TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 19, No. 4, August 2021, pp. 1177~1184
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v19i4.18464

Physical cyber-security algorithm for wireless sensor networks

Dhuha Dheyaa Khudhur[1], Muayad Sadik Croock[2]
[1]Computer Engineering Department, University of Technology, Baghdad, Iraq
[2]Control and Systems Engineering Department, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Nov 7, 2020
Revised Mar 17, 2021
Accepted Mar 30, 2021

Keywords:

Cyber-security
DoS attack
Embedded system
MQTT broker

ABSTRACT

Today, the wireless sensor network (WSN) plays an important role in our daily life. In addition, it is used in many applications such as military, medical, greenhouse, and transport. Due to the sending data between its nodes or to the base station requires a connection link, the sensor nodes can be exposed to the many attacks that exploit the weaknesses of the network. One of the most important types of these attacks is the denial of service (DoS). DoS attack exhausts the system's resources that lead the system to be out of service. In this paper, a cyber-security algorithm is proposed for physical level of WSN that adopts message queuing telemetry transport (MQTT) protocol for data transmission and networking. This algorithm predicts the DoS attacks at the first time of happening to be isolated from the WSN. It includes three stages of detecting the attack, predicting the effects of this attack and preventing the attacks by excluding the predicted nodes from the WSN. We applied a type of DoS attack that is a DoS injection attack (DoSIA) on the network protocol. The proposed algorithm is tested by adopting three case studies to cover the most common cases of attacks. The experiment results show the superior of the proposed algorithm in detecting and solving the cyber-attacks.

Corresponding Author:

Dhuha Dheyaa Khudhur
Department of Computer Engineering
University of Technology
Alsinaa Street, Baghdad, Iraq
Email: ce.19.07@grad.uotechnology.edu.iq

1. INTRODUCTION

The technology of wireless sensor network (WSN) has emerged as a suitable option to cover many groundbreaking activities and support the different requirements of our daily life. WSN is a low-cost and less energy consumption wireless network that is designed from thousands of intelligent sensor networks. These sensors are sensing the many different parameters depending on the based environment requirements [1]. Besides, the network may be in multi-levels topology, so the sensor node needs to send its readings to the neighboring nodes that are in turn to send the received data to another node until it reaches the desired place [2].

At the other hand, WSN is widely used for many applications such as military [3], medical care [4], ground earthquake monitoring [5], smart cities [6], greenhouses [7], and air pollution monitoring [8]. These applications are sensitive to their data as well as most or perhaps all of them relate to people's lives. Therefore, securing this data and its confidentiality against any attacker who intercepts it, has become very important. Normally, the attacker tries to change this data or monopolizes some network nodes to failed data inject. That is in turn leads to slow down or stop the entire network. Therefore, the network must be secured from any attackers or unauthorized users [9]-[12] and the infected nodes should be isolated as soon as detected [13]. In addition, there are many problems facing the WSN, as well as most of the systems in our real world, which is the failure [14]. The denial of service (DoS) attack is the most famous attack that is facing the WSN in cyber-security side. This attack aims to take full advantage of weaknesses in the network by sending a lot of unnecessary requests to consume the server's resources. Thus, server or communication networks become unable to deliver the required services [15]-[18].

Due to the importance of keeping the WSN or any other applications free from any problem. So, the minimizing, preventing problems as well as finding optimal solutions for these problems, have been the most interested topic in many researches. We discuss some of the researchers' focus on the methods that were applied to identifying, detect, mitigate, prevent and limit of cyber-attacks that penetrate systems. Kurniawan and Yazid [19], the authors proposed a way to detect and mitigate denial of service attacks on a wireless sensor network. This was done by meaning of an intruder detection system and a blocking application for the node that has been detected as an attacker. In another meaning, all the packets sent from the attacker were dropped to protect the system from all attacks. While the authors of [20] proposed an intruder detection system (IDS) platform based on convolutional neural network (CNN) which is called IDS-CNN to detect DoS attack.

Hasan *et al.* [21], the authors proposed an offline system based on the message queuing telemetry transport (MQTT) that was secured against cyber-attacks to monitor and control air conditioners and coolers in the store. Besides, the exchange of data inside the store took place over an internal network that was not connected to the outside world or another network. They used a single interface to continuously monitor and manage the system to meet its requirements in real-time.

