Computers, Materials & Continua
DOI:10.32604/cmc.2022.023399
Article

Tech Science Press

An IoT-Based Intrusion Detection System Approach for TCP SYN Attacks

Abdelwahed Berguiga* **and Ahlem Harchay**

Department of Computer Science, College of Science and Arts in Gurayat, Jouf University, Sakakah, Saudi Arabia
*Corresponding Author: Abdelwahed Berguiga. Email: awberguiga@ju.edu.sa
Received: 06 September 2021; Accepted: 27 October 2021

Abstract: The success of Internet of Things (IoT) deployment has emerged important smart applications. These applications are running independently on different platforms, almost everywhere in the world. Internet of Medical Things (IoMT), also referred as the healthcare Internet of Things, is the most widely deployed application against COVID-19 and offering extensive healthcare services that are connected to the healthcare information technologies systems. Indeed, with the impact of the COVID-19 pandemic, a large number of interconnected devices designed to create smart networks. These networks monitor patients from remote locations as well as tracking medication orders. However, IoT may be jeopardized by attacks such as TCP SYN flooding and sinkhole attacks. In this paper, we address the issue of detecting Denial of Service attacks performed by TCP SYN flooding attacker nodes. For this purpose, we develop a new algorithm for Intrusion Detection System (IDS) to detect malicious activities in the Internet of Medical Things. The proposed scheme minimizes as possible the number of attacks to ensure data security, and preserve confidentiality of gathered data. In order to check the viability of our approach, we evaluate analytically and via simulations the performance of our proposed solution under different probability of attacks.

Keywords: IoT; intrusion detection system; denial-of-service; TCP SYN flooding; attacks

1 Introduction

Internet of Things has become as a powerful industrial revolution by which a huge of heterogeneous objects such as sensors, mobile devices, cameras, and vehicles can connect with each other via Internet. These objects collect immense kinds of data and being further processed and analyzed in order to extract useful information. Internet of Things (IoT), specifically the Internet of Medical Things (IoMT) [1], is gaining importance to deal with the unprecedented COVID-19 pandemic. IoMT strategy has now become more exploring in many solutions such as heart rate variability (HRV), respiratory rate variability (RRV) affected by COVID-19 outbreak. Medical and healthcare

professionals monitor and control vital signs of patients remotely and guarantees giving patients medicines and getting complete health care [2–4]. Indeed, monitor remotely the status of infected patients, collect data, and analyze data deploy the concept of interconnected network for an effective flow and exchange of data. This enable interconnected devices/operations to be in connection with the service benefactors for discussing any issue and cooperation remotely [5]. However, given that these devices are often constrained by limited resources (processing, memory, and power) a new routing protocol for Low-Power and Lossy network (RPL) was proposed as a standard for such constrained environments. Compared to classical routing protocols, RPL has many advantages such as energy efficiency and it is designed specifically for Low-Power and Lossy networks [6]. However, as aforementioned, due to their limited capacity in terms of power, memory and computational capacity, RPL, like AODV protocol, does not provide security for these devices so these Low Lossy networks may be exposed to various threats and security attacks [7] such as sinkhole attacks, selective forward attacks, Sybil attack, replay attack, Denial-of-Service (DoS) attack, neighbor attack, etc. Therefore, an Intrusion Detection System (IDS), also known as first line of defense is typically used to ensure network security where all mobile objects operate in safe mode. The function of IDS is to monitor network operations and detect intrusions in network systems. In this article, we focus on security service attack, namely TCP SYN flooding attack, that is a subclass of Denial-of-Service attack. TCP SYN flooding attack is the critical DoS attack that can degrade the performance and lifetime of the network drastically. In TCP SYN attack, the attacker sends multiple TCP request packets to initiate the connection and thus resulting in slow down the distant node and consequently can weaken the network performance.

The present paper is organized as follows: In Section 2, we review the various state-of-the-art literature on attack classification in IoT network. In Section 3, we analyzed and discussed analytically of DoS attack on network performance. Then, we introduce the proposed algorithm that can be implemented on IoT environment. The simulation implementation and results are presented and evaluated in Section 4. Finally, we conclude this paper in Section 5.

