DoS packets. For example, by implementing a Firewall Rule to block Internet Control Message Protocol (ICMP) PING Packets, shall protect a system from ICMP PING Flood Attack. However, this will be very radical solution and there will be problems with the system. The same concept applied in Intrusion Detection System (IDS). Based on IoT Security Framework proposed by Rahman et. al. 2016, one of the security components required to secure an IoT implementation is by deploying IDS in the network (Rahman A.F.A, 2016)

An IDS is used to monitor the intrusion and malicious traffic in particular node and network (Upadhyay, 2016). Intrusion is an unwanted or malicious activity which is harmful to IoT System and specifically IoT Sensor Nodes. IDS can be a software or hardware tools. IDS detect the network packets and determine whether they are intruders or legitimate users. Mainly there are three components of IDS: monitoring, analysis and detection in traditional IDS model as shown in Figure 1 (Upadhyay, 2016). Analysis and detection are a core component of IDS which detects the intrusions according to specified algorithm (Upadhyay, 2016). The monitoring module monitors the network traffics, signatures and patterns.

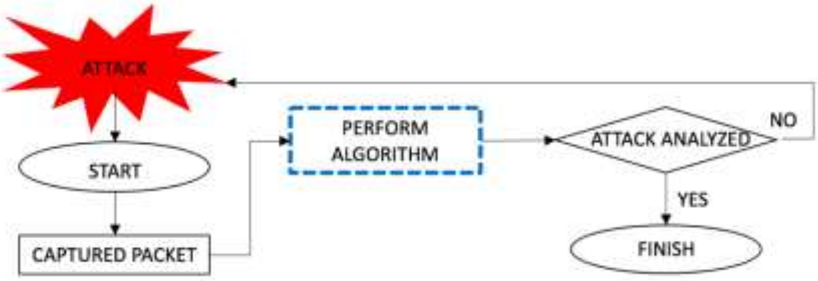


Figure 1. Traditional IDS

However, most available IDS was design to monitor the network are not suitable to be embed inside an IoT Sensor Node itself (Upadhyay, 2016). Therefore, this paper proposed a lightweight IDS algorithm as a mitigation to DoS Attack. The algorithm shall be designed in lightweight to adhere to IoT Sensor Node low computational power and energy consumption. The requirement of low computational power and low energy consumption limits the adoption of many IDS research. Therefore, this paper takes a different approach on developing a lightweight IDS algorithm for IoT Sensor node using data conducted on actual environment, and not based on simulation data.

3. Approach

The idea of using data from actual security assessment before designing security solution will be the core element in this paper. The approach is to study IoT Sensor Node behaviour in terms of energy drop during an actual DoS attack. Rahman et. al. 2014 discussed in detail regarding cyber-attacks on IoT Sensor Node. The paper successfully conducted four type of attacks on IoT Sensor Node (Rahman A.F.A., Ahmad R. and Ramli S.N, 2014). The four attacks are Denial of Service, Eavesdropping, Role

Bypass and Authentication Bypass (Rahman A.F.A., Ahmad R. and Ramli S.N, 2014). Daud et. al. 2018 successfully shows the impact of Denial of Service (DoS) attack on IoT Sensor Node (M. Daud, 2018). In the study, it was concluded that DoS attack has significant impact on sensor (using AA size Zn/MnO2 Battery) energy consumption and significantly reduce sensor lifespan from around 1000 minutes to 100 minutes only (M. Daud, 2018).

A study of assessing the impact of DoS attack on IoT Sensor Nodes was conducted in an actual environment and the data was discussed in detail in a study conducted by Daud et. al. 2018. A research by Rahman et.al. 2018 shall be used as benchmark to measure energy consumption of IoT Sensor Node. The findings by Daud et. al. 2018 and Rahman et. al. 2018 will be translated into algorithm to facilitate further research on coding and programming.

This paper will be divided into five sections. The first section discuss the introduction of IoT and IDS. The second section discuss the related works on type of IDS currently available. Then, this paper will proposed the lightweight algorithm for IoT Sensor Node. The forth section discuss the result of the implementation of the proposed IDS algorithm for IoT Sensor Node before conclude the paper in section five.

