IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 July 2022, accepted 20 August 2022, date of publication 31 August 2022, date of current version 8 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3203070

RESEARCH ARTICLE

SHE Networks: Security, Health, and Emergency Networks Traffic Priority Management Based on ML and SDN

FOUAD A. YASEEN[1], NAHLAH ABDULRAHMAN ALKHALIDI[2], AND HAMED S. AL-RAWESHIDY[3], (Senior Member, IEEE)

[1]Electronics and Communication Department, College of Engineering, University of Baghdad, Baghdad 10071, Iraq
[2]Computer Science Department, College of Science, University of Baghdad, Baghdad 10071, Iraq
[3]Department of Electronic and Electrical Engineering, College of Engineering, Design and Physical Sciences, Brunel University London, Uxbridge, London UB8 3PH, U.K.

Corresponding author: Hamed S. Al-Raweshidy (hamed.al-raweshidy@brunel.ac.uk)

ABSTRACT Recently, the increasing demand to transfer data through the Internet has pushed the Internet infrastructure to the final edge of the ability of these networks. This high demand causes a deficiency of rapid response to emergencies and disasters to control or reduce the devastating effects of these disasters. As one of the main cornerstones to address the data traffic forwarding issue, the Internet networks need to impose the highest priority on the special networks: Security, Health, and Emergency (SHE) data traffic. These networks work in closed and private domains to serve a group of users for specific tasks. Our novel proposed network flow priority management based on ML and SDN fulfills high control to give the required flow priority to SHE data traffic. The proposal relies on selected header bits from the traffic class field of a packet using the ML to prioritize traffic flows according to the precedence levels by governing the Differentiated Services Code Point (DSCP) bits in keeping with network administrator policies. The proposed network has been evaluated and performed utilizing the MATLAB platform and the Mininet simulator. The results of extensive testing show enhancement by applying our forcing priority algorithm obtained an efficient reduction in queuing delay and lost packets. The average waiting time in queue was reduced by around 61%, and the lost packets hit 0.005% when adopting the SDN-based ML network traffic priority management.

INDEX TERMS AI, DSCP, packet header, precedence level, SDN.

I. INTRODUCTION

Nowadays, the world is experiencing natural terrible changes and challenges besides terrorist threats. In order to prevent or at least reduce the destructive effects of these disasters, world countries need reliable and trusted communication networks. Such special networks will help in saving the people and the country's national security. Therefore, these special networks have the highest traffic priority to ensure speed response by responsible humans. To enable the forwarding of Security, Health, and Emergency (SHE)'s data traffic over Internet networks, this data traffic must be deported and transferred through public telecommunication networks. This process requires that communication networks include diverse and modern technologies such as Machine Learning (ML), Artificial Intelligence (AI) [1], and Software-Defined Networking (SDN) to attain the highest performance of these networks [2]. To guarantee efficient data transferring of SHE networks across the public Internet links, that needs to dedicate the highest priority for this data if these special networks fail in the wake of severe risks.

The term ''special networks'' in this paper indicates that networks connect their users within a private and authenticated login to communicate with each other in close domain networks. As examples of such networks are Ad hoc [3], security or police, cellular, and health networks. However, some of these networks are considered confidential, secretive, and not available for public use. Therefore, there is restricted

The associate editor coordinating the review of this manuscript and approving it for publication was Qingli Li.

information for research about some of the special networks, i.e., not many references are available. On the other hand, all the traffic data of these networks can be processed and forwarded within packets that pass over Internet infrastructures.

SHE networks can exist in two structures: Based stationary infrastructures and Non-stationary infrastructure networks. The stationary infrastructure depends on a fixed groundwork, where links route the data traffic to a base station within predefined paths. It is relatively expensive and cannot be applied in hostile conditions such as proactive catastrophes handling applications (abnormal weather forecasting, earth quacks, volcano). While, the non-stationary network does not depend on fixed network devices, i.e., wireless infrastructure networks such as Ad-hoc, security, and health networks. These networks rely on a closed domain structure where the users can only communicate efficiently within this domain. In the case of failure of the non-stationary networks, they could use the Internet links to deliver information but without high priority for their data traffic. To solve the issue of the priority of data forwarding over Internet links; this data should take the highest priority by network devices for emergency routing.

