

A new algorithm to enhance security against cyber threats for internet of things application

Radwan S. Abujassar¹, Mohamed Sayed¹, Husam Yaseen²

¹Faculty of Computer Studies, Arab Open University, Al-Ardiya, Kuwait

²School of Business and Finance, American University of Madaba, Amman, Jordan

Article Info

Article history:

Received Sep 8, 2022

Revised Dec 11, 2022

Accepted Dec 17, 2022

Keywords:

Buffer optimization

Internet of things

Quality of service

Rout attack with detection algorithm

User data protocol

ABSTRACT

One major problem is detecting the unsuitability of traffic caused by a distributed denial of services (DDoS) attack produced by third party nodes, such as smart phones and other handheld Wi-Fi devices. During the transmission between the devices, there are rising in the number of cyber attacks on systems by using negligible packets, which lead to suspension of the services between source and destination, and can find the vulnerabilities on the network. These vulnerable issues have led to a reduction in the reliability of networks and a reduction in consumer confidence. In this paper, we will introduce a new algorithm called rout attack with detection algorithm (RAWD) to reduce the affect of any attack by checking the packet injection, and to avoid number of cyber attacks being received by the destination and transferred through a determined path or alternative path based on the problem. The proposed algorithm will forward the real time traffic to the required destination from a new alternative backup path which is computed by it before the attacked occurred. The results have showed an improvement when the attack occurred and the alternative path has used to make sure the continuity of receiving the data to the main destination without any affection.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Radwan S. Abujassar

Faculty of Computer Studies, Arab Open University

Al-Ardiya, Kuwait

Email: r.abujassar@aou.edu.kw

1. INTRODUCTION

Currently, internet of things (IoT) is starting to spread widely across the world, which is increasing the interconnection of physical moving data packets or “things” through the internet and from source to destination. Each end user is uniquely identified by using radio frequency identifier (RFID) tags. However, during transmission of the data between source and destination, security should be applied to provide more confidentiality and reliable networks. Now cyber security plays an essential role in all communication, as it is critical infrastructure for all resources. Therefore, protecting the current industrial system with robust cyber security is considered one of the most important priorities for all organizations, such as internet service provider (ISP) [1]. Various end IoT smart devices for sensing and acting, intermediary nodes with wired or wireless connectivity for data relaying, and application servers in the cloud for data monitoring and analysis make up the conventional internet of things architecture. IoT devices frequently connect with one another without much input from end users, creating a broad and self-sufficient network. Adversaries in the cybersphere can endanger many people’s safety and privacy in our daily lives and during communications as the line between computers and

users becomes blurry. Clearly, the increased usefulness of wireless communication devices has made the IoT appealing to malicious software and digital viruses.

In order for researchers to easily create their own use cases, model IoT devices into them, and then generate and analyze the traffic of the use case in order to develop better security solutions for IoT, the main goal of this work is to propose a new algorithm that can reroute the traffic of an IoT generator device from another node that has been affected by the attacker. The introduced and proposed algorithm can also be used in huge networks with big number of nodes for testing different IoT-based network utilities like switches and routers, by generating a large amount of IoT device traffic. Moreover, it can also be used for the designing and testing of IoT security providing entities like intrusion detection system (IDS) and intrusion prevention system (IPS). The key contributions of this work are as:

- We proposed an open-source framework which consists of an IoT traffic generator tool which is capable of generating IoT normal and attack traffic over a real-time network using a single physical machine.
- We devised IoT device modelling by introducing the concept of time profile and data profile in order to better emulate the IoT devices.
- Furthermore, we implemented a real-time traffic between source and destination nodes using the proposed IoT traffic generation framework and demonstrated how the generated traffic can be rerouted in case of the cyber attack.

In this paper, we will explain the models for cyber security in IoT networks. Nowadays, IoT networks represent a promising new technology which connects all technologies together, such as smart phones, TV, CC cameras, robotics, and so on. The IoT is starting to be implemented widely and has grown very rapidly, but it is still facing problems with cyber security and loopholes in its networks. Therefore, people may be reluctant to use the IoT technology in the future. One well-known problem is known as distributed denial of service (DDoS). Such an attack can affect many IoT systems and the communications between end users using the network [2].

The structure of the paper is organized as follows: section 2 presents a snapshot of cyber security in the IoT and highlights the recent applications used for all new devices. In section 3, we discuss related works on incentive programs, as well as earlier research on the internet of things and how it pertains to network performance. In section 4 we also describe our proposed technique and compare our results with other existing protocols. The performance of the suggested strategy is next assessed once the findings are given in section 5. Finally, a conclusion is given and future work is discussed in section 6.

2. CYBER SECURITY IN IOT NETWORKS

Currently, the internet of things is an emerging and promising technology, which connects all network devices around the world through the internet. IoT technology can provide improvements that assist our personal work by making our lives more professional. The IoT also comprises of a network of intelligent items connecting to one another globally over the internet without any interference from end users. It is yet vulnerable to cyber-attacks just like any other network. Any network can effectively identify cyberattacks using an IDS [3]. Most of the latest IDSs are based on machine learning algorithms for the training and detecting of cyber-attacks on the network. In addition, various smart algorithms have been proposed by many authors for detecting the IDS and the proposed algorithm will help to detect attacks and also provide a very rapid solution in case any nodes in the network are affected. As shown in Figure 1 a vast number of connected devices form a network known as fog computing, which is an improved version of centralized cloud computing. Distributed fog nodes are located closer to the IoT network objects in fog computing, which resolves the scalability bottlenecks, high bandwidth consumption quality of service (QoS) degradation, and high latency limitations in cloud computing [4].

A fog network is ideal for the practical implementation and success of the IoT networks. In this paper, a fog network is one of the most important factors behind the success of our proposed algorithm and the solution to the attack problem in a very fast mechanism. The proposed algorithm will work in the global cloud network and can also work in cluster networks having many nodes connected to each other. The IoT network contains many connections between different types of smart object. Hence, an attack can occur because of a big loophole in cyber security. Typically, cyber security in the IoT concentrates on two main approaches. Firstly, analysis leads to the discovery of policies for security. Secondly, artificial intelligence and machine learning are employed. Both can lead to the detection of any anomalous patterns. The IoT presents a complex system

and security analysis can only be conducted in an automated and timely manner [5]. The proposed technique is adopted to improve cyber security, including training for each node on how to detect threading in the network or any suspicious behaviors. The main aim is not to stop the attaching, but it finds other nodes in the network which are not affected, so that the performance of delivering any data packets can be retrained and improve the QoS.