2 Related Works

Routing Protocol for Low-Power and Lossy Networks (RPL) is a new standard on Internet of Things (IoT) [8]. Since its standardization by the IETF in 2011, RPL has rapidly become the routing protocol in the world of tiny and embedded networking device. RPL deploys the paradigm of a Destination-Oriented Directed Acyclic Graph (DODAG) that has a tree-like structure connected to a data sink of the graph, named DODAG root [9,10]. This root is the final destination in the network architecture and it connects others descendant nodes to the Internet. Fig. 1 illustrates an example of an RPL network that allows creating groups, known as instances, of multiple loop-free routing topologies [11]. At the same time, an RPL node has the possibility to join to many instances on the network but only join one DODAG in an instance. On RPL networks, three traffic patterns are possible: (i) multipoint-to-point traffic (MP2P) where traffic is sent in upward routes, i.e., from end nodes to the root; (ii) point-to-multipoint traffic (P2MP) where traffic is sent in downward routes, i.e., from the root to end nodes; and (iii) point-to-point traffic (P2P) from one RPL node to another one on the same DODAG.

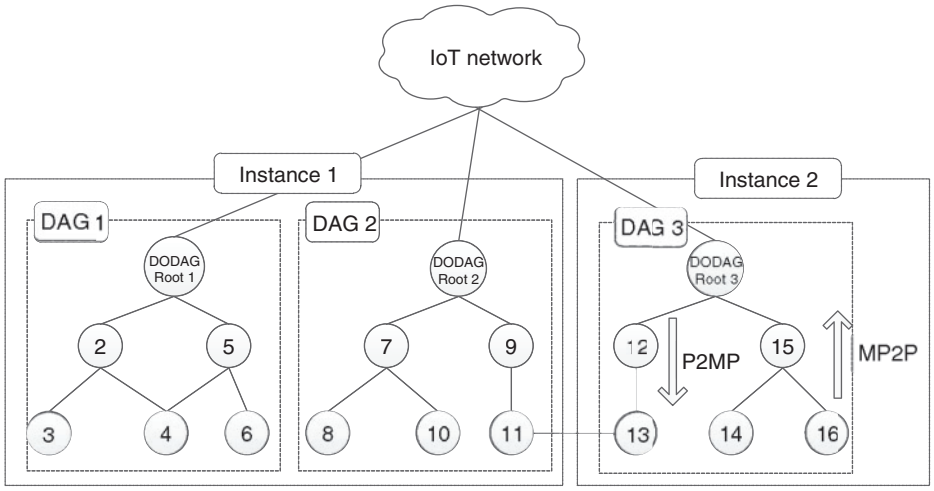

Figure 1: A RPL network with three DODAGs in two instances

The root node on the DODAG acts as a Border Router (BR) to connect RPL nodes together and to the Internet. As aforementioned, given that RPL does not offer any security policies to low power networks, IoT services are vulnerable to a large variety of intruders and security attacks [12]. Such attacks can be external attacks as well as internal attacks and has as targeting the exhaustion of network resources (energy, memory and power). According to this vulnerability, we can note some of the particular topology attacks including hello flood, Sinkhole, Sybil, Wormhole, Blackhole, etc. Therefore, IDS solutions are efficient to monitor the network behavior and detect the compromised nodes. Pongle et al. [13] survey four most widely used approaches in IDS; Event detection-based IDS, Signature detection-based IDS, Host based IDS, and Specification based IDS. In event detection method, IDS captures the event triggered in the network to analyze them. If the IDS detect an attack, it will raise alarm. Jun et al. [14] propose a specification of Event detection-based IDS where event pattern is defined and stored in database using SQL and EPL (Event Processing Language). In signature-based IDS system approach, a signature pattern is compared with one stored in the IDS internal database. If the pattern is matching, an alarm will be generated. Oh et al. [15] proposed an example of signature-based IDS for resource-constrained sensor network connected to IP network. Authors in [16] have proposed IDS of immunity-based intrusion detection technology and dynamic defense. Indeed, self-learning and self-adaptation is employed dynamically to detect malicious events. In host-based IDS method, known also as hybrid method, a detection module is implemented in every device of the RPL network. Each node on the network acts as a monitoring node. Authors in [17] have proposed host-based IDS for intrusion detection on RPL networks such as forged or altered information, and selective-forwarding. The proposed overhead is small enough to deploy it on low power networks. In specification-based IDS scheme, also known as software engineering based [18] or Finite state machine (FSM) based IDS [19], a network expert defines manually a set of rules that are used as references to the behavior of network peripherals. Intrusion is detected by the IDS when there is a suspicious activity and deviation from the defined rules. The proposed scheme is tested on the Contiki platform. An abstract of the normal operations of a network is built manually and malicious activities are detected based on some specifications for RPL. However, the proposed scheme is described without no validation nor simulations has been proposed. In [20] Abduvaliyev et al. deploy the combination between anomaly and misuse based intrusion detection techniques (defined as hybrid intrusion detection system). Indeed, this technique incurs high detection