Our contribution aims to enhance packets traffic forwarding based on SDN and ML in case of failure of the SHE network through the Internet. We propose novel traffic priority management, the novelty of our proposal relies on selecting specific header bits from the traffic class field rather than checking the whole header bits (320bit). Selecting header bits depends on which one of SHE traffic should be with the highest priority. Controlling the differentiated service and assured forwarding bits in a packet header field forces desired priority for specific traffic. The proposal relies on selected header bits from the traffic class field of a packet using the ML to prioritize traffic flows according to the precedence levels by governing the Differentiated Services Code Point (DSCP) bits in keeping with network administrator policies. The traffic management based on selected bit shows improvements in several aspects, such as processing time delay, consuming power, and reducing the burden on the server. The rest of the paper is organized as background and related works in section II, the proposed network is described in section III. The SDN controller and the OpenFlow Switch (OFS) are exhibited in section IV, in section V, forced flow priority control is presented. Simulation and performance evaluation are explained in section VI.

II. BACKGROUND AND RELATED WORKS

In the last two decades, numerous study institutes focused on in-depth research on packet engineering for different network technologies and topologies. A series of fulfillment has been performed in forwarding and routing protocols, network traffic classification, and Quality of Service (QoS) [4], [5], [6]. In [7], they presented an ML approach to optimize network performance and attain optimal energy efficiency by applying a Q-learning algorithm. To guarantee the QoS acquainted with a secure routing protocol, Guo *et al.*, proposed a deep-reinforcement algorithm that relies on history traffic requests by interacting with the underlying network circumstances and dynamically optimizing the routing guideline [8]. The emergence of ML presents a modern methodology for data traffic classification. The ML mechanism requires extracting the features of the data. The processed data compares to the earlier knowledge available to the trainer, which usually considers the form of analyzing data collected and transferred to the classifier to manage data classification. The authors of [9] used different ML algorithms for the accurate traffic classification of mobile applications. Also, the classified traffic flows of each application were controlled by the QoS by applying the SDN controller. In [10], They used Internet protocol autonomous system inquiry based on deep packet inspection and ML technique for traffic classification. They obtained a fast and acceptable flow classification for diverse kinds of traffics.

The SDN technology emerged to overcome the diverse kinds of network devices produced by many different companies. The SDN architecture relies on separation the data layer from the control layer. In the SDN scene, the control packets do not use the conventional IP routing alone, but they could employ various mechanisms and algorithms according to the task to be executed by the algorithm [11]. Moeyersons *et al.*, proposed an executable SDN to ensure the bandwidth required for emergency traffic flows in online and offline cases. The online model suggested repeated recalculations as the best solution for all demanded flows. The offline approach allows for problem optimization for a set of flows, but it is computationally costly, particularly a variant where the streams can be split across parallel paths [12]. Authors in [13] presented a mechanism for bandwidth guaranteed by applying a prioritization method to determine the absolute packets flow priority. The geospatial streams are mapped into segments with various QoS levels.

The rising of using AI in communication networks transforms network management into a cognitive manner to forward data packets. Where a network can self-react and self-adapt to improving statuses with minimum manwork efforts. The QoS for traffic identification by Using ML and DPI in SDN has been proposed by [4]. They suggested a design that combines semi-supervised ML and DPI of multi-classifier in SDN to classify streams into various QoS levels. The classifier can modify the fast emergence of network utilization and changeable flow features of a current network by repeating re-training based on the changing traffic database. Chang *et al.* presented offline and online traffic analysis applications that relied on deep learning techniques over an SDN testbed. They employed an open network flow dataset with the seven most common applications, such as the testing datasets and deep learning training [14].

To address the forwarding challenges of SHE networks traffic within Internet infrastructure, we propose novel priority management based on ML, and SDN. By controlling the differentiated service and assured forwarding bits in a packet header field to force desired priority for specific

traffic. Therefore, SHE networks must have the highest traffic priority to guarantee a fast response by the people in charge. To speed up the passing of SHE packet flows over the Internet, the proposed task of the ML is to classify and identify incoming flow packets that are forwarded to the AI to make forwarding decisions. Then, the classified packet flow will be given the highest priority and QoS by the SDN controller to pass through the Internet devices depending on the AI decisions.