Nurjahan *et al.* [22], the authors proposed a method to detect and prevent cyber-attacks as distributed denial of service (DDoS) and factitious disorder imposed on another (FDIA) on the cyber-physical system. This was done using specialized techniques to detect and identify the attack. Data were collected by LMS filter and they used a Chi-square detector to determine whether an attack occurred or not and fuzzy logic-based attack classifier (FLAC) to determine a particular attack name on the basis of such criteria.

Syed *et al.* [23], the authors proposed a machine learning framework for detecting and evaluating the denial-of-service attacks on the MQTT protocol. They designed and tested the attack to capture normal, offensive traffic, and statistical flow features based on dimension. Besides, the control packet field size/length and MQTT characteristics were evaluated for attack detection.

Nur and Tozal [24], the authors proposed a new probabilistic package scheme of tagging to calculate progress paths from an attacker to a victim location and assign the protection to the upstream internet service providers (ISPs). The obtained results were indicated that the victim location can create a progress path from the attacker after getting 23 packages on average.

Firdous *et al.* [25], the authors proposed the threat model with a particular focus on MQTT-based IoT deployments. They performed tests to measure the effect of DoS attacks on the MQTT broker, which are represented for the two types of attack (SYN flooding and large payload attacks). Potrino *et al.* [26], the authors evaluated and designed a new IoT safety system. The working principle of the system were based on a group of sensors and actuators, which are exchanging messages via the MQTT protocol.

Chiwariro and Rajendran [27], the authors proposed a lightweight (HMAC) or/and data encryption lightweight algorithm. This secret is to ensure the safety and protection of the communication messages via MQTT protocol. Andy *et al.* [28], the authors discussed several reasons for the existence of some IoT systems that do not provide adequate protection. Haripriya and Kulothungan [29], the authors proposed an intrusion detection scheme of the Secure-MQTT that called lightweight fuzzy logic, for detecting malicious behavior during the conversation of IoT devices. The approach suggested uses a fuzzy logic-based approach method to detect the node's malicious activity with the aid of an interpolation process of fuzzy law.

While Sandhu *et al.* [30] proposed an intrusion detection system (IDS) to detect the flooding attack which causes connection failure that was based on a distributed and randomized node presented. Moreover, they are implemented a machine learning technique to improve the network's reliability under a flood attack. Franjić [31] suggested looking at the use of modern computer techniques, through books and information online resources. In addition, detecting malicious software and tools, which are leading to computer sabotage such as identity theft, important data destruction and creating a harmful computer network.

In this paper, a cyber-security algorithm is presented for WSN that uses MQTT networking protocol for communication. It detects the DoS attack at the first stage and then includes the underlying node in prediction process to ensure if its DoS or not before excluding it from WSN. The DoS attacks detection is based on the transmission time (message period) depending on the behavior of DoS attacks.

2. PROPOSED SYSTEM

Figure 1 shows the block diagram of the proposed system prototype that is monitoring and sensing environment parameters of temperature and soil moisture. The WSN structure includes three sensor nodes

(NodeMCU ESP8266) as the microcontroller, two sensors (DS18B20, temperature sensors), two soil moisture sensors, two actuators (LED1, LED2), and a microcomputer (Raspberry pi3). Figure 2 shows the hardware components of the implemented prototype. To send the data between NodeMCU and Raspberry pi3, wireless fidelity (Wi-Fi) connection, and internet of things (IoT) MQTT protocol are applied that adopts TCP/IP and (publish/subscribe) protocol.

The exchanging data are received and analyzed by the base station (represented in a Raspberry Pi). By inspecting the obtained data in real-time mode, the monitoring process is conducted here. In addition, we apply DoSIA for the above-mentioned environment parameters from one of our network nodes against the MQTT Broker. We adopt python programming language in Raspberry pi 3 to build the proposed algorithm.