and low false positive rates. Shin et al. [21] developed IDS for wireless industrial sensor networks (WISNs). They proposed a hierarchical framework for intrusion detection and prevention for WISNs. Through simulations on NesC simulator, authors present detailed results about the accuracy of the proposed scheme. Loulianou et al. [22] proposed signature-based IDS to detect DDoS attacks in IoT networks. The proposed scheme comprises two units, namely IDS router and IDS detectors. These two modules are deployed in a hybrid manner. The IDS router, placed on the border gateway, performs detection and firewall functionalities. IDS detectors employ sensors to monitor traffic and forward information about malicious nodes to the gateway for further action. Authors in [23] proposed new knowledge-driven IDS, namely Kalis, which combines signature rules and anomaly detection processes to detect attacks on IoT networks. Indeed, Kalis collect autonomously knowledge about features and entities of the monitored network and prevents DoS attacks. According to the authors, the proposed system enables detection of DoS and routing attacks. However, Kalis requires installation of particular detection modules to focuses on routing attacks that limits its accuracy. Tab. 1 gives the summary of attack on RPL with method used to detect intruders.

Table 1: Summary of IDS Schemes

Proposed scheme	Security threat	Detection method	Placement	Topology	Validation strategy
Jun et al. [14]	-	Anomaly-based	Centralized	Single hop	-
Oh et al. [15]	Routing Attacks	Signature-based	Distributed	Multi-hop	Simulation
Liu et al. [16]	-	Hybrid	Hybrid	-	None
Raza et al. [17]	Routing attacks	Hybrid	Distributed	Multi-hop	Simulation
Le et al. [18]	Routing attacks	Anomaly-based	Distributed	Multi-hop	Simulation
Le et al. [19]	-	Specification-based	Hybrid	-	None
Abduvaliyev et al. [20]	DoS attacks	Hybrid	Centralized	Single hop	Simulation
Shin et al. [21]	DoS attacks	Anomaly-based	Centralized	Single hop	Simulation
Loulianou et al. [22]	Routing attacks	Signature-based	Hybrid	Multi-hop	Simulation
Midi et al. [23]	Routing attacks, DoS attacks	Hybrid	Centralized	Multi-hop	Simulation
Proposed scheme	DoS attacks	Anomaly-based	Hybrid	Multi-hop	Simulation

3 Contribution

Our proposal consists of an IDS which prevents any disruption against the network. It is considered as the first line of defense for security by monitoring network traffic. All network activities are analyzed and any abnormal traffic or malicious activity will be alerted by the IDS and appropriate actions should be taken. The main objective of our proposed scheme is to detect earlier TCP SYN attacks. Indeed, in this paper, an IDS is proposed to detect TCP SYN attack in IoT networks. Fig. 2 illustrates the application scenario used in this study. We consider the case of remote medical monitoring application. We adopt the case of a patient that wears different wireless sensors collecting vital recordings such as respiration rate, saturation of peripheral oxygen (SpO2), electrocardiography (ECG), accelerometers, gyroscopes, etc. These sensor nodes are attached to the patient's body and communicate, via access point, with servers in cloud. An attack model is composed of distant malicious attacker that is expected to act as a simple healthcare professional, but he violates the security policy and sending spoofed SYN packets to the victim sensor. The malicious healthcare professional starts a transmission by sending a SYN to the distant server. Then, the server allocates a buffer for the distant client and a SYN Acknowledge (ACK) packet is sent to the client in order to complete the connection setup. When the connection is complete, the attacker floods the victim with a large volume of traffic and continuous data stream disables the victim from providing services to the legitimate users (legitimate healthcare professional).