4. Related Works

Since IoT will consists a complex infrastructure from sensors to cloud, the challenge to cybersecurity is to choose which area to be secure first and worth invested in. Any approach taken should consists and cover all angle of IoT components and the most important is that the approach is easy to implement (Rahman A.F.A, 2016). If the developed security approach is too complex, it will be extremely difficult for other organizations to implement it. Any security approach should be easy to implement to secure their IoT system (Rahman A.F.A, 2016). Therefore, this paper proposed an algorithm that targeted to ease the implementation of IDS on IoT Sensor Node, by using data obtained from an actual environment, and then tested it also on an actual environment without relying on simulated data. An algorithm may be expressed in number of ways including flow charts and pseudo code. There are many other ways of expressing an algorithm but this paper will be focusing on only two of it. An algorithm developed for the IoT should be adhere to criteria of basic algorithm as shown in Table 1.

Table 1. Algorithm Criteria

No.	Algorithm criteria	Description
1	Input	These are the values that are supplied externally to the algorithm.
2	Output	These are the results that are produced by the algorithm.
3	Definiteness	Each step must be clear and unambiguous.
4	Finiteness	The algorithm must terminate after a finite number of steps.
5	Effectiveness	Each step must be basic enough and feasible and it should be practically possible to perform the step.

In this paper, the algorithm is designed specifically for detecting a DoS attack on IoT Sensor node. The algorithm shall be lightweight to adhere to IoT Sensor Node low computational power and low energy consumption. Results from Rahman et. al. 2017 and Daud et. al. 2018 will be used and translated into the algorithm. Rahman et. al. 2017 studies the energy consumption of these two types of cluster without DoS attack (Rahman A.F.A., Ahmad R. and Ramli S.N, 2014). There are two clusters, Cluster A and Cluster B. The Cluster A consist of 5 units of IoT Sensor nodes making up as a single Cluster A, and the second Cluster B consist of 10 units of IoT Sensor nodes making up as a single Cluster B (Rahman A.F.A., Ahmad R. and Ramli S.N, 2014). This research will be used as benchmark to study the energy drop of IoT Sensor Nodes.

Daud et. al. 2018 studies the impact of DoS attacks on these two types of cluster of IoT Sensor nodes by measuring the energy drop in minutes of time (M. Daud, 2018). The experiments conducted in (M. Daud, 2018) used a basic wireless datalogging hardware with a very basic Sensor to Cloud to develop a Smart Water Monitoring System as testbed shown in Figure 2.

The Smart Water Monitoring System testbed is using Wi-Fi IEEE 802.11 that widely uses in cloud architecture and based on the environment implementation. The testbed reads the value of 5 IoT Sensor Nodes, battery, time, pH sensor, oxidation sensor, and turbidity sensor every 5 minutes and sends it to Cloud server listening on TCP port 80 as shown in Figure 3 (Rahman A.F.A., Ahmad R. and Ramli S.N, 2014). The Cloud server will listen for communications on port 80 and print out data received in the standard output (S. Syafiq, 2018). The data recorded by the Smart Water Monitoring System testbed are shown in Figure 3.