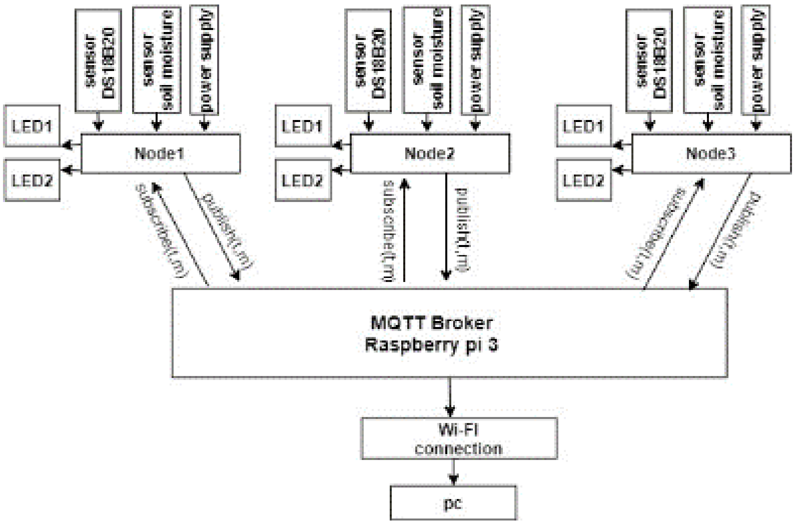


Figure 1. The block diagram of the proposed system

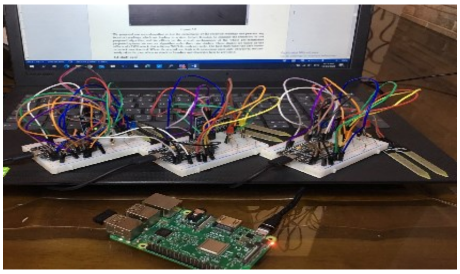


Figure 2. Used hardware components

As mentioned above, we proposed an algorithm to detect, mitigate, and prevent the effect of DoS attack on WSN. This algorithm tests the data received from three nodes by examining the difference of the received time as well as the message size between two consecutive messages within specified thresholds. The first threshold is taken according to the minimum time differences between all the pre-received readings from included nodes, which is 10 seconds. Moreover, the second threshold considers the difference of message size between two selected types of reading messages. We meant by message size is the possible readings range of maximum and minimum values. These thresholds increase the possibility of being such node is a DoS attack. This/these node (s) is/are entered to prediction stage to decided later to be DoS or not. The decision is based on continuing the same crossing of the two thresholds. Figure 3 shows a flow chart of the proposed algorithm, which can be summarized in the following:

- Receiving data from the nodes by the Raspberry Pi (base station).
- We test the incoming data by examining the time difference and the size of the message compared to the threshold for the sequential messages respectively. It is important to note that the nodes send their readings every 10 seconds to be received by base station at the same time.
- If a difference is found between sequential messages, then we put the node under DoS suspicion and increase the suspicion counter by one. The Raspberry pi 3 returns to receiving the next data from the node.

– If the suspicion counter of the node is greater than or equal to the total tolerance for the wrong reading, we block the suspicion node's IP address and consider it as a DoS attack. This node is disconnected from the WSN by blocking its IP address.

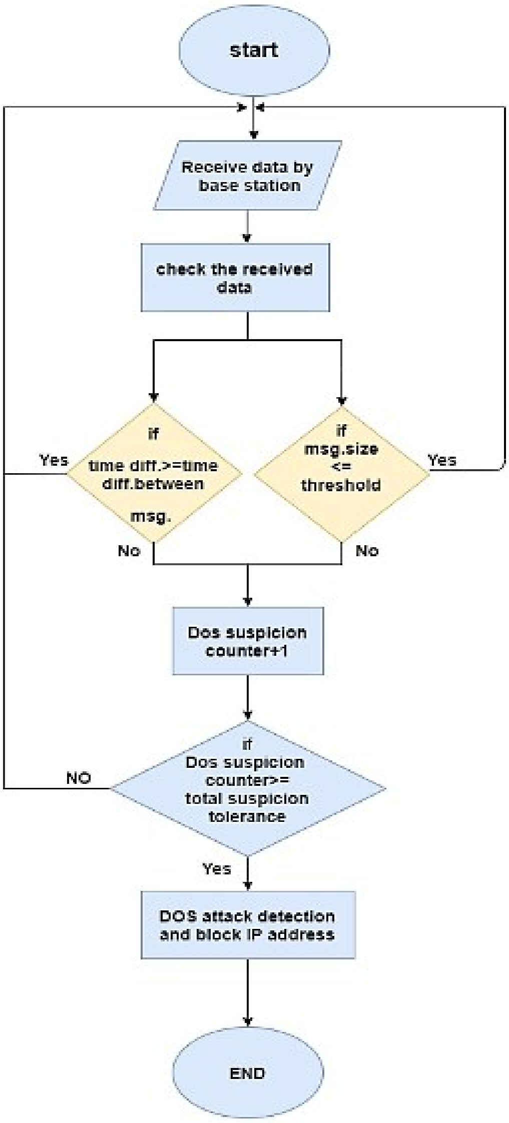

start
Receive data by base station
check the received data
if time diff.>=time diff.between msg.
if msg.size <= threshold
Yes
Yes
No
No
Dos suspicion counter+1
if Dos suspicion counter>= total suspicion tolerance
NO
Yes
DOS attack detection and block IP address
END