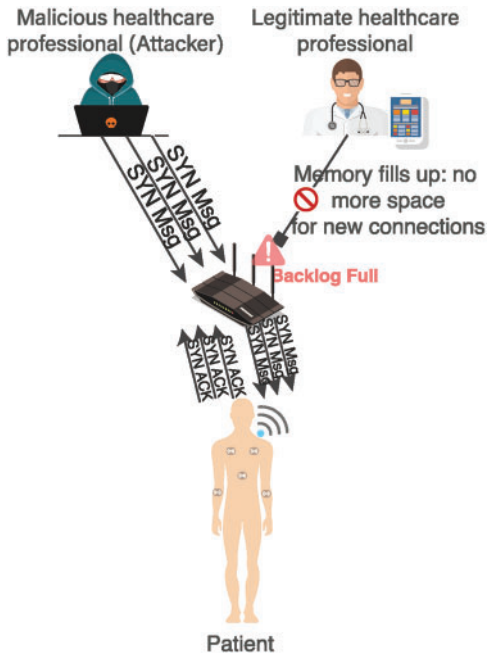

Figure 2: Remote medical monitoring application

The proposed solution in this paper aims to detect vulnerabilities to such attacks. We analyze and evaluate the proposed detection capability. In fact, detecting attack is considered as a first step towards obtaining a reliable estimate about TCP handshake protocol, which in turn facilitates eliminating the disruptive effects of missed-detection and false alarm. To satisfy this requirement and assuring good estimation performance of our proposed scheme, we use a relevant metric as a probability of missed-detection. This metric must be less than a given value.

3.1 Network Model

As aforementioned, we consider the case of a remote IoT-based monitoring and sensing system. We consider a set of randomly distributed sensor nodes (sensors wearable by patients). All sensor nodes are connected to a full function device carried by the patient [24]. This full function device acts as a gateway, namely *body coordinator*. It has the responsibility to forward all data received from wearable sensors to the distant medical monitoring platform. We consider a network composed of N nodes, N = {n: n = 1, . . . ,N}. These nodes act as monitoring and collect data and vital signs or symptoms (glucose level, temperature, heart rates, breathing rates, etc.) from body coordinator carried by the patient. In the case of normal connection, client or distant medical monitoring platform starts transmission by sending a SYN to the body coordinator.

On a legitimate TCP connection, the client initiates the connection by sending a SYN requesting to the distant server. Then, the server allocates some resources such as buffer for the client and replies with a SYN/ACK packet acknowledging receipt of the SYN packet. In this stage, we have a half-open connection state and the server enter in the waiting state to complete the connection setup and begin transferring data. Indeed, the number of connections the server can be maintained while it is in the half-open connection is controlled in a limited backlog queue and when this number exceeds the queue size all subsequent incoming connections will be rejected, which will create a Denial of Service (DoS) condition. We consider a single server system composed of the body coordinator in our study case. This server serves N users. We assume that the system is slotted with unit fixed slot $t \in \{0, 1, 2, \ldots, T\}$. The server receives a large number of TCP SYN messages. We define A(t) the amount of packet arriving into the server's queue at time slot t. We assume that A(t) is a stationary process and follows a Poisson distribution. The arrival rate of packets denoted as $\lambda \in \{\lambda_1, \lambda_2, \ldots, \lambda_n\}$, where $\lambda_n = E[A(t)]$. Let q(t) denote the backlog queue length of the server at time slot t, with Q(0) = 0. The dynamics of queue length of the server node in each discrete time slot is calculating using Eq. (1):

$$Q(t+1) = \max\{Q(t) - \mu(t) + \lambda(t)\} \tag{1}$$

$$Q(0) = 0,$$

given as

$$Q(t+1) = [Q(t) + A(t) - D(t)]^{+}$$

where $\gamma^{+} = \max(\gamma, 0)$. In general, its own arrival and departure processes characterize the server queue model. When departures are less than arrivals this lead to the growth of queue backlog. We denoted that the system is stable if the mean queue length of the server is finite. Q(t), μ(t) and A(t) are semantically stand for the queue backlog, the departure and arrival processes of the Server at t respectively, describing the quantity added/removed to the queue in the time slot t. A queue is at finite-time stable if:

$$\limsup_{n\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} E(q(t)) < \infty \tag{2}$$

Fig. 3 depicts the arrive-departure process. Mostly, clients in the network send their own legal number of SYN request messages. In order to detect if there is SYN attacks, we propose a Threshold of SYN requests can be send by one node without opening a session and proceed a three-way handshake process. In other word, each node must send a number of SYN request smaller than a given threshold, indicated by *Thre*. However, in the case of SYN attacks will exist malicious activity that desire to deteriorate the network performance by injecting a huge number of TCP SYN flood requests, greater

than a threshold, and therefore exhausting the server workload and resources such as memory and queue length.

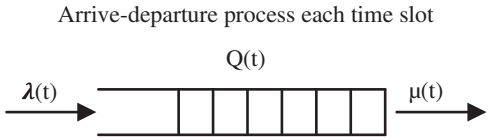

Figure 3: Arrive-departure process at each time slot

The Intrusion Detection System (IDS) is a good choice to monitor nodes behavior and detect if there is a begin of attack or not, and then issues alerts to Cybersecurity Operations Center (CsOC) for investigation. Indeed, once the TCP SYN request threshold limit is reached, the IDS issues a TCP SYN flood attack and filter out abnormal packets taking part in DoS attacks. Let *Req* the number of request resources and *Thre* is the threshold value that can made the maximum number of requests at time slot t. Properly, the attack decision rule can be illustrated as follows:

$$\begin{cases} D0: Req \leq Thre \\ D1: Req > Thre \end{cases} \tag{3}$$

where D0 indicating the absenteeism of any TCP SYN flood attack and D1 indicating the presence of a legitimate attack [12]. To address the behavior of our proposed IDS, we illustrate through the diagram on Fig. 4 our research methodology.