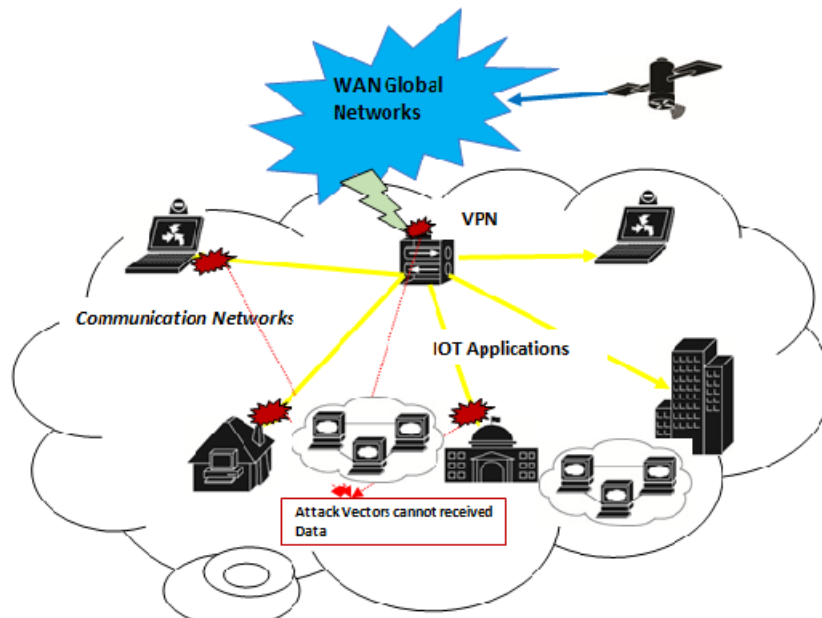


Figure 1. IoT attack

2.1. IoT main features

In the IoT environment, the resources of any IoT devices – such as any smart objects – are typically limited in terms of computation, storage, memory, and power. Therefore, any new technologies that can meet the needs of resource-constrained devices in the IoT are considered very important regarding the number of users, which increases every day. A considerable effort has gone into researching cyber threat intelligence in the past few years and a number of sophisticated techniques have been developed that can perform cyber security detection. In the IoT environment, many solutions have been found that enable cyber security needs to be more efficiently handled [6]. Broadly speaking, computational intelligence algorithms are used in IoT security solutions, such as malware detection, cyber threat identification, suspicious behavior monitoring, intrusion detection, and stopping cyber-attackers as it showed in Figure 2.

According to a large portion of this research, the distinctive features of the IoT make it easier to exploit devices and spread IoT malware. The primary resources, diverse links, and fragile usability are some of these elements. Compared to the intermediate nodes located in the networks, which connect them with the infrastructure through wired connectivity, the IoT devices which are designed to perform sensing and actuation operations easily have limited computation and communication capabilities. For this reason, the algorithms and mechanisms applied on IoT devices are helping to find an urgent solution in the case of attacks occurring. As a result, the attacker can expend far fewer resources to break into IoT devices, rendering them the targets of malicious users [7], [8].

In order to support the many different kinds of IoT applications, devices are usually equipped with heterogeneous communication and computation capabilities for the purpose of seamless operations. The heterogeneity and potentially vast amount of IoT devices facilitate the fabrication of an identity and the hiding of malware. Moreover, as shown in Figure 3, compromised IoT all devices and might disseminate attacks via heterogeneous communication links [9]. Hence, IoT devices might disseminate IDS or malware via heterogeneous communication links, as explained.

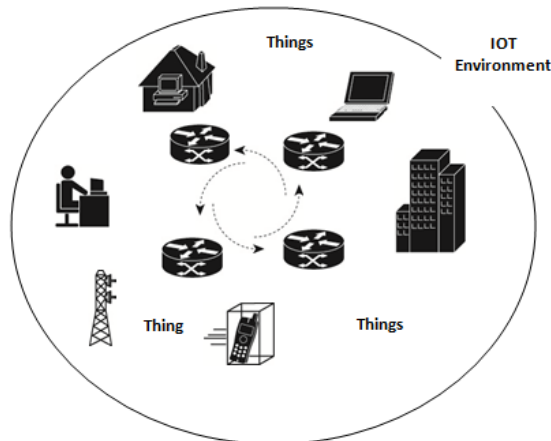


Figure 2. IoT Environment

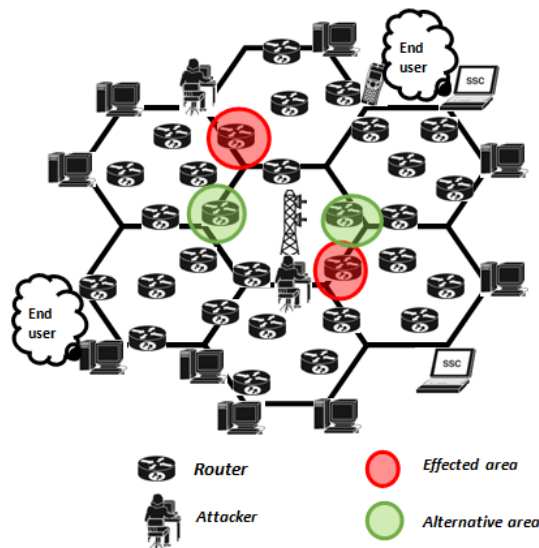


Figure 3. Illustration of cyber attack under patch scheme

Infrastructure links: IoT malware can propagate using infrastructure-based communication technologies, such as global system for mobile communications (GSM)/general packet radio service (GPRS)/universal mobile telecommunication system (UMTS)/long term evolution (LTE) and wireless local area network (WLAN), via intermediate nodes or any access points. In particular, IoT malware inherits the threats caused by any computer or device malware. Similar to computer malware, most IoT malware families today scan the IP address for vulnerable victims and then spread via the Internet between huge numbers of nodes [10]. End-to-end links: IoT malware can use near field communication (NFC) and proximity-based wireless connection technologies to infect nearby devices. This causes IoT malware to be stored and to start spreading by utilizing ubiquity and mobility [11]. The last point here is called usability, which is described as follows: security is only as strong as its weakest link. The person who develops, runs, and employs the system is frequently referred to as the system's weakest link. Additionally, users may decide to disregard or even circumvent a security feature if it stops them from doing the intended action (for example, due to poor user interface design, slow performance, or unclear instructions). IoT devices frequently lack convenient input and output interfaces, making it possible for non-technical users to get around the original security mechanisms. This raises the probability and danger of human mistake and makes malware more likely to propagate [12], [13].

Recently, the ratio of smart phones, tablets, and smart watches to people was almost one person to two devices. Today, technical innovation is increasing, and the market for smartphones is always expanding. The IoT is a hot issue right now, and smart cities are being built using it extensively. This technology is expected to transform many aspects of our daily lives given the booming nature of research in this subject, both in academia and industry. The three-layered structure of the IoT model is determined by its functionalities and consists of a perception layer, a network layer, and an application layer [14]. As follows, this is further explained:

- Perception layer: This is considering the main sense of the IoT. It aims at recognizing any objects with gathering all information. This layer contains RFID tags with its labels' and code readers.
- Network layer: This layer represents the entire and main work of the IoT. It processes and forwards information which is received from the main perception layer to upper layer such as the application layer [14].
- Application layer: To actualize the IoT's advanced capabilities, this layer fuses the socio-business requirements for the technology. The fusion of industrial demands and machine intelligence with IoT and industrial technologies is represented by this layer. The IoT has a two-system structure, which has been the subject of extensive research. To fully comprehend the IoT and its two-system structure, it is necessary to analyze the internet and communications networks [15].