Figure 3. The flow chart of the proposed algorithm

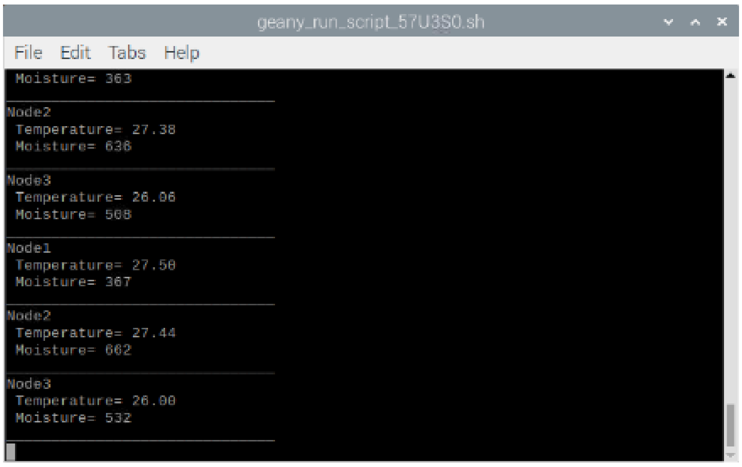
3. RESULTS AND ANALYSIS

As mention previously, our proposed system is composed of three nodes connected to the network protocol (MQTT) that is receiving their reading data. Besides, it sends back these readings to the base station (Raspberry Pi3). Figure 4 shows the Raspberry Pi3 window which is remotely accessed by the virtual network computing (VNC) viewer platform, that is installed on the PC. Through this platform, python code is responsible for displaying the sensor readings for three nodes via the MQTT broker.

The proposed algorithm tests the correctness of the received readings and prevent any incorrect readings which are leading to system failure. Besides, to examine the reliability of the proposed algorithm and its effects on the overall performance of the whole pre-mentioned proposed system, three test case studies are adopted. These studies are based on the effects of a DoS attack that is facing WSN through any node. The first study takes the case where no attack was detected. While, the second one deals with suspicious cases only. Moreover, the last study takes the case when an attack is founding and illustrated how to prevent it.

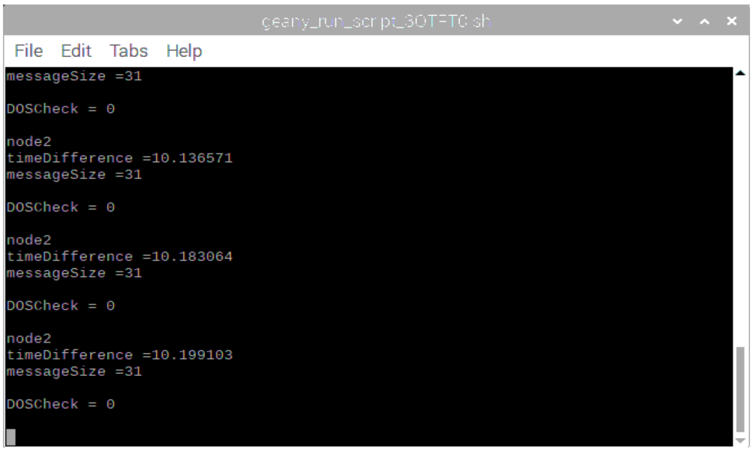
3.1. Case study one

This study includes testing the received data, received from any node through the above-mentioned algorithm. If there is no difference found, the WSN works normally and the nodes send readings every 10 seconds that are received by base station as well. Thus, this case study is not considered as a DoS attack (DoS check=0) as shown Figure 5. As a result, the WSN works normally and involved nodes exchange data smoothly as shown Figure 6.