3.2 IDS Criteria

To further enhance the detection rate and minimize the false alarm rate of IDS, network administrator must define an objective function to reduce the probability of false alarm as much as possible. Indeed, it can happen in some cases that the number of TCP SYN, due to a bad quality of connection, trigger a false alarms and others are labeled as unknown attacks. The IDS must be able to detect abnormal TCP SYN connection and classify them as unacceptable. Thus, without loss of generality, IDS must offer a high-quality detection's precision and the trade-off between the ability to detect correctly the setup of many false positives and true positives attacks. Thereby, the metrics can be described as follows:

- True Positive (TP): when the number of actual attack is classified as an attack.
- True Negative (TN): when the number of actual normal is classified as normal.
- False Positive (FP): when the number of actual normal is classified as attack.
- False Negative (FN): when the number of actual attack is classified as normal.

Tab. 2 represents the Truth table for intrusion assertion by an IDS. Further, another main performance targets for any intrusion detection system involves precision, recall, accuracy, and specificity.

If the probability of false alarm is less than a threshold probability, then the IDS triggers that particular sequence is abnormal. We can formulate the problem as follows:

$$\min_{m_{Thre}} \quad P_{fa}$$

$$Subject\ to \quad P_{miss} \leq \beta \tag{4}$$

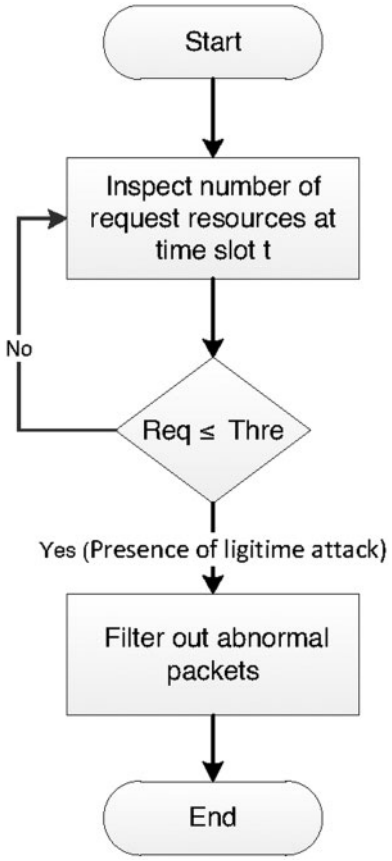

Figure 4: Research methodology

Table 2: Summary of predictive classes

		Predictive class	
		Normal	Attack
Actual class	Normal	True negative	False positive
	Attack	False negative	True positive

where P_{fa} is the probability of false alarm (false positive), i.e., the flow is normal traffic and it is not an attack affected but it is wrongly classified as an attack. P_{miss} is the probability of missed detection (False negative), i.e., the flow received by the server is an attack affected but it is wrongly classified as normal traffic. Indeed, in order to minimize the false negative errors, we need to fix an optimal trust threshold β and therefore the missed detection must be smaller than a given value β. The threshold value can be searched to minimize the total cost for a specific cost ratio of false negative errors to false positive errors.

3.3 Materials and Methods

3.3.1 The Conway–Maxwell–Poisson Distribution Model and Probability Function

The CMP distribution is a generalization of the Poisson distribution. It is a natural two-parameter that was originally developed in 1962 by Conway and Maxwell to model queues and services rates. Let Y denote a Conway–Maxwell–Poisson distributed random variable denoting the number of TCP SYN attacks during a single time slot. The probability mass function (pmf) of P(X = x) using the CMP distribution is given by:

$$P(Y = y) = \frac{\lambda^{y}}{(y!)^{\upsilon}} \frac{1}{Z(\lambda, \upsilon)} \quad y = 0,\ 1,\ 2,\ \ldots \qquad \lambda > 0 \quad \textit{and} \quad \vartheta \geq 0 \tag{5}$$

where

$$Z(\lambda, \vartheta) = \sum_{j=0}^{\infty} \frac{\lambda^{j}}{(y!)^{\vartheta}}$$