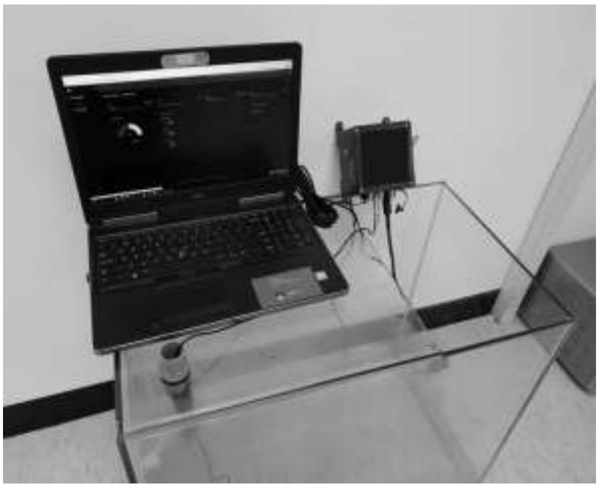
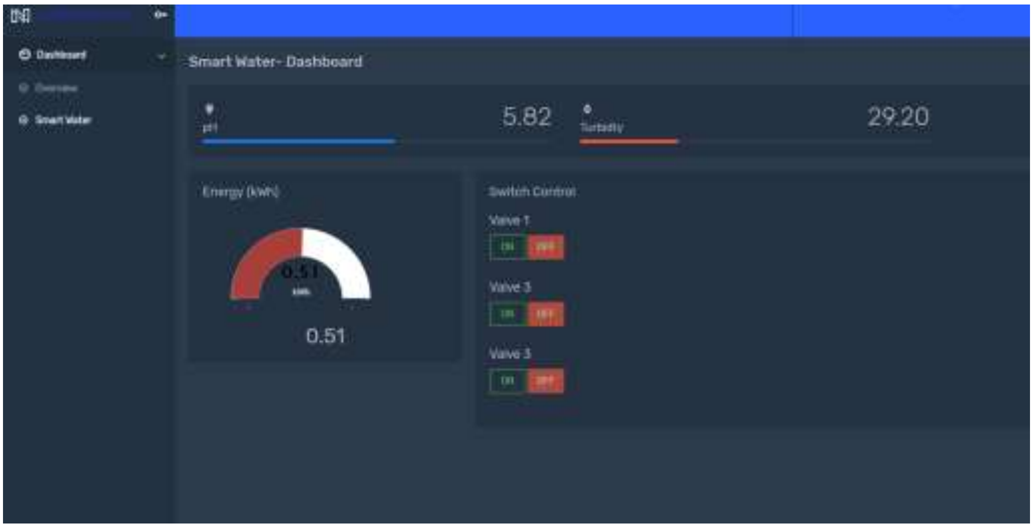


Figure 2. Smart Water Monitoring System Testbed



Smart Water- Dashboard

pH 5.82

Turbidity 29.20

Energy (kWh)

0.51 kWh

0.51

Switch Control

Valve 1 ON OFF

Valve 3 ON OFF

Valve 3 ON OFF

Figure 3. The Cloud shows Sample Data from Smart Water testbed in real time (S. Syafiq, 2018)

This paper will not discuss the details of the Cloud development setup such as the language used and the protocol used to communicate between the cloud and Smart Water Monitoring System testbed. However, the Cloud was set up just to receive data without any optimization or security installed and configured. Since the approach of this paper is to focus on studying the impact of the DoS attacks launch by the Attacker. The detail of each testbed may be referred to the paper by Syamsul et. al. 2018.

Based on Daud et. al. 2018 the energy drop calculation is depending on the relationship of actual energy consumption (volt) per minutes (min). Energy drop may be affected by the number of devices connected, high network utilization and data overload in each cluster node (M. Daud, 2018). However, during a DoS attack, the incoming anomalies packet will affect high energy consumption of infected nodes (M. Daud, 2018). As briefly discussed in the previous section, DoS is an activity to make assets of the IoT Sensor Node unavailable to its intended user. In this paper DoS is an activity to make the IoT Sensor Node unavailable and unable to transmit its signal towards the Cloud. A vulnerable sensor node may become victim of a DoS attack only by receiving too much of the Hello World packets. An attacker may use the Hello World packets and crafted it as malicious packets known as Deauthentication packets in an attempts to flood the network as shown in Figure 4.

In an outbreak environment, energy drop might drag 100% consumption of energy of each infected node (M. Daud, 2018). The energy drops for Cluster A (consist of 5 units of IoT Sensor Node) and Cluster B (consist of 10 units of IoT Sensor Node) shall be referred in Figure 5 and Figure 6.