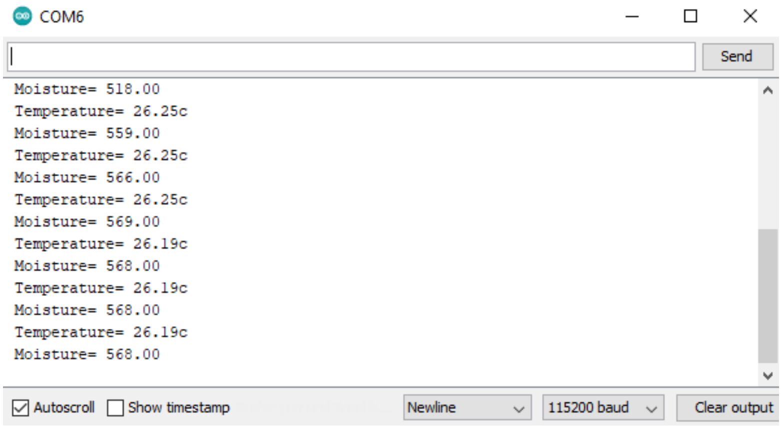
```
 Moisture= 363
______________________________
Node2
 Temperature= 27.38
 Moisture= 638
______________________________
Node3
 Temperature= 26.06
 Moisture= 508
______________________________
Node1
 Temperature= 27.50
 Moisture= 367
______________________________
Node2
 Temperature= 27.44
 Moisture= 602
______________________________
Node3
 Temperature= 26.00
 Moisture= 532
______________________________
```

Figure 4. The Raspberry Pi3 window



```
messageSize =31

DOSCheck = 0

node2
timeDifference =10.136571
messageSize =31

DOSCheck = 0

node2
timeDifference =10.183064
messageSize =31

DOSCheck = 0

node2
timeDifference =10.199103
messageSize =31

DOSCheck = 0
```

Figure 5. Case study one: normal message receiving

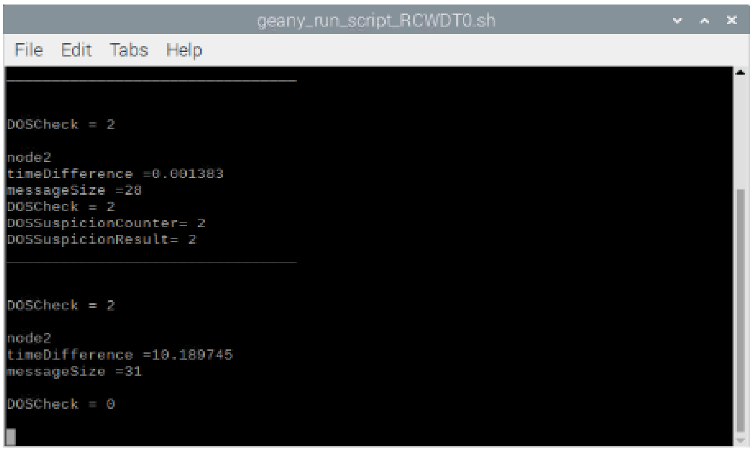


```
Moisture= 518.00
Temperature= 26.25c
Moisture= 559.00
Temperature= 26.25c
Moisture= 566.00
Temperature= 26.25c
Moisture= 569.00
Temperature= 26.19c
Moisture= 568.00
Temperature= 26.19c
Moisture= 568.00
Temperature= 26.19c
Moisture= 568.00
```

Figure 6. Case study one: normal serial monitoring output

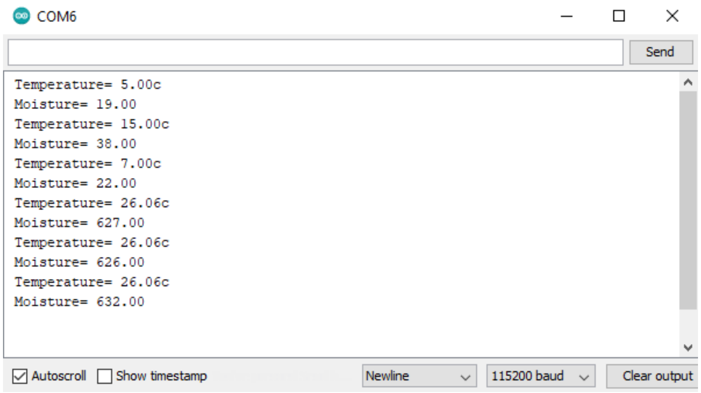
3.2. Case study two

This study includes testing the received data from any node through the above-mentioned algorithm. If a difference is found between the received time and the message size for such node, this node is a DoS suspicion that is putted under monitoring. It is important to note that the normal thresholds of message time difference and size are 10 seconds and 31, respectively. After receiving two sequential messages from the DoS suspicion node (DoS check=2), it starts to send messages with normal thresholds. Therefore, this node is excluded from the DoS suspicion list and return back to accepted list and set (DoS check=0) as shown Figure 7. As a result, this node keeps going to send its reading to the base station, as shown Figure 8.



```
________________________________________


DOSCheck = 2

node2
timeDifference =0.001383
messageSize =28
DOSCheck = 2
DOSSuspicionCounter= 2
DOSSuspicionResult= 2

________________________________________


DOSCheck = 2

node2
timeDifference =10.189745
messageSize =31

DOSCheck = 0
```