3. RELATED WORKS

The internet of things is a term that Kevin Ashton initially coined in 1998 to describe the future of the Internet and pervasive computing [16]. The ability to connect and reach people around the world in the future is made possible by this technological revolution. Whether a thing is a connecting device or not, "things" on the IoT refer to any object on the earth. Anything can be a part of the internet, from a smart device to a tree's leaf node or a bottle of beverage. Over the platform, the objects become communication nodes. IoT sensors and smart communication systems generate data that must be examined in real time using deep learning techniques, or they can be used to train deep learning for smart models. Given the low-latency requirements of edge devices and the additional benefits. It provides in terms of privacy, bandwidth efficiency, and scalability, edge computing is a potential solution to support good and better computation [4].

This paper aims to provide a comprehensive review of the current state of edge computing with the use of smart IoT end devices [16]. This paper also explains an overview of applications where deep learning technology has used at the network edge, explains the techniques for training deep learning models across numerous edge devices and examines various methodology for swiftly conducting deep learning inference across a combination of end devices, edge servers, and the cloud [6]. IoT applications using smart devices have rapidly increased in number and started to be widely used by a diverse range of end users. This is because of the scale of development of smart devices [17]. IoT devices are employed in remote health monitoring and emergency notification systems. Why do we mention healthcare? Nowadays, as during coronavirus disease (COVID-19), people are not able to travel and consult their doctor. Hence, they have started to use the internet to keep in contact for any emergency issues.

As a result, people have begun to employ monitoring devices, which range from basic ones like blood pressure and heart rate monitors to more sophisticated ones that can keep an eye on specialized implants like pacemakers, FitBit gadgets, risk bands, and cutting-edge hearing aids. Real-time data transfer on the patient's vital signs is made possible via the IoT using this network. An emergency alert is triggered whenever one of these crucial factors changes significantly.

The early IoT-based healthcare research initiatives were centered on this phenomena. Integrity ensures that an opponent cannot disconnect and corrupt the video data while it is being transmitted. The IoT is based on information sharing between many types of devices, including interior gateway protocol (IGP) or mobile ad-hoc network (MANET) networks. When data are received from the correct sender, it is crucial to assure data accuracy by using a virtual path with a high-priority label and to check to see if the data have been altered during transmission.

Yuan *et al.* [18] has done an experiment to demonstrate that the reliability and performance of the clouds under investigation fall short of expectations. As a result, despite showing a terrible adaptability based on temporary and immediate resources, the author has noted in his research that cloud computing is insufficient and inefficient for complete scientific processing. The present study has therefore studied the improvement of current clouds related to computer networks and the establishment of a unique research avenue. By including

more cloud services, such as a database, private cloud, queuing service, and storage, future work can expand on this. The network layer of the IoT offers functionality in terms of real data-time traffic routing and transmissions to many different IoT devices over the IGP or MANET networks. Internet gateways, switching and routing devices, among others, operate with the application of recent updated technologies. The network gateways serve as mediators between different IoT nodes by aggregating, filtering and transmitting data to and from different sensors [19]. This paper will also describe the various difficulties, such as cyberattacks, which have an impact on technology and network performance. The following ideas will be retained by the reader as a result of this essay: Understanding the network use cases for deep learning at the network edge, typical methods for accelerating deep learning inference, distributed training on edge devices, and current trends and possibilities [20].

According to IBM, the huge number of devices which are connected to the internet will be increased more and more, and will exceed the number of human beings. The focus of current research has tended to be on the control of real-time traffic data by locating the finest historical nodes that can offer the most reliable path based on their history. Our algorithm will take care of this. Buriol *et al.* [21] talked about anomalous traffic scenarios, the spread of information, and the identification of delay or failure that shows a dangerous traffic pattern, as in the case of IoT activities involving real-time data. In this research, we present an algorithm to identify real-time high-emergency data that must be sent from destination to receiver nodes, to clear all other unneeded traffic to create room for these data, and to do so utilizing nodes with a high-priority label. We provide a low-cost speech recognition method and implement inquiry packet detection to identify the existence of labeled data traffic using our algorithm. Attacks might cause delays and failures as well, thus the suggested approach will help to utilize another node did not not affected by any threatening .

Increased attacks lead to so many issues, which affect our daily life of an individual or disturb the services for all users connected on the network. To avoid much delay time being wasted on the main path, controlling traffic using clever algorithms that can choose guaranteed paths is crucial [22]. The number of road accidents has also increased due to traffic. The suggested approach employs cloud computing to report to the next station when it detects high-emergency real-time data flow. Data transport between the server and client is made possible by two different processes. Numerous projects have been undertaken in the area of traffic engineering. The transmission control protocol/internet protocol (TCP/IP) protocol is used in the proposed system to transport data [13].

The main concern that comes up with IoT-cloud integration is the real fact that from base infrastructural to service domains, cloud models are beset by many different security challenges, such as application services attack, data integrity attack, privacy, trusts, identity, and standardization. All these challenges are most likely to occur when two or more platforms are merged, thus raising some deep research questions which need to be explored. Accordingly, some research studies by the international data corporation (IDC) claim that, while business company leaders notice the potential of the IoT, they are deeply skeptical about the system's inherent security challenges on the main network. Moreover, the study asserts that most business leaders admit having a limited understanding of the security threats IoT brings during transmission. In addition, a related study from Klynveld Peat Marwick Goerdeler (KPMG) stated that the security breaches in consumer data, as well as up to date attacks on cyber infrastructure systems worldwide, make IoT users lose trust and avoid solution providers who have not taken the appropriate measures to protect their systems [23]. The major challenge of cyber security on IoT platforms is a global concern which requires a holistic assessment on the part of research and different industrial communities [24], [25].

4. PROBLEM DEFINITION

Currently, the data in the network which needs to be transferred from source to final destination faces many problems because of attackers, such as delays, congestion, the loss of data packets preventing any data from being received or even raising jitters. The internet has grown with the increase in the number of users and many generations have been raised, such as 5G or fiber optic. Both are results of the increase in network speed when exchanging data. Hence, IoT is considered one of the most important topics and has started to be used in some parts in the world. The problem here is two parts. Firstly, we need to concerns on the instructions (data packets) of how to be received between sender and end nodes when using a smart machine which will execute these instructions without any delay, in an accurate way, once the threat has occurred. Secondly, the proposed algorithm will deal with these notifications coming from a smart machine by sending a notification

to the sender node to start using a new path, which will help to accomplish the mission successfully.