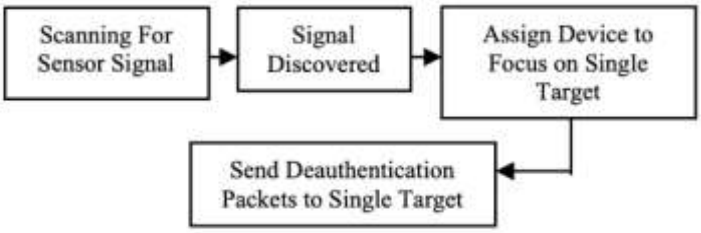

Scanning For Sensor Signal
Signal Discovered
Assign Device to Focus on Single Target
Send Deauthentication Packets to Single Target

Figure 4. Denial of Service Process

For reference, Sensor Node 1 was configured as the DoS victim (can also be referred as malicious node) for both Cluster A and Cluster B. Based on Figure 5 and Figure 6, the Cloud unable to receive any data from Sensor Node 1. This resulting in no data reading received after the fifth minutes of testing. The Cloud indicated that the IoT Sensor Node 1 has no energy and report as zero voltage. The lifespan of Sensor Node 1 is significantly less compared to its neighbours (Sensor Node 2 to Sensor Node 10) and the IoT Sensor Node 1 was completely shut off after the 145 minutes of testing for Cluster A and 125 minutes of testing for Cluster B.

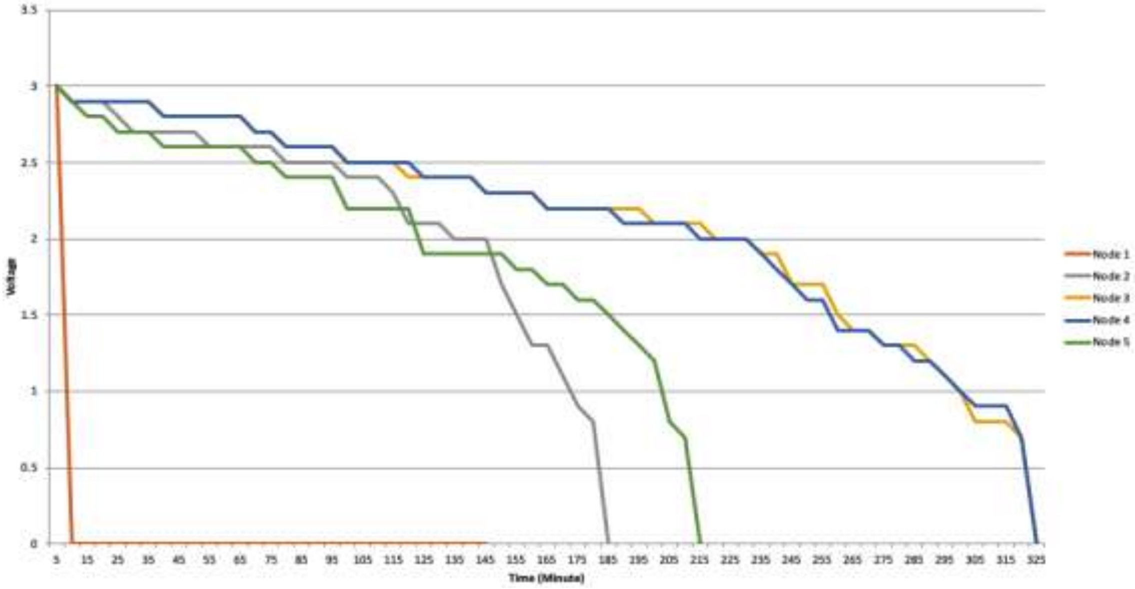


Figure 5. DoS on Cluster A

Table 2. Results from Cluster A and Cluster B

Cluster	Energy Drop	With DoS Attack (minutes)	Without DoS Attack (minutes)
Cluster A (5 Nodes)	0.03%	20	120
	10%	30	720-820
	50%	155-185	1200-1300
Cluster B (10 Nodes)	0.03%	10-20	120
	10%	35-50	720-820
	50%	130-140	1200-1300