Figure 7. Case study two, DoS suspicion to normal

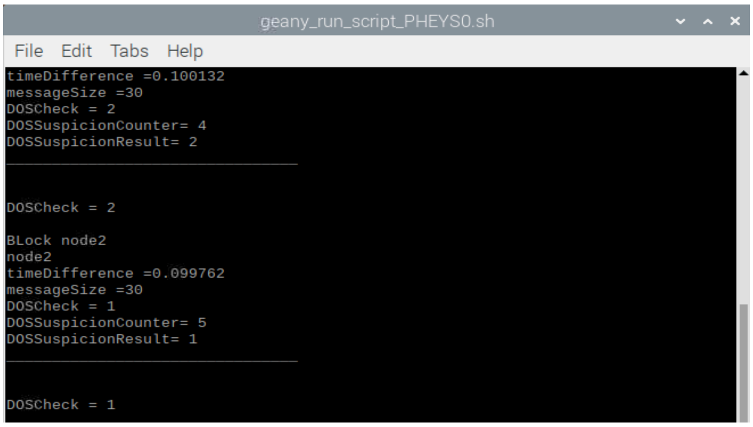


```
Temperature= 5.00c
Moisture= 19.00
Temperature= 15.00c
Moisture= 38.00
Temperature= 7.00c
Moisture= 22.00
Temperature= 26.06c
Moisture= 627.00
Temperature= 26.06c
Moisture= 626.00
Temperature= 26.06c
Moisture= 632.00
```

Figure 8. Case study two, normal serial monitoring output

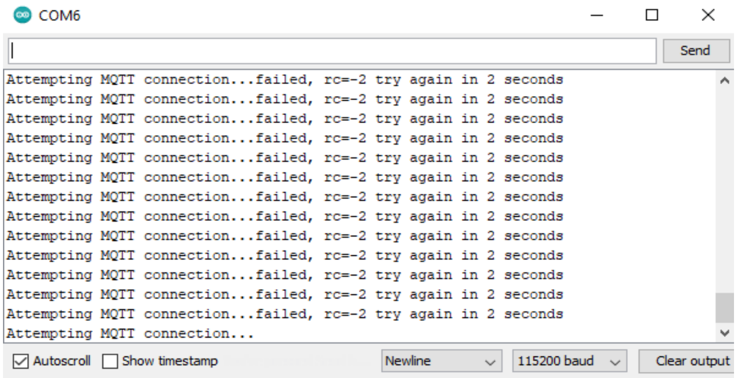
3.3. Case study three

This study addresses the effect of DoSIA Attack on the MQTT Broker installed on Raspberry Pi3 (base station). This attack is injected into one of WSN nodes to test the vulnerabilities of MQTT Broker and how it protected. As mentioned above, the proposed algorithm detects this type of attack by monitoring the time difference and the size of the message compared to the threshold. If a difference is found. Thus, this node is DoS suspicion to be monitored for five received messages. If the crossing of thresholds is continued, then the algorithm decides this node to be DoS attacker and should be isolated from the considered WSN and set (DoS check=1). As a result, its IP address is blocked to avoid receiving other data from it as shown in Figure 9. Finally, this node cannot send data anymore as shown in Figure 10.



```
timeDifference =0.100132
messageSize =30
DOSCheck = 2
DOSSuspicionCounter= 4
DOSSuspicionResult= 2
________________________________________


DOSCheck = 2

BLock node2
node2
timeDifference =0.099762
messageSize =30
DOSCheck = 1
DOSSuspicionCounter= 5
DOSSuspicionResult= 1
________________________________________


DOSCheck = 1
```

Figure 9. Case study three, DoS detection of node 2



```
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...failed, rc=-2 try again in 2 seconds
Attempting MQTT connection...
```