Hence, we mainly consider the data which is forwarded and received as real time traffic in live streaming connections, and these connections should be reliable. No problems can occur while the connection is open between them (source and destination). There are some examples - such as emergency situations, or performing surgery via live video streaming, when this problem could have severe consequences. As we mentioned, traffic paths might not work effectively due to congestion in the network. In this paper we proposed an intelligent algorithm to work with the routing protocol and to focus on the node buffers, and also on the loss of important packets during connections. The main object is to reduce and avoid delay if the buffer for each node on the selected path has any of these packets, by making our route attack with detection algorithm (RAWD) algorithms reroute the main traffic, and distinguish between the negligible packets and high priority ones, in order to begin forwarding the main data to the required destination. All of the devices may also be intelligent to accomplish the goals. By providing more effective solutions, our algorithm will assist the current routing protocol and even hardware devices in establishing stronger links that will result in the successful completion of the mission between the source and the destination. However, our algorithm's drawback is that it must determine which network nodes have been impacted by the attacker. The main problem is if the attacker or intrusion affects the nodes on the main path and also the one that can be used for backup. As a result, the algorithm will take more time to find another path. Therefore, we have found a solution to this problem by using different ways of rerouting traffic, such as from adjacent nodes or from the source itself.

As a result, in the suggested system, traffic control is carried out automatically with the aid of the IoT, and the required steps are made to address these issues. In order to compute a new way from source to destination by choosing a different path that has not yet been affected, we developed a clever method RAWD that can compute an alternate path from the node that is currently under assault on the main path first. A monitoring packet is also present to keep an eye out for any emergency packets that may arrive inside the buffer but have not yet been delivered. The program will attempt to warn the node that must be dispatched immediately in order to finish the task.

4.1. The new technique and algorithm

In order to ensure that there is always at least one available path between the source and the destination in the network design, we have suggested a novel path-protecting technique that makes use of a mesh topology and our heuristic algorithm. We are concerned with one approach for network survival: a restoration technique that might be more effective in terms of resource usage. The ability to recover from node failure is a key benefit of mesh topology-based path protection over links. It can discover a variety of additional routes between every node in the network. Additionally, our suggested method ensures that the traffic between the source and destination will not be lost and that the new way will not be impacted [26], [27].

We employed the suggested technique to examine the performance of the best path in the network design on networks with a large number of nodes, such as mesh topology. Any topology containing a huge number of nodes is considered to be more attractive for hacking and at the same time useful for finding an optimal solution for large or medium networks, with a lot of traffic passing from it. For a network with a small number of nodes, there are various challenges, including lengthy processing times and a need for numerous variables and restrictions for path protection [28]. As a result, these factors serve as powerful inducements to create speedier path protection with reference to the few and few edges between nodes. The goal is to determine the overall spare capacity in the event of a path failure. The main important role is to select the topology that meets all required rules to find many alternative paths such as p-cycle topologies [24]. We have two kinds of path as follows:

- Full and main path relationship checked, which determines that the path span is disjointed for a given primary one, or it might be used by the primary one, with guarantees that there is another branch from the same source can have different port connected with other path but it might be longer than the main one deliver the packets to the destination without affecting the QoS network once the attack has occurred. If the path does not contain a common path on the mesh topology then our algorithm cannot be applied in this case. Other than end nodes, the path could have one or more common nodes.
- Path mutual relations are examined to see whether the paths are mutually and totally disconnected and to see if they lack common spans yet have nodes other than end nodes.

In Figure 4, we showed a RAWD algorithm how it works for detecting and determining the required path to open the new path between source and destination before any injection. The RAWD algorithm comes

to check where the path that has low congestion. It may also be the second-shortest way, but this is not necessary because, as our results demonstrated, once we reserve the area with the least amount of congestion and maintain it open for emergency vehicles, the wait will not be much increased. The RAWD algorithm will use link-state database (LSDB) for each node to make sure this node is capable of being used during the normal transmission, with any disturbance or noise. This is based on the old history for each node in the topology and its' fault tolerance capacity. As we show in the flowchart, the algorithm will start to work after the main routing protocol has built the main routing table for the networks.