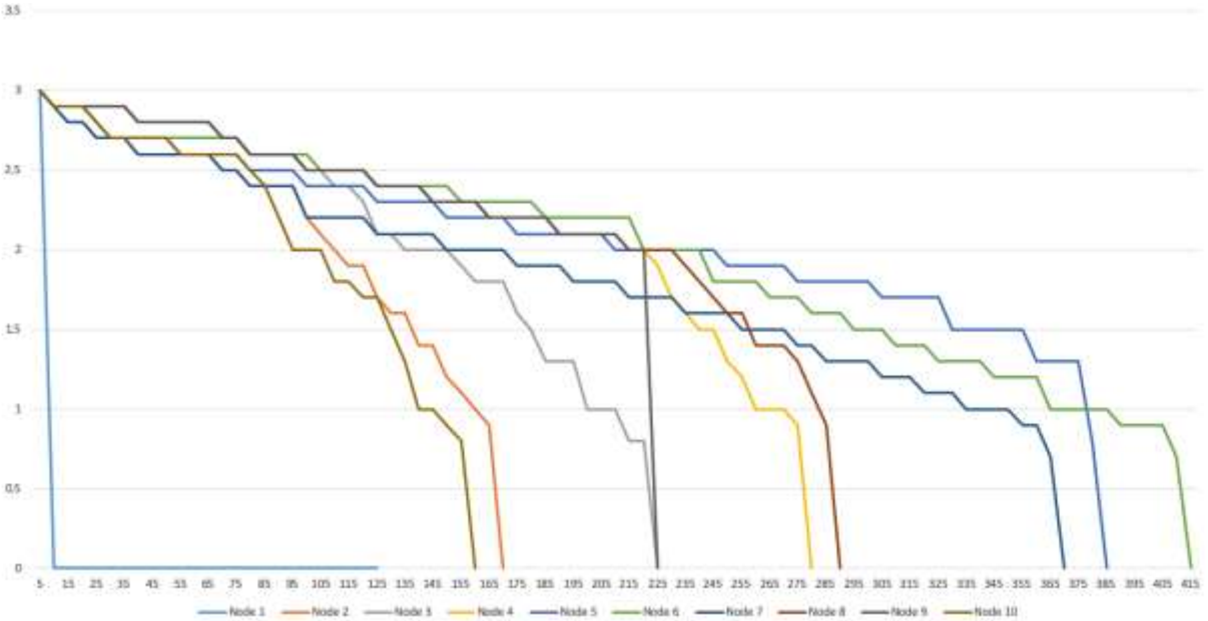


Figure 6. DoS on Cluster B

Based on Table 2, for Cluster A, during a DoS attack, the energy drops 0.03% in 20 minutes time, 10% in 30 minutes and 50% in between 155 to 185 minutes. For Cluster B, during a DoS attack, the energy drops 0.03% in between 10 to 20 minutes time, 10% in between 35 to 50 minutes and 50% in between 130 to 140 minutes. The results from the experiment shown in Figure 5 and Figure 6 shall prove that IoT Sensor Node is susceptible to a DoS attack. This data will be used and translated into an algorithm. Therefore, (M. Daud, 2018) recommends the adoption of security measure to counter the vulnerability, for example the implementation of the various Intrusion Detection System to detect DoS attack patterns and signature, and clustering sensor nodes to increase network lifespan to ensure the availability and increase IoT system lifespan.

5. Proposed IDS Algorithm for IoT Sensor Node

This paper proposed IDS algorithm for IoT Sensor Node as shown in Figure 7. As discussed in previous section, this paper will be focusing in developing a lightweight IDS algorithm for IoT Sensor Node based on previous experiment. The proposed IDS algorithm for IoT Sensor Node shall prevents the abnormal energy consumption by monitoring, calculating and evaluating energy drop from each cluster nodes based on few condition. In abnormal cluster node behaviour, if energy drop is more than

0.03% in less than 20 minutes, anomalies packet will be analysed and abnormalities is classified as an attack. Anomalies packets will be drop and the affected cluster will switch to a different non-overlapping channel to terminate the outbreak.

A pseudo code was developed based on the flow chart, shown in Figure 8. The Pseudo code is a set of sequential written human language instructions, usually numbered, that is used to describe the actions a program will take when it is coded in a programming language. The algorithm in the pseudocode helps programmers or nonprogrammers determine the step-by-step actions a program must take to complete a required or desired action. Programming languages are difficult to read for most people, but pseudocode allows nonprogrammers, such as business analysts, to review the steps to confirm the proposed code matches the coding specifications. By writing the code in human language first, the programmer safeguards against leaving out an important step. Some programmers write pseudocode in a separate document, while others write directly in the programming language using comments before the actual code. This provides a handy reference during coding. The development of pseudo code for this paper is to assists different language programmers to adopt the algorithm in their coding. So that the algorithm shall benefit to more programmers rather than a single programming language.