☑ Autoscroll ☐ Show timestamp Newline 115200 baud

Figure 10. Case study three, node2 cannot send data

4. CONCLUSION

A cyber-security algorithm for WSN was proposed to deal with DoS attacks. It used two important thresholds to detect the DoS attacks, which are the time difference and size of received messages from included nodes. The proposed algorithm included detection stage, prediction stage and isolating stage. The detection was processed for the first detection of crossing the threshold, while the prediction is performed for monitoring the suspicion node for five messages, and the isolation is applied for ensured DoS nodes. The proposed algorithm showed great results in detecting and preventing the wrong injection of data. Thus, it is making the system drive a clean and correct dataset and keep service resources out from exploited.

REFERENCES

[1] A. Kore and D. Kadam, “IoT Based Real Time Greenhouse monitoring system using Raspberry Pi,” *International Research Journal of Engineering and Technology (IRJET)*, vol. 06, no. 04, 2019.

[2] S. G. Nikhade, "Wireless sensor network system using Raspberry Pi and zigbee for environmental monitoring applications," *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM),* Chennai, 2015, pp. 376-381, doi: 10.1109/ICSTM.2015.7225445.

[3] I. Ahmad, K. Shah and S. Ullah, "Military Applications using Wireless Sensor Networks: A survey," *International Journal of Engineering Science and Computing*, vol. 6, no. 6, pp. 7039-7043, June 2016, doi: 10.4010/2016.1678.

[4] N. S. Ali, Z. A. A. Alyasseri, and A. Abdulmohson, “Real-Time Heart Pulse Monitoring Technique Using Wireless Sensor Network and Mobile Application,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 8, no. 6, pp. 5118-512, Dec. 2018, doi:10.11591/ijece.v8i6.pp5118-5126.

[5] M. ur Rahman, S. Rahman, S. Mansoor, V. Deep, and M. Aashkaar, “Implementation of ICT and wireless sensor networks for earthquake alert and disaster management in earthquake prone areas,” *Procedia Comput. Sci.,* vol. 85, pp. 92-99, 2016, doi: 10.1016/j.procs.2016.05.184.

[6] B. Kantarci and S. Oktug, “Special issue: Wireless sensor and actuator networks for smart cities,” *J. Sens. Actuator Netw.*, vol. 7, no. 4, pp. 1-5, 2018, doi: 10.3390/jsan7040049.

[7] A. Kochhar and N. Kumar, “Wireless sensor networks for greenhouses: An end-to-end review,” Computers and Electronics in Agriculture, vol. 163, Aug. 2019, doi: 10.1016/j.compag.2019.104877.

[8] A. Chaturvedi and L. Shrivastava, "IOT Based Wireless Sensor Network for Air Pollution Monitoring," *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT),* Apr. 2020, doi: 10.1109/csnt48778.2020.9115733.

[9] A. Pedersen, "Altering Perceptions, Visualizing Sub-ground Metal Objects," *Emerging Science Journal*, vol. 4, no. 3, pp. 205-213, Jun. 2020, doi: 10.28991/esj-2020-01224.

[10] B. Fazelabdolabadi and M. H. Golestan, "Towards Bayesian Quantification of Permeability in Micro-scale Porous Structures – The Database of Micro Networks," *HighTech and Innovation Journal*, vol. 1, no. 4, pp. 148-160, Dec. 2020, doi: 10.28991/hij-2020-01-04-02.

[11] T. Chu, A. Y. Chua, and E. L. Secco, "A wearable MYO gesture armband controlling Sphero BB-8 robot," *HighTech. Innov. J.,* vol. 1, no. 4, pp. 179-186, 2020, doi: 10.28991/HIJ-2020-01-04-05.

[12] A. A. Astaneh and S. Gheisari, "Review and Comparison of Routing Metrics in Cognitive Radio Networks," *Emerging Science Journal*, vol. 2, no. 4, pp. 191-201, Sep. 2018, doi: 10.28991/esj-2018-01143.

[13] A. S. A. Daia, R. A. Ramadan, and M. B. Fayek, "Sensor Networks Attacks Classifications and Mitigation," Annals of Emerging Technologies in Computing, vol. 2, no. 4, pp. 28-43, Oct. 2018, doi:10.33166/aetic.2018.04.003.

[14] M. S. Croock, S. D. Khuder, and Z. A. Hassan, "Self-checking method for fault tolerance solution in wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 4, pp. 4416-4425, Aug. 2020, doi:10.11591/ijece.v10i4.pp4416-4425.