III. PROPOSED SYSTEM DESCRIPTION

Currently, Internet traffic suffers from greedy service applications, such as multimedia streaming, network drivers storage, and real-time video games; are forcing the Internet network resources to the critical edge [15]. In the case of an emergency, it is necessary to prioritize network data traffic coming to and from SHE networks in the event of large civilian masses, disasters, and breakout pandemics to coordinate response and relief. Such as the case of COVID-19, the Internet traffic experienced an unprecedented demand for data forwarding, which caused critical congestion in Internet traffic networks. Therefore, an urgent need is raised for a system that controls giving precedence to the passing of emergency network data. Our proposal addresses this issue by prioritizing SHE network traffic, where data must be forwarded with high priority and QoS across different Internet infrastructure networks. The SDN networking technology is widely spread in different domains at the service provider levels which composes the current Internet infrastructure. Although, not all Internet infrastructures are applied to SDN technology. Therefore, we assume our proposal applies to those administrative domains that deploy SDN technology in their networking infrastructures. So, in the proposed system, the human decision-maker represents the network domains administrator that supervises the Internet and the special networks in a country uses the SDN networks, besides the traditional networking infrastructures.

Figure 1 illustrates the proposed SHE networks architecture that consists of three main parts:

- The Gateway and analytic servers.
- The ML and Automatic Decision-Maker (ADM).
- The SDN controller and OpenFlow Switches (OFS).

To provide a clear vision of the suggested idea, we explain the task of each part with details in the flowing sections.

A. GATEWAY AND ANALYTIC SERVERS

The gateway is a pivotal checkpoint for data traffic on its way from or to other networks. It communicates and send data between Internet networks and service networks, that means the gateway provides access to the Internet and all IP networks. The incoming traffic is subjected to verify the priority and QoS based on the ML, ADM, and SDN to make decisions. When there is no information about the incoming traffic in the gateway and analytic servers, the traffic will be sent to the ML for classification. Then the classified data is

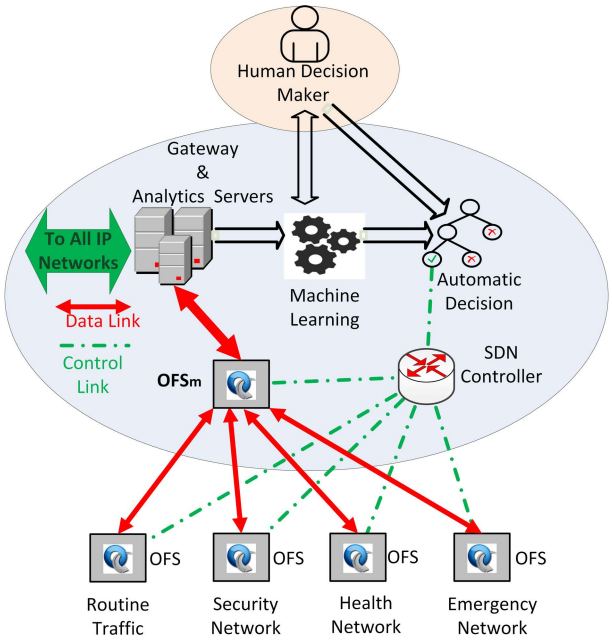

FIGURE 1. Proposed SHE networks.

subordinated to make a decision by the ADM according to the administrator policy. Whilst, in the case of information availability of the arrived traffic flow to the gateway and analytic servers, it will assign the required priority and QoS without asking the ML and ADM based on previous decisions for that traffic flow.