Parameter λ is the CMP "location" (intensity) and ν is the dispersion parameter, i.e., Y ∼ CMP(λ, ν). Z(λ, ν) is often called the "Z-function" and represents a normalizing constant. The CMP distribution is a generalization of some well-known discrete distributions. When $\nu = 1$ (and thus $Z(\lambda, \vartheta) = exp^{\lambda}$ an ordinary Poisson (λ) distribution results) Eq. (5) can be written as:

$$P(X = m) = \frac{\lambda^{m}}{(m!)} exp^{-\lambda} \tag{6}$$

Therefore, based on the decision rule in Eq. (5), P_{miss} is calculated as follows:

$$P_{miss} = P(X < m_{thre}) = \sum_{m=0}^{m_{Thre}-1} P(X = m) = \sum_{m=0}^{m_{Thre}-1} \frac{\lambda^{m}}{(m!)} exp^{-\lambda} \tag{7}$$

Our proposed IDS implements an algorithm to calculate the probability of missed attack in each time slot. This probability is compared with a threshold value and depending on the comparison result, an appropriate alarm or signal is handled. This missed detection probability must be smaller than β. The complete process of attack detection is described in Algorithm 1. Firstly, two variables are fixed by the system administrator, namely P_{fa} and β, which represent the probability of false alarm and the upper bound on the false alarm probability, respectively. On each iteration, we calculate the probability of missed detection and the threshold value based on equation adopted on Eq. (7).

Algorithm 1: IDS detection algorithm

Input: P_{fa}, β
Output: m_{thre}
1: procedure IDS PROCEDURE
2: $P_{fa} \leftarrow 0$
3: $m_{thre} \leftarrow 0$
4: *loop*:
5: **if** $P_{fa} < \beta$ **then**
6: $P_{fa} \leftarrow P_{fa} + P(X = m_{thre})$
7: $m_{thre} \leftarrow m_{thre} + 1$

(Continued)

Algorithm 1: Continued

8: **goto** *loop*.
9: **close**;
10: **end if**
11: **end procedure**

4 Performance Evaluation

This section describes the simulation model used on this study and evaluate the IDS performance against any TCP SYN attack. Simulations carried out using the Matlab programming environment. To simplify our analysis, we assume that we have an IoT network composed of N = 50 source nodes. Each node sends one TCP SYN request packet per time slot. Packets sent has an average length of $\lambda_s = 40$ *bytes*. All received packets are stored on the server queue (coordinator node) to be served later with an average rate of $\mu = 1950$ *bytes per time slot*. The Time simulation employed on this study is at horizon of T = 1500 time slots. We consider a network with TCP SYN attack without the admission of the Intrusion Detection System. We calculate the backlog queue for an optimal trust threshold $\beta = 0.2$ and different probability values such as Pa = {0; 0.3; 0.6; 0.9}. Fig. 5 illustrates the backlog queue under different probability values of attack. As expected, we can see that the backlog queue linearly increases as probability of attack increases.

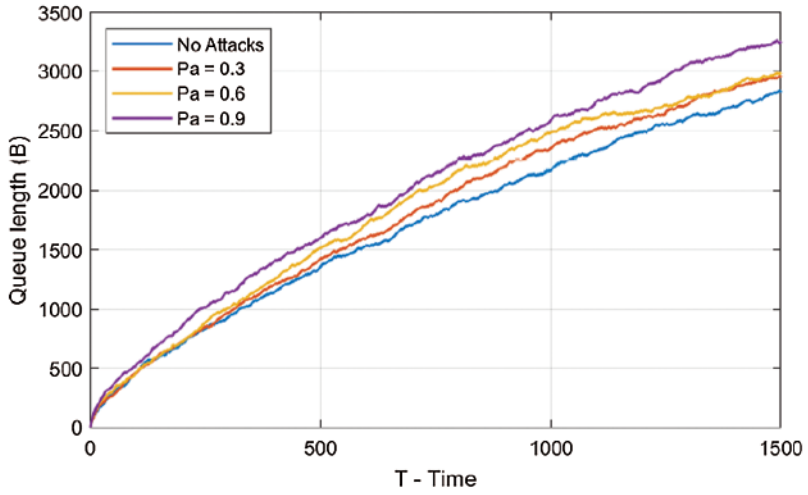

Figure 5: Attack probabilities without IDS

As well, Fig. 6 shows that the backlog queue with probability Pa = 0.9 is quite large compared to one who has Pa = 0.3. Indeed, when the probability attack increases this lead in growing queue length. If these attacks traffic condition persist for a long time, the queue will block all other traffics that can be normal traffic and therefore cause bad influence on resource performance. To evaluate our proposed scheme, we illustrate on Fig. 6 the queue length of the server in the presence of the IDS. Fig. 6 has been illustrated with a probability of attack Pa = 0.6, $\beta = 0.2$, and L = 40B. Fig. 6 shows the queue length of the server in the case where there is no attack, the case of an attack occurs without IDS deployment, and the case with the presence of the IDS with probability Pa = 0.6. As we can see, without IDS the queue length grows to a value of 2874 Bytes. However, when we apply an IDS in the