[15] Z. A. Baig, S. Sanguanpong, S. N. Firdous, V. N. VO, T. G. Nguyen, and C. So-In, "Averaged dependence estimators for DoS attack detection in IoT networks," *Future Generation Computer Systems*, vol. 102, pp. 198-209, Jan. 2020, doi: 10.1016/j.future.2019.08.007.

[16] S. Patil and S. Chaudhari, "DoS attack prevention technique in Wireless Sensor Networks," *Procedia Comput. Sci.,* vol. 79, pp. 715-721, Feb. 2016, doi: 10.1016/j.procs.2016.03.094.

[17] L. Cao, X. Jiang, Y. Zhao, S. Wang, D. You and X. Xu, "A Survey of Network Attacks on Cyber-Physical Systems," *IEEE Access*, vol. 8, pp. 44219-44227, 2020, doi: 10.1109/ACCESS.2020.2977423.

[18] Ž. Gavrić and D. Simić, "Overview of DoS attacks on wireless sensor networks and experimental results for simulation of interference attacks," Ingeniería e Investigación, vol. 38, no. 1, pp. 130-138, Jan. 2018, doi: 10.15446/ing.investig.v38n1.65453.

[19] M. T. Kurniawan and S. Yazid, "Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System," *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE),* Jun. 2020, doi: 10.1109/icecce49384.2020.9179255.

[20] S.-N. Nguyen, V.-Q. Nguyen, J. Choi, and K. Kim, "Design and implementation of intrusion detection system using convolutional neural network for DoS detection," in *Proceedings of the 2nd International Conference on Machine Learning and Soft Computing - ICMLSC '18*, 2018, doi: 10.1145/3184066.3184089.

[21] N. I. Hasan, M. T. Hasan, N. H. Turja, R. Raiyan, S. Saha, and M. F. Hossain, "A Cyber-Secured MQTT based Offline Automation System," *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET),* Mar. 2019, doi: 10.1109/wispnet45539.2019.9032743.

[22] Nurjahan, F. Nizam, S. Chaki, S. Al Mamun and M. S. Kaiser, "Attack detection and prevention in the Cyber Physical System," *2016 International Conference on Computer Communication and Informatics (ICCCI),* Coimbatore, 2016, pp. 1-6, doi: 10.1109/ICCCI.2016.7480022.

[23] N. F. Syed, Z. Baig, A. Ibrahim, and C. Valli, "Denial of service attack detection through machine learning for the IoT," *Journal of Information and Telecommunication*, vol. 4, no. 4, pp. 482-503, Jun. 2020, doi:10.1080/24751839.2020.1767484.

[24] A. Y. Nur and M. E. Tozal, "Defending Cyber-Physical Systems against DoS Attacks," *2016 IEEE International Conference on Smart Computing (SMARTCOMP),* May 2016, doi: 10.1109/smartcomp.2016.7501685.

[25] S. N. Firdous, Z. Baig, C. Valli, and A. Ibrahim, "Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol," *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jun. 2017, doi: 10.1109/ithings-greencom-cpscom-smartdata.2017.115.

[26] G. Potrino, F. de Rango, and A. F. Santamaria, "Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker," *2019 IEEE Wireless Communications and Networking Conference (WCNC),* Apr. 2019, doi: 10.1109/wcnc.2019.8885553.

[27] R. Chiwariro and S. Rajendran, "Security in Publish/Subscribe Protocol for Internet of Things," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 16, pp. 231-242, 2018.

[28] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack Scenarios and Security Analysis of MQTT Communication Protocol in IoT System," *Proceeding of the Electrical Engineering Computer Science and Informatics*, vol. 4, no. 1, Oct. 2017, doi: 10.11591/eecsi.v4.1064.

[29] A. P. Haripriya and K. Kulothungan, "Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1-15, Apr. 2019, doi: 10.1186/s13638-019-1402-8.

[30] J. K. Sandhu, A. K. Verma, and P. S. Rana, "Enhancing dependability of wireless sensor network under flooding attack: a machine learning perspective," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 33, no. 2, pp. 73-89, 2020, doi: 10.1504/ijahuc.2020.105461.

[31] S. Franjić, "Cybercrime is Very Dangerous Form of Criminal Behavior and Cybersecurity," *Emerging Science Journal*, vol. 4, pp. 18–26, Oct. 2020.