B. ML TRAFFIC CLASSIFICATION

Current traffic classification analysis relies on the packets header content and payload to identify traffic flows. However, the packet header involves sufficient information for traffic flow classification. To perform our proposal for online and offline traffic classification, we apply traffic flow statistical set characteristics such as packet length, byte, bit accounts, and packet direction. Modern applications aim to develop encryption for higher privacy and security. These applications use widely known secure protocols such as SSH, SSL, HTTPS, etc. Therefore, traffic flow classifications necessitate an intelligently and efficiently analysis based on the bits chosen from the packet headers rather than the entire field [16]. Furthermore, the traffic subjects for examining can be treated as a single packet or a flow (1^{st} packet as a guider) to be categorized. Thus, this points to adaptability in choosing the labeled features and controlling the number of these features. In our previous proposed algorithm mechanism FDPHI [16], we performed traffic classification based on the bit account of the arrived packet. Due to the widespread deployment of applying IPv6 in Internet infrastructure networks, we focused on the IPv6 packet header. Consider packets, bytes, and bits statistics of the header, which hold sufficient information to identify packets as unique identifiers for the application, in addition to sequence-dependent of arriving packets. This

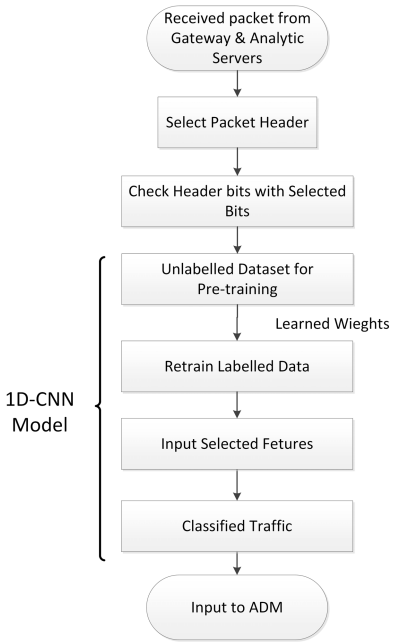

FIGURE 2. Proposed ML For SHE algorithm.

process will give unique identifiers for the income packets flow. The FDPHI uses 1D-CNN to automate learning the most representative features of traffic flow classes as in Figure 2 illustrates the ML traffic classifier. The semi-supervised ML approach obtains its learning from both unlabeled and labeled datasets. The ML applies a large amount of unlabeled data with a small number of categorized datasets to feed the ML to classify the data traffic. The ML classifies the traffic flow that sequentially enters the classifier as an input of three columns matrix (packet number, packet direction, and bit position). Various portions of the unlabeled dataset were sampled many times for pre-training by the CNN to extract learned weights. These weights are used to re-train on labeled datasets to extract selected features of the flow. Our system extracts flow features from the header bits. Those features can be utilized as input parameters by the automatic decision-maker. In IPv6, the header bits are 320, as shown in Figure 3. The position and order of the header bits specify the deduced features of the data flow based on the chosen bits. That means the order of the selected header bits determine traffic flow characteristics. At this point, the ML classify traffic according to the elected header bits. The automatic decision-maker assigns the necessary priority to SHE traffic to be forwarded by the SDN controller via the underneath OpenFlow Switches (OFS)s.

C. DIFFERENTIATED SERVICES BASED ON ADM

The Automatic Decision-Maker (ADM) receives the classified traffic from the ML that categorizes incoming flows into Security, Health, and Emergency traffic. The ADM prioritizes classified traffic to precedence levels according to network administrator policies by controlling the Differentiated Services Code Point (DSCP) bits. Algorithm 1 illustrates the procedure that is adopted to prioritize packets based on DSCP bits (DS5-DS3) and drop probability bits (DS2-DS1) in the suggested system. The field of traffic class (8bits) indicates IPv6 packet priority [17]. It supports routers to manage the traffic flow according to the packet priority. As congestion happens on a network device, the packets with the lowest priority level consider "routine traffic" or discarded.

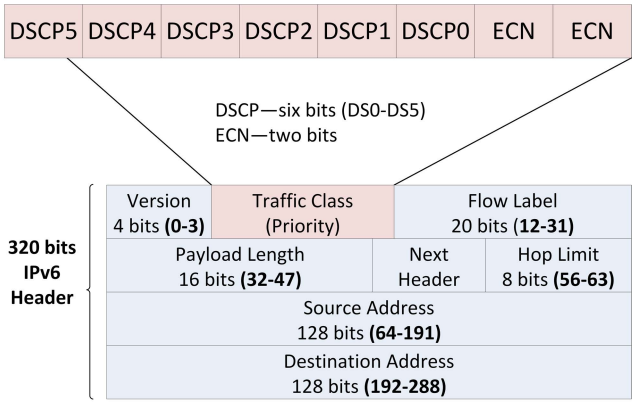

FIGURE 3. IPv6 packet header fields and bits order.