front of the server queue, we show clearly that the number of queue size decreases. This is due to the comparison of the number of requests against the threshold value. If the number of requests exceed a specific threshold, as defined by network administrator, all other request packets from such node will be handled as attack messages and should be rejected. Fig. 6 shows the effect of probability of attack with the IDS deployment on the queue length size. As expected, place IDS to cover attacks for different probabilities of attacks can minimize as possible server congestion and thus reducing network overload

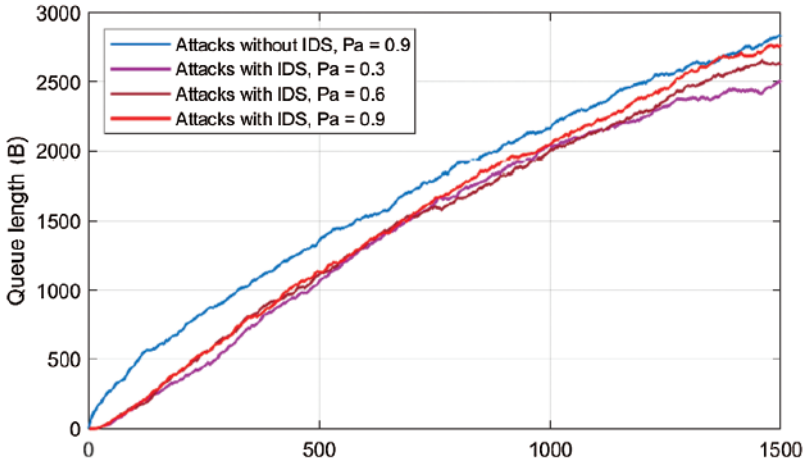

Figure 6: Attack probabilities with IDS

5 Conclusion and Future Works

In this paper, we proposed an anomaly-based IDS for medical IoT networks. Indeed, open environment of Internet of Medical Things (IoMT) can be a potential primary target for various attacks. The proposed approach permits to identify suspicious network traffic and anomalies against IoT networks based on the network parameters, which allows us checking whether the medical IoT network is under TCP SYN attacks or not. Empirical results obtained by the proposed IDS solution seems to provide reasonable solution to predict probability of attacks on medical IoT networks. The proposed IDS has been evaluated analytically and via Matlab simulations. Results obtained show valuable contribution to the IoT architecture. In our plane for future work, more number of attacks will be considered and we plan to implement the proposed architecture in a real-world IoT environment. This will be achieved by importing the IDS system to ContikiOS devices and study several other factors affecting the detection process.

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at Jouf University for funding this work through research Grant No (DSR-2021-02-0103).

Funding Statement: Funding for this study was received from the Deanship of Scientific Research (DSR) at Jouf University, Sakakah, Kingdom of Saudi Arabia under the Grant No: DSR-2021-02-0103.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Vishnu, S. J. Ramson and R. Jegan, "Internet of medical things (IOMT)-An overview," in *Proc. 5th Int. Conf. on Devices, Circuits and Systems (ICDCS)*, Karunya Institute of Technology and Sciences, Coimbatore, Tamilnadu, India, pp. 101–104, 2020.

[2] R. P. Singh, M. Javaid, A. Haleem and R. Suman, "Internet of things (iot) applications to fight against covid-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp. 521–524, 2020.

[3] E. Luz, P. Silva, R. Silva, L. Silva, J. Guimaraes *et al.*, "Towards an effective and efficient deep learning model for covid-19 patterns detection in x-ray images," *Research on Biomedical Engineering*, vol. 34, no. 4, pp. 1–14, 2021.

[4] L. Rachakonda, S. P. Mohanty and E. Kougianos, "Ilog: An intelligent device for automatic food intake monitoring and stress detection in the iomt," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 2, pp. 115–124, 2020.

[5] L. Bai, D. Yang, X. Wang, L. Tong, X. Zhu *et al.*, "Chinese experts consensus on the internet of things-aided diagnosis and treatment of coronavirus disease 2019 (covid-19)," *Clinical eHealth*, vol. 3, pp. 7–15, 2020.