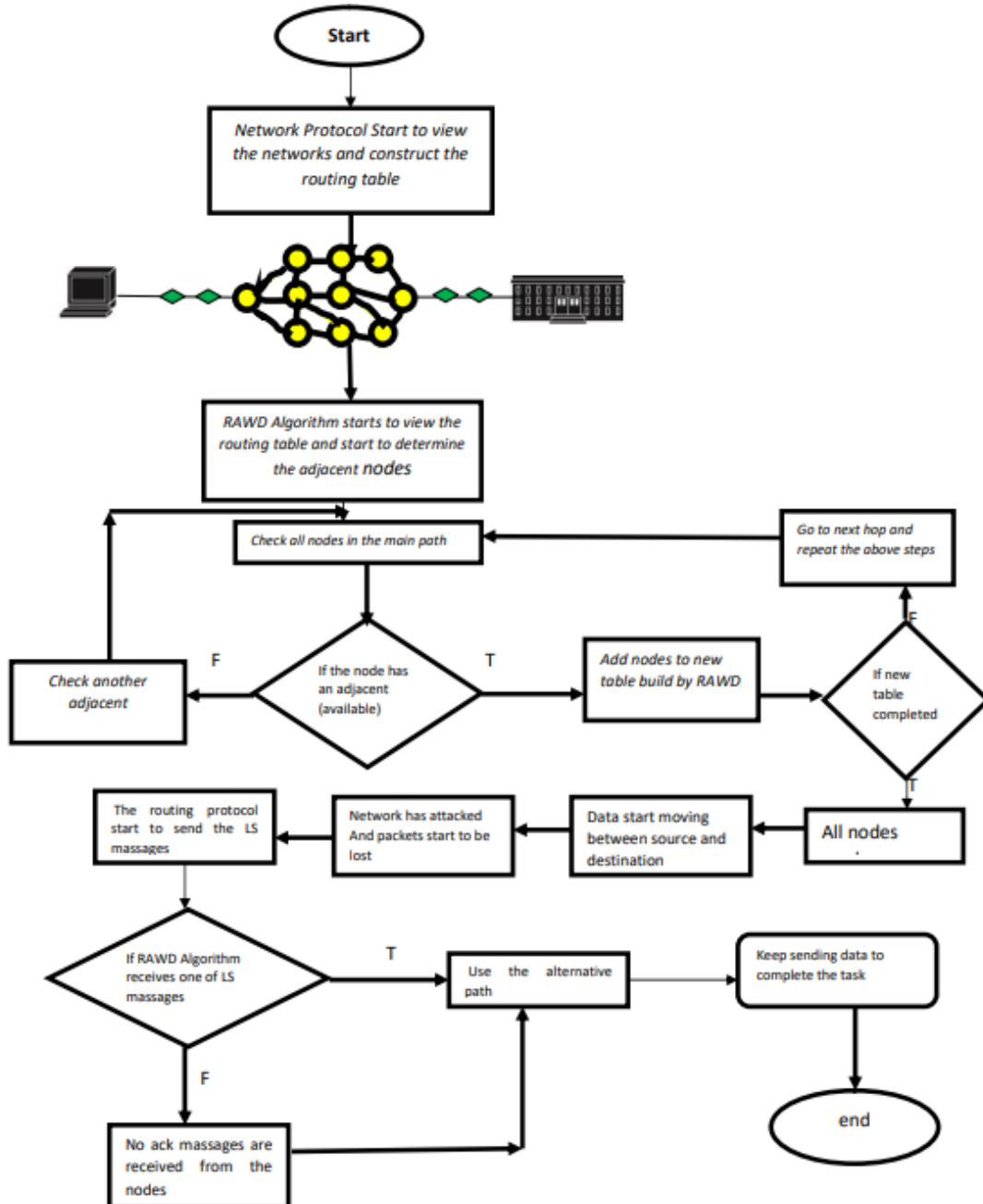


Figure 4. Flowchart of the proposed algorithm

The algorithm 1 shows how the nodes are selected after the routing table is constructed by the existing routing protocol, as we can apply the proposed algorithm for pre-active or pro-active protocol. Hereafter,

the algorithm will be working on the network before any attack, but at the same time the algorithm keeps monitoring the nodes or links if they go down in order to provide a fast solution in case of being affected by the attacker once the connection is lost. The RAWD algorithm will be able to start figuring out the path between the source and its destination thanks to the IoT smart approach, which is based on the information gathering and registered record. This will allow the algorithm to start transmitting and receiving data.

Algorithm 1 PSO

```

1: SelectMainPath( $T_r, s, d, edges\_to\_avoid$ )
2:  $T_r$ : Routing table constructed by existing RP
3:  $V$ : The vertices for each node  $G(V, E)$ 
4:  $s$ : Negligible packets
5: RAWD: The RAWD view RT and then start to maintain the backup one
6: MainData: exchanging Packets
7:  $d$ : The final destination
8:  $p_a(s, NextHop) \leftarrow \emptyset$  packets start moving from S to D
9: if  $s \neq d$ 
10:    $q_{sub} \leftarrow \emptyset$  Node Buffer's
11:   while  $Q \neq \emptyset$  and  $pa(s, NextHop \text{ to } dest) = \emptyset$  do
12:      $(q_{sub}, x) \leftarrow Front(Q)$ 
13:     for all  $dk \in \Gamma(x)$   $k$ : is the intermediate node which consider next hop
14:        $e \leftarrow (x, k)$  full path
15:        $p_a(s, d) \leftarrow q_{sub} \cup e \cup P_r(T_r, k, d)$   $k$  all intermediate nodes  $n$ 
16:       Enqueue( $Q, (q_{sub} \cup e, k)$ )
17:     end for
18:     Dequeue( $Q$ )
19:
20:   end while
21:    $Q \leftarrow \emptyset$ 
22:
23: end if
24: return  $p_a(s, d)$ 

```

The main backup path will only be available for any emergency issue which has been raised from any nodes on the main path. However, in case the nodes in the main path receive other packets, the RAWD will reroute any other packets via its other adjacent nodes has been selected by the RAWD algorithm to deliver data packets to the final destination. The smart algorithm needs to work without having any effect on other traffic. Each node can store large emergency packets in its buffer if they are received, preventing packet loss and maintaining a high level of service. Considering the enormous availability in the path, this will not cause the delay to grow. Since the routing protocol constructs the routing table and then configures our algorithm in accordance with the succeeding steps inside the routing protocol, it may be utilized with any routing protocol, as we already said. This presumes the deployment of a proactive routing mechanism. In contrast, a pre-active one eliminates the requirement to scan the full topology because the algorithm can only select the fastest way without knowledge of the network's other nodes. As illustrated in Figure 3, will make the assumption in our protocol that every node on the principal path is connected to an adjacent node that has met all of our protocol requirements.

- The RAWD algorithm chooses all nodes on the path, all of which should be recorded and have a very solid history, to be part of the booked path between the source and the desired destination. The algorithm will make a decision based on the data taken from the LSDB to create the routing table.
- To gain a complete picture of the network, the RAWD algorithm will import the routing table, which is produced from the routing protocol. From there, it will begin to choose nodes one by one until we reach our target.
- In this technique, all nodes on the main path should has at least an adjacent node, and then by using RWAD algorithm this adjacent node will be ready to receive other data traffic from the selected node if it receives packets by mistake or is broadcasting one.
- To prevent a network loop, the nearby node needs to be aware that any packets it receives from the chosen node on the path should pass through another node and not be sent back. This can be done by sending inquiry packets to all nearby nodes, alerting them that the packets have come from it and will be sent to you directly. Do not transmit the packets back to me until I send information packets indicating that I am

available and the session is over. First, this mechanism scans and verifies every path between nodes in the main routing table; second, it creates a path from the main routing table (if possible); or, if we use a pre-active protocol, such as ad hoc on-demand distance vector (AODV), we can use the same path.

Algorithm 1 using a buffer as an example, the algorithm demonstrates how it functions in general. We will locate the chosen nodes from the complete topology between sender and destination based on the link status database. While the routing protocol will compute the main routing table with the optimal and shortest path between any source and destination. Once its completed, all emergency packets will begin to be transmitted hop by hop as soon as the data will start to be sent.

5. SIMULATION ENVIRONMENT

This section presents a detailed explanation of sending secure data between source and destination. We simulate in network simulation (NS2) a 30-minutes on-line live packets streaming as user datagram protocol (UDP) packets and also, with this kind of traffic, if we lose any drop packets we cannot get them again, such as TCP protocol. In addition, the UDP protocol is a good example of video live streaming packet transmission. The QoS is optimized in source point computing during healthcare, or any other video transmission at a remote location. Better visualization with big sensing is analyzed during remote sensing to portray a clear picture and also provide a highway for receiving data in less time of the incident of attack throughout many experiments, with the multi-hop communication scenario. A good example would be conducting surgery abroad using IoT smart robotics. This kind of operation needs to be a very high priority, and any delay or loss of connection would be a huge disaster. The backup path is considered one of the most important priorities nowadays. The backup path not only prevents disastrous problems; it also increases the performance and efficiency of the network. This will increase the reliability for all end users and companies. Here, we make the assumption that the media stream has substantial variability, such as when an emergency patient is being dissected during surgery, which results in higher delays and higher peak variable frame rates. In Table 1, we describe the configuration parameters. The experimental results in Table 1 show a study of RAWD's performance when re-routing regular packets based on different buffer sizes with the start-up delays of 0 to 2 frames. It was found that decreasing idle time reduces the rate variability of the media sequence. The simulation is running for expecting a 99% confidence level in the outcome. The parameters configuration are presented in Table 1. As mentioned above, we contrast RAWD with other prior research. In order to demonstrate that our new technique, RAWD, will not impact networks if other packets are forwarded to different destinations concurrently, an experiment is showing that takes into account the client buffer size. By lowering the packet loss ratio, which displays a smooth packets mean ratio, less delay, and less jitter, we are able to establish a trade-off between packet size and buffer size. We simulated various mesh topology scenarios in NS2 to assess the efficacy of the RAWD algorithm in a smart city IoT setting.