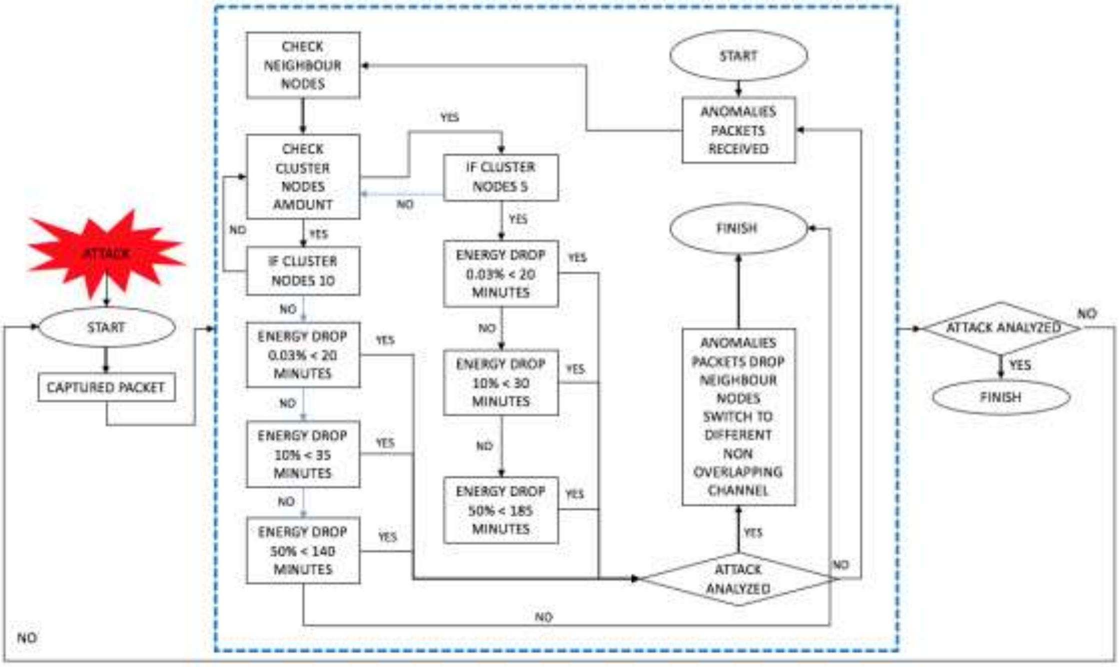
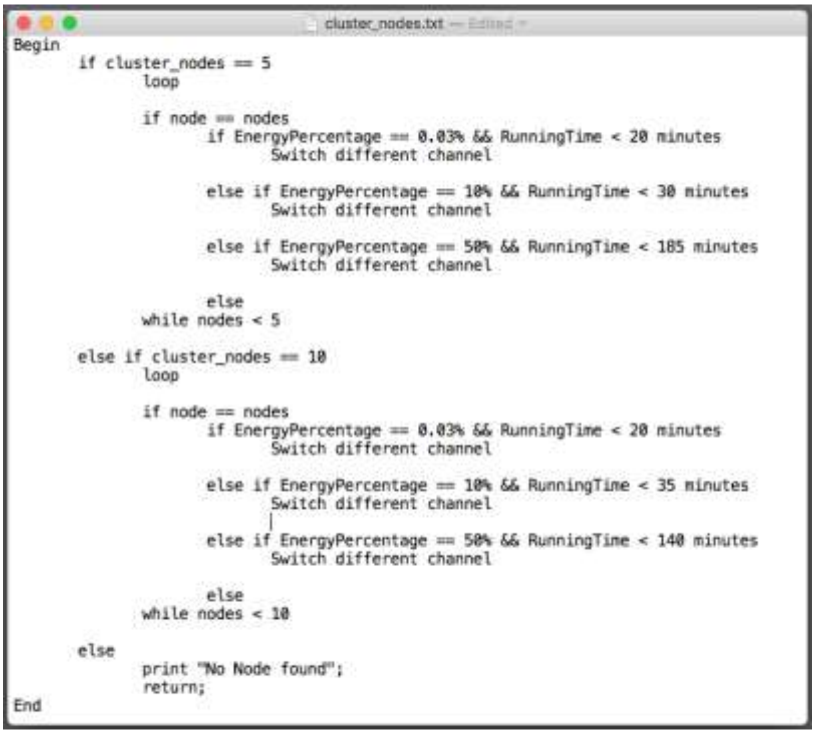