[6] T. Zhang, A. H. Sodhro, Z. Luo, N. Zahid, M. W. Nawaz *et al.*, "A joint deep learning and internet of medical things driven framework for elderly patients," *IEEE Access*, vol. 8, pp. 75822–75832, 2020.

[7] A. Kamble, V. S. Malemath and D. Patil, "Security attacks and secure routing protocols in rpl-based internet of things: Survey," in *Proc. Int. Conf. on Emerging Trends & Innovation in ICT (ICEI)*, Pune, Maharashtra, India, pp. 33–39, 2017.

[8] R. Alexander, A. Brandt, J. Vasseur, J. Hui, K. Pister *et al.* "RPL: IPv6 routing protocol for Low-power and lossy networks," RFC 6550, Mar. 2012.

[9] I. Kechiche, I. Bousnina and A. Samet, "A comparative study of rpl objective functions," in *Proc. Sixth Int. Conf. on Communications and Networking (ComNet)*, Hammamet, Tunisia, pp. 1–6, 2017.

[10] A. Al-Abdi, W. Mardini, S. Aljawarneh and T. Mohammed, "Using of multiple rpl instances for enhancing the performance of iot-based systems," in *Proc. of the Second Int. Conf. on Data Science, E-Learning and Information Systems*, Dubai United Arab Emirates, pp. 1–5, 2019.

[11] E. Aljarrah, M. B. Yassein and S. Aljawarneh, "Routing protocol of low-power and lossy network: Survey and open issues," in *Int. Conf. on Engineering & MIS (ICEMIS)*, Agadir, Morocco, IEEE, pp. 1–6, 2016.

[12] A. Abdollahi and M. Fathi, "An intrusion detection system on ping of death attacks in iot networks," *Wireless Personal Communications*, vol. 65, no. 4, pp. 1–14, 2020.

[13] P. Pongle and G. Chavan, "A survey: Attacks on rpl and 6lowpan in iot," in *Proc. Int. Conf. on Pervasive Computing (ICPC)*, Pune, India, IEEE, pp. 1–6, 2015.

[14] C. Jun and C. Chi, "Design of complex event-processing ids in internet of things," in *Proc. Sixth Int. Conf. on Measuring Technology and Mechatronics Automation*, Zhangjiajie, China, IEEE, pp. 226–229, 2014.

[15] D. Oh, D. Kim and W. W. Ro, "A malicious pattern detection engine for embedded security systems in the internet of things," *Sensors Journal*, vol. 14, no. 12, pp. 24 188–24 211, 2014.

[16] C. Liu, J. Yang, R. Chen, Y. Zhang and J. Zeng, "Research on immunity-based intrusion detection technology for the internet of things," in *Proc. Seventh Int. Conf. on Natural Computation*, Shanghai, China, pp. 212–216, 2011.

[17] S. Raza, L. Wallgren and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad Hoc Networks Journal*, vol. 11, no. 8, pp. 2661–2674, 2013.

[18] A. Le, J. Loo, A. Lasebae, M. Aiash and Y. Luo, "6lowpan: A study on qos security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189–1212, 2012.

[19] A. Le, J. Loo, Y. Luo and A. Lasebae, "Specification-based ids for securing rpl from topology attacks," in *IFIP Wireless Days (WD)*, Niagara Falls, ON, Canada, IEEE, pp. 1–3, 2011.

[20] A. Abduvaliyev, S. Lee and Y. -K. Lee, "Energy efficient hybrid intrusion detection system for wireless sensor networks," in *Proc. Int. Conf. on Electronics and Information Engineering*, Kyoto, Japan, vol. 2, pp. V2–25, 2010.
[21] S. Shin, T. Kwon, G. -Y. Jo, Y. Park and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 4, pp. 744–757, 2010.
[22] P. Ioulianou, V. Vasilakis, I. Moscholios and M. Logothetis, "A signature-based intrusion detection system for the internet of things," *Information and Communication Technology Form*, Graz, Austria, 2018.
[23] D. Midi, A. Rullo, A. Mudgerikar and E. Bertino, "Kalis—A system for knowledge-driven adaptable intrusion detection for the internet of things," in *IEEE 37th Int. Conf. on Distributed Computing Systems (ICDCS)*, Atlanta, GA, USA, pp. 656–666, 2017.
[24] K. Kumar, N. Kumar and R. Shah, "Role of iot to avoid spreading of covid-19," *International Journal of Intelligent Networks*, vol. 1, pp. 32–35, 2020.