The number of nodes varied depending on the scenario. We also gave each experiment's potential network traffic capacity some thought. The topology that we have used is from 50 raised up to 200 nodes; the source node was at the beginning of the network, while the destination node alternately generated normal and urgent data packets over the course of a few seconds. NS2 was performed to determine how effectively the proposed long VPN path will work in receiving high-priority traffic for medical operations or any other important high-emergency traffic needing the on-demand protocol between nodes in networks. The data transmission in the networks was well supported by the information acquired by the NS2 simulation. An average was calculated after 30 iterations of the simulation. The bit rate was set to 2 Mb/s, and the packet size was 100B. During the simulation, a traffic rate of 200 kb/s was produced from the source node to the destination.

Table 1. Experimental parameters for medical instruction transmission

Parameter	Value	Value	Parameter
Total video frames (F)	1440	Video frame total time (T1)	30 min
Video frame rate (r(t))	3 sec	Video frame length (L_f)	100 B
Video frame arrival time (t)	5sec	Inter-arrival time δ	1 msec
Buffer size (Buffer)	64 KB, 512 KB, 2 MB, 4 MB	Initial buffer size	0

Before examining the performance issues for the network topologies with relation to computing a next hop over various networks, it is critical to identify the network factors that can affect the QoS of the streamed

video traffic. The main focus of this study is on three elements in order to more precisely predict how video traffic methods will perform:

- Packet loss ratio: This is the packet lost during the transmission
- Average delay time in the buffer: it is the time between sending and receiving data packets include the time that all packets stayed in the buffer.

However, by applying our technique to prepare an adjacent node to be the next hop if the necessary conditions are present, we have added an extension to the routing protocol. As we previously explained, we add enquiry packets with negligible sizes to find the next hop as an alternative to urgent packets and gather all the required information about the full topology. However, by applying our technique to prepare an adjacent node to be the next hop if the necessary conditions are present, we have added an extension to the routing protocol. As we previously explained, by adding an inquiry of urgent packets. this tiny inquiry packets are going to discover the next hop and collect all the necessary data about the entire topology.

5.1. Experimental results

We have particularly seen how node density affects the latency of real-time traffic transmission. By steadily adding nodes, we were able to simulate the reference scenarios, and the simulation was ran 20 times for each test. The confidence intervals that were gathered were consistently less than 5% of the predicted average. In Figure 5, the streaming test was built between source and destination, so the data traffics are starting to move via the main path. The initial test is done when the many unknown packets start to appear in the network. This issue will start to affect the performance of the live image or video streaming. In this case, many events can occur, such as failure in the path, or the node cannot tolerate the huge number of negligible packets that will affect the nodes on the main path.

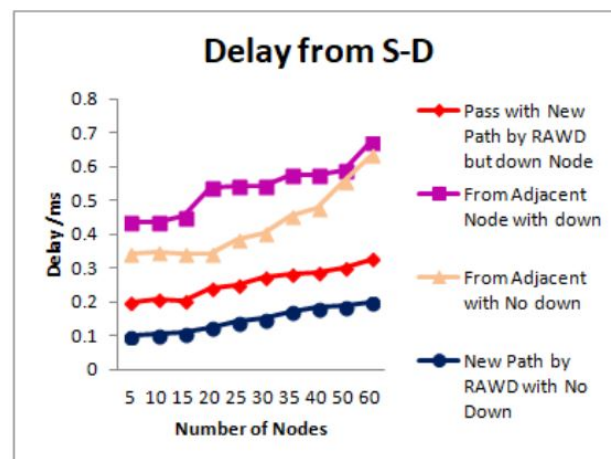


Figure 5. Link utilization for the all networks

As shown in Figure 5, the utilization has been increased on the main path, but the proposed algorithm can use another path with new nodes in the same networks to reroute the traffic to the required destination. It is a smart way that RAWD can detect the attack by checking the unknown packets. However, the algorithm showed that the new backup path can be used without any congestion.

Figure 6 confirmed the result of the utilization by showing that the load is going down for the new path. The results compared well with different types of network effect, such as node failure, adjacent failure and link down. We have also showed when the routing protocol handles the problem by recomputing and creating a new routing table to find a new path between source and destination. We have found the problem can be solved, but it will take a lot of time. This is because the existing routing protocol should compute the routing from the beginning.

In Figure 7 we compared the results produced by the RAWD algorithm and all the other cases mentioned, such as the main routing protocol without any enhancements. As we can see, the delay has been reduced by our proposed algorithm, as it has used the path which is not under attack. The other results show different

effects but we can see that in both situations the rerouting traffic from the adjacent is getting high. This is because the main path is still under attack, so if any other traffic needs to be passed via it, then the congestion will be increased and the load will be increased, as we can see in Figure 6.

We can also see that the RAWD algorithm has created a new path to improve the way for high priority traffic between source and destination. In terms of receiving real-time data, the proposed algorithm has showed improvements by reducing delay and loss of packets in live streaming transmission. In addition, the data packets showed continuity improvements when passing between the nodes among a network. According to the RAWD algorithm, a secure path was booked between the source and destination. This path has been selected as a second best path which has selected by our proposed algorithm. The path consider secure as it s coming from the adjacent node which is effected by the attacker. Based on the routing table that is produced by the network's primary routing protocol, the algorithm chose this introduce secure path. However, in Figure 7, we made sure that the nodes are only passed to emergency packets and that the long path is reserved until the session duration is up, the delay time has also decreased.