ATTACK
START
CAPTURED PACKET
NO
CHECK NEIGHBOUR NODES
CHECK CLUSTER NODES AMOUNT
YES
NO
IF CLUSTER NODES 5
NO
YES
IF CLUSTER NODES 10
NO
ENERGY DROP 0.03% < 20 MINUTES
YES
NO
ENERGY DROP 10% < 35 MINUTES
YES
NO
ENERGY DROP 50% < 140 MINUTES
YES
ENERGY DROP 0.03% < 20 MINUTES
YES
NO
ENERGY DROP 10% < 30 MINUTES
YES
NO
ENERGY DROP 50% < 185 MINUTES
YES
START
ANOMALIES PACKETS RECEIVED
FINISH
ANOMALIES PACKETS DROP NEIGHBOUR NODES SWITCH TO DIFFERENT NON OVERLAPPING CHANNEL
YES
ATTACK ANALYZED
NO
NO
ATTACK ANALYZED
NO
YES
FINISH

Figure 7. The proposed IDS algorithm for IoT Sensor Node



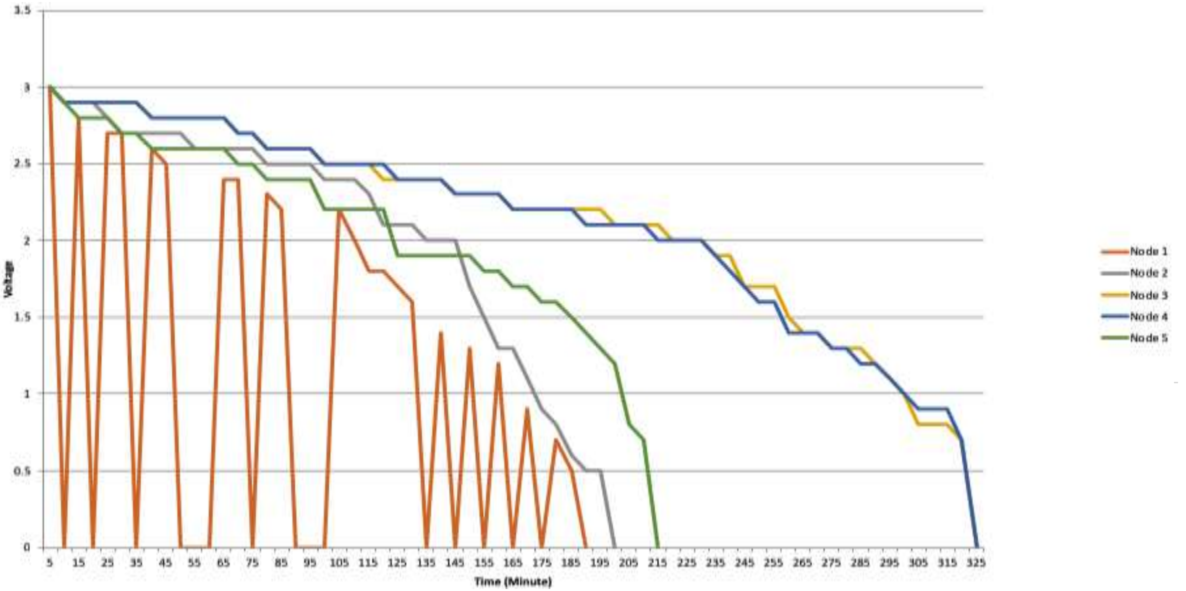
```
Begin
        if cluster_nodes == 5
                loop

                if node == nodes
                        if EnergyPercentage == 0.03% && RunningTime < 20 minutes
                                Switch different channel

                        else if EnergyPercentage == 10% && RunningTime < 30 minutes
                                Switch different channel

                        else if EnergyPercentage == 50% && RunningTime < 185 minutes
                                Switch different channel

                        else
                while nodes < 5

        else if cluster_nodes == 10
                loop

                if node == nodes
                        if EnergyPercentage == 0.03% && RunningTime < 20 minutes
                                Switch different channel

                        else if EnergyPercentage == 10% && RunningTime < 35 minutes
                                Switch different channel

                        else if EnergyPercentage == 50% && RunningTime < 140 minutes
                                Switch different channel

                        else
                while nodes < 10

        else
                print "No Node found";
                return;
End
```