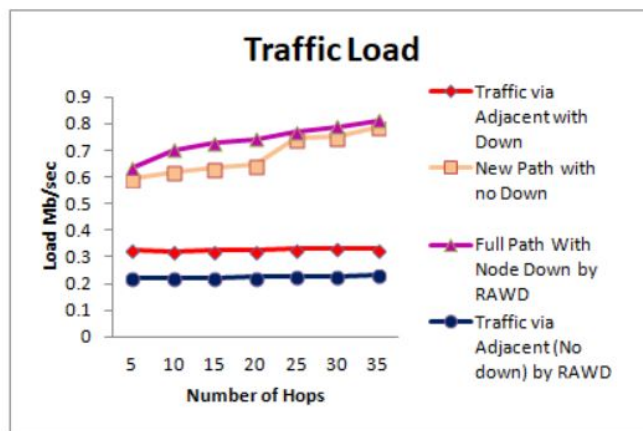


Figure 6. Load in the network

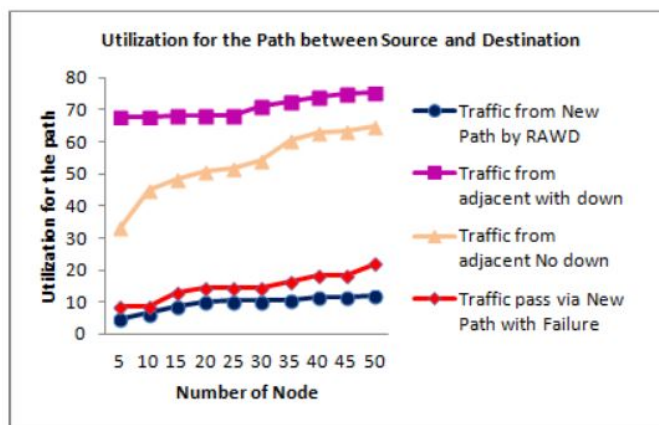


Figure 7. Packet delay from S-D

The Figures 8 and 9 illustrate various scenarios, such as the unexpected rerouting of regular packets that a node selected for booking may experience. In this situation, the algorithm can reroute the traffic to the nearby node; although though the delay time would lengthen, it will still be better than in all other situations. The total number of packets received across all experiments determines the throughput.

Additionally, the loss of packets will be decreased because of the delay will be reduced and the path between the source and destination will be set aside for the priority packets, as shown in Figure 8 and the

throughput will be increased. We can prove our results by looking at Figure 5. The results here show how the average path utilization has been affected by the main data and other packets are coming from an unknown source. However, their range is below the threshold values of latency and jitters for receiving the data. On the other hand, the mean packet loss value increased even with an increase in the node buffer size. However, The testing results make it clear that any parameter from node buffer size and reroute that varies out of proportion to each other would have an effect on the proposed RAWD's performance.

After doing an experimental research, it was discovered that our suggested technique significantly improves when the primary path is subjected to a DoS assault. In Figure 9, it is observed that the negligible packet, or in other words the attacking one, has formed a heavy load on the network. We have monitored the network when any attack occurred and we found out that these packets are causing harm as we can see in the Figure 9. In the meantime, so the being affected can lead to loss of the connection, and waiting for a solution from the main routing protocol or any other firewalls.

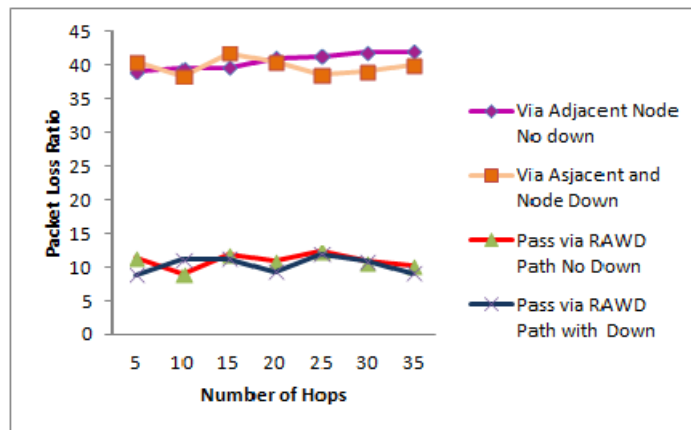


Figure 8. Packets loss during the attack

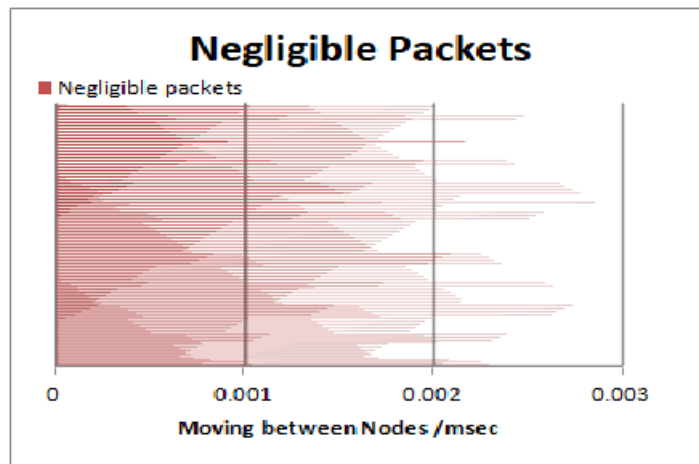


Figure 9. Unknown packet (attacker)

6. CONCLUSION

The paper proposes a new algorithm, RAWD, to create a new and smart path in the network between source and destination. This path will be used in case an attacker tries to broadcast a huge number of negligible packets, to increase the speed of receiving the emergency data and secure one during the DoS attack. The emergency evaluation problem is transformed into a conventional network flow problem in order to address

the issues of network congestion, delay time, and throughput, as well as to reduce the load on the necessary path and the amount of time required for evacuation. Creating a backup path from the current routing table by taking a thorough picture of all network nodes is the goal here. We also try to make each node retain the main packets in its buffer until starting to reroute from the new path. Additionally, the buffer enables us to prevent the loss of any emergency packets that may unintentionally come from other nodes. These regular packets will be diverted immediately along the secure way, which is taken into consideration in the event of an attack. When the packets are given a priority, managing the network congestion problem is easier. Our simulation results have shown that our solution outperforms the alternatives in terms of network congestion, throughput, delay time, loss ratio, and network overheads, among many other important metrics.

ACKNOWLEDGEMENTS

This research was supported and funded by the research sector, Arab Open University -Kuwait Branch under decision number 22005.





REFERENCES

- [1] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: a survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, Mar. 2021, doi: 10.3390/iot2010009.
- [2] S.-M. Cheng, P.-Y. Chen, C.-C. Lin, and H.-C. Hsiao, "Traffic-aware patching for cyber security in mobile IoT," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 29–35, 2017, doi: 10.1109/MCOM.2017.1600993.
- [3] Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog computing security and privacy for the internet of thing applications: state-of-the-art," *Security and Privacy*, vol. 4, no. 2, Mar. 2021, doi: 10.1002/spy2.145.
- [4] O. Tavallaie, J. Taheri, and A. Y. Zomaya, "Design and optimization of traffic-aware TSCH scheduling for mobile 6TiSCH networks," in *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, May 2021, pp. 234–246, doi: 10.1145/3450268.3453523.
- [5] R. Sethi, B. Bhushan, N. Sharma, R. Kumar, and I. Kaushik, "Applicability of industrial IoT in diversified sectors: evolution, applications and challenges," in *Multimedia Technologies in the Internet of Things Environment*, Springer, 2021, pp. 45–67.
- [6] H. Cui, P. Sun, and A. Boukerche, "A novel cloud-based traffic aware data routing protocol for smart connected vehicles," *Computing*, vol. 104, no. 7, pp. 1701–1720, Jul. 2022, doi: 10.1007/s00607-022-01068-3.
- [7] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber security threats to IoT applications and service domains," *Wireless Personal Communications*, vol. 95, no. 1, pp. 169–185, 2017, doi: 10.1007/s11277-017-4434-6.
- [8] A. M. Albalawi and M. A. Almaiah, "Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in Iot environment," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 9, pp. 2988–3011, 2022.
- [9] F. Ullah *et al.*, "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/ACCESS.2019.2937347.
- [10] S. Ghazanfar, F. Hussain, A. U. Rehman, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT-flock: an open-source framework for IoT traffic generation," in *2020 International Conference on Emerging Trends in Smart Technologies (ICETST)*, Mar. 2020, pp. 1–6, doi: 10.1109/ICETST49965.2020.9080732.
- [11] I. Cvitić, D. Peraković, M. Periša, and M. Botica, "Novel approach for detection of IoT generated DDoS traffic," *Wireless Networks*, vol. 27, no. 3, pp. 1573–1586, Apr. 2021, doi: 10.1007/s11276-019-02043-1.
- [12] R. J. Raimundo and A. T. Rosário, "Cybersecurity in the internet of things in industrial management," *Applied Sciences*, vol. 12, no. 3, Feb. 2022, doi: 10.3390/app12031598.
- [13] A. Rayes and S. Salam, *Internet of things from hype to reality*. Cham: Springer International Publishing, 2022.
- [14] M. S. Farooq, O. O. Sohail, A. Abid, and S. Rasheed, "A survey on the role of iot in agriculture for the implementation of smart livestock environment," *IEEE Access*, vol. 10, pp. 9483–9505, 2022, doi: 10.1109/ACCESS.2022.3142848.
- [15] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPL-based routing protocols in IoT applications: a review," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 5952–5967, 2019, doi: 10.1109/JSEN.2019.2910881.
- [16] S. K. Prasad, T. Sharma, V. Sharma, and S. Chauhan, "RSETR: route stability based energy and traffic aware reactive routing protocol for mobile ad hoc network," in *2022 IEEE Delhi Section Conference (DELCON)*, Feb. 2022, pp. 1–9, doi: 10.1109/DELCON54057.2022.9753442.
- [17] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, "Attestation-enabled secure and scalable routing protocol for IoT networks," *Ad Hoc Networks*, vol. 98, Mar. 2020, doi: 10.1016/j.adhoc.2019.102054.
- [18] X. Yuan, C. Li, and X. Li, "DeepDefense: identifying DDoS attack via deep learning," in *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, May 2017, pp. 1–8, doi: 10.1109/SMARTCOMP.2017.7946998.
- [19] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT





- communications,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3677.
- [20] B. Susilo and R. F. Sari, “Intrusion detection in IoT networks using deep learning algorithm,” *Information*, vol. 11, no. 5, May 2020, doi: 10.3390/info11050279.
- [21] L. S. Buriol, M. G. C. Resende, C. C. Ribeiro, and M. Thorup, “A memetic algorithm for OSPF routing,” in *Proceedings of the 6th INFORMS Telecom*, 2002, pp. 187–188.
- [22] M. A. V. Paul, T. A. Sagar, S. Venkatesan, and A. K. Gupta, “Impact of mobility in IoT devices for healthcare,” in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 21, doi: 10.1007/978-3-319-93940-7_11, 2019, pp. 243–261.
- [23] K. Sha, T. A. Yang, W. Wei, and S. Davari, “A survey of edge computing-based designs for IoT security,” *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, May 2020, doi: 10.1016/j.dcan.2019.08.006.
- [24] M. Z. Gunduz and R. Das, “Cyber-security on smart grid: Threats and potential solutions,” *Computer Networks*, vol. 169, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
- [25] D. G. S. Pivoto, L. F. F. de Almeida, R. da Rosa Righi, J. J. P. C. Rodrigues, A. B. Lugli, and A. M. Alberti, “Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review,” *Journal of Manufacturing Systems*, vol. 58, pp. 176–192, Jan. 2021, doi: 10.1016/j.jmsy.2020.11.017.
- [26] M. Al-Husban, A. Al-Husban, and H. Yaseen, “Cyber attack detection technique to improve cyber security using data mining methods,” in *Istanbul Bosphorus International Cyberpolitics, Cyberlaw and Cybersecurity Conference*, 2017.
- [27] H. Yaseen, A. S. Al-Adwan, M. Nofal, H. Hmoud, and R. S. Abujassar, “Factors influencing cloud computing adoption among SMEs: the jordanian context,” *Information Development*, Apr. 2022, doi: 10.1177/02666669211047916.
- [28] R. S. Abujassar, H. Yaseen, and A. S. Al-Adwan, “A highly effective route for real-time traffic using an iot smart algorithm for tele-surgery using 5G networks,” *Journal of Sensor and Actuator Networks*, vol. 10, no. 2, Apr. 2021, doi: 10.3390/jsan10020030.

BIOGRAPHIES OF AUTHORS







Radwan S. Abujassar     is currently Associate professor at the Computer Science at the ITC program in Arab Open University which is following the OU University in UK. Dr Radwan was in the computer Engineering department of the faculty of Engineering at the Bursa Orhangazi University in Turkey. Dr. Radwan received his B.Sc. degree from Applied Science University, Amman, Jordan in 2004, and M.Sc. degree from New York Institute of Technology in 2007, both in computer science. His Ph.D. degree in computing and electronic in the field of IP recovery in IGP and MANET networks from University of Essex, UK in 2012. His research interests include network and controls, routing protocols, cloud computing and network security. He can be contacted at email: r.abujassar@aou.edu.kw.



Mohamed Sayed     received his B.S. degree in Computer Engineering from Alexandria University as the first rank in June 1987, his M.Sc. degree in Engineering Mathematics from Alexandria University in 1992 and Ph.D. degree in Mathematics of Computing from Birmingham University in 1998. Prof. He is now the Rector of the Arab Open University in Kuwait. His research interests are in computational algebra and enumeration, pattern recognition and deep machine learning. He is a member of IEEE, LMS, SIAM. He can be contacted at email: msayed@aou.edu.kw.



Husam Yaseen     is an Associate Professor of E-Business and Business Analytics at American University of Madaba, Jordan. He holds a Ph.D. in Information Systems/E-Commerce from The University of Portsmouth, UK. He is particularly specialized in digital business transformation and development. His research interests include UX, Digital Marketing, Business Analytics, e-commerce, IoT, cyber security, cloud computing and online purchase behaviour. Address: Business Administration Department, Faculty of Business and Finance, American University of Madaba. He can be contacted at email: h.yaseen@aum.edu.jo.