Figure 8. The proposed IDS algorithm for IoT Sensor Node in Pseudo Code

6. Result and Discussion

In this paper, the proposed algorithm designed specifically for mitigating a DoS attack on IoT Sensor node was successfully developed. The lightweight algorithm adhere to IoT Sensor Node low computational power and low energy consumption. Further analysis on the implementation of the proposed algorithm on actual environment using the Smart Water Monitoring System testbed shows a significantly improved lifespan of IoT Sensor Node. From Figure 5 and Figure 6, the Sensor Node 1 was configured as the DoS victim and the lifespan of the sensor node is less then 150 minutes. However, after the implementation of the proposed algorithm, the lifespan of Sensor Node 1 was increased up to 190 minutes. This shows that the algorithm was successfully increased the lifespan of Sensor Node 1.

Further analysis on the Figure 9 shows that the algorithm was successfully sending data to the cloud even during the DoS attack on Sensor Node 1. This result shows that the algorithm was not only improved the lifespan of IoT Sensor Node by 40 minutes, but also improved the quality service of the IoT network. The proposed algorithm, was designed to provide the IoT Sensor Node with the capability of switching to other non-overlapping channel to increase the quality service of IoT



network. Therefore, the objective of using data from previous experiments and translated it to develop a DoS mitigation to secure IoT Sensor Node, thus increased the lifespan of IoT Sensor Nodes was successfully achieved.

Figure 9. Result after the implementation of proposed algorithm

7. Conclusion

All the data and requirements successfully merged and used to developed a lightweight algorithm for DoS mitigation. Even though the improvement of IoT Sensor Node lifespan is not huge, the algorithm may be improved and may become a good foundation for future research. For future research, it is recommended that this lightweight algorithm to be enhance and to further study and improved the effectiveness of this algorithm to sustain an actual DoS Attack in real environment.

Acknowledgements

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) for the support and facilities provided. This research paper is supported by Fundamental Research Grants No: USIM/FRGS/FST/32/51414. We also would like to thank the CyberSecurity Malaysia, an Agency under the Ministry of Communication and Multimedia Malaysia (KKMM) for their contribution, support and facilities provided.

References

Rahman, A.F.A., Halim, A.A., Alwi, N.H.M., Alwi, K.S., Mohamad, F.A., Taufiq, M.N., Mohamad, M.Z. and Abidin, K.A.Z., 2018, June. Measuring Sensor to Cloud Energy Consumption. In Proceedings of the 2018 2nd High Performance Computing and Cluster Technologies Conference (pp. 43-47). ACM.

Daud, M., Rasiah, R., George, M., Asirvatham, D., Rahman, A.F.A. and 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.

Rahman, A.F.A., Daud, M. and Mohamad, M.Z., 2016, March. Securing sensor to cloud ecosystem using internet of things (iot) security framework. In Proceedings of the International Conference on Internet of things and Cloud Computing (p. 79). ACM.

Rahman, A.F.A., Ahmad, R. and Ramli, S.N., 2014, February. Forensics readiness for wireless body area network (WBAN) system. In 16th International Conference on Advanced Communication Technology (pp. 177-180). IEEE.

Syafiq, S., Rahman, A.F.A., Salleh, M.N.T., Mohamad, F.A., Daud, M. and Mohd, M., 2018, November. Comparison on Scorecard and Dashboard in Smart Water Monitoring Application. In Proceedings of the 23rd Conference of Open Innovations Association FRUCT (p. 77). FRUCT Oy.

Sherasiya, T. and Upadhyay, H., 2016. Intrusion detection system for internet of things. Int. J. Adv. Res. Innov. Ideas Educ.(IJARIIE), 2(3).