TABLE 1. DSCP precedence level.

Precedence Level	Description
0	Best Effort
1	Class 1
2	Class 2
3	Class 3
4	Class 4
5	Express Forwarding (EF)
6	Apply common IP routing protocols
7	link layer & network layer keep alive

By performing DSCP on our proposal, the DSCP is a set of End to End (E2E) QoS abilities. E2E QoS is the capability of the network devices to fulfill the service expected by a particular network traffic flow from one end to another. The IPv6 header is a fixed size of 320 bits, as shown in Figure 3. Our algorithm focuses on the 8 bits of the traffic class field that consists of a (6 bits) DSCP to handle priority packet classification. The remaining (2 bits) are Explicit Congestion Notification (ECN) precedence values divided into two ranges: i) congestion control traffic and ii) non-congestion control traffic [18].

To describe how to set the DSCP values in QoS and the relation between DSCP and IPv6 precedence. Table 1 illustrates the DSCP uses precedence bits where the three most significant bits: DS5, DS4, and DS3 determine the priority level. While (DS2 and DS1) set the drop probability. The default value of DS0 is always zero. A network device prioritizes flow via class first. Later it distinguishes and prioritizes the same class flow to three levels (High, Medium, and Low), taking into account the drop probability. The DSCP model does not define an exact definition of "high," "medium,"

TABLE 2. DSCP coding for defining AF classes and probability.

Drop	Class 1	Class 2	Class 3	Class4
Low	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Medium	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
High	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

and ''low'' drop probability. Not all network devices meet the DSCP setting (DS2 and DS1); even though these devices recognize the DS2 and DS1, that does not mean the network devices trigger the same Per Hope Behavior (PHB) forwarding activity at each node. Due to each device implementing its response based on its configuration [19]. To avoid the problem of triggering the individual PHB forwarding action at each network node, the SDN infrastructure in our proposal tackles a concrete solution to an Assured Forwarding (AF). Table 2 represents the DSCP coding for setting the AF classes alongside the probability of a packet. The AF is a means for differentiating service levels for IP forwarding assurances.

Also, the AF per hope behavior ensures guaranteed bandwidth for an AF class and provides access to additional bandwidth, if possible. Classes 1-4 indicate the AF classes (as shown with red font in Table 2), AF1x to AF4x, and x represents the probability drop (Low-01, Medium-10, High-11) as shown with green font. For each class, according to a network's policy, flow can be picked for a PHB relied on demanded throughput, jitter, delay, packets loss, or according to the priority of the available network services.

Algorithm 1 illustrates the procedure of differentiating and prioritizing traffic flows based on header field bits (bits 4 - 11). The classified traffic by the ML is input to the ADM to force DSCP Precedence Levels (DS5-DS3) by setting AF classes and drop probability. The SDN controller responds to these actions to order the OFSm and other OFSs to forward the prioritized traffic. Algorithm 2 explains in detail the forcing priority steps of assigning DSCP precedence levels and AF classes.

Algorithm 1: Differentiate and Prioritize Traffic Flow

```
Input Classified Traffic Flow
Classified Traffic Policy
Check header field (bits 4-11)
if Traffic is SHE then
    Determine the Highest Priority (Security, Health,
      or Emergency) Policy
    Assign DSCP Precedence Levels (DS5-DS3)
    Set AF Class & Drop Probability (DS2 & DS1)
    Go to Step 11
else
    Routine Forwarding
    Order SDN Controller to Schedule Class & Drop
      Probability (AF)
    Create or Update Flow Tables by SDN Controller
    Send Flow Tables to OFSs
    Forward Traffic Flow According to Priority Policy
      Through OFSs
end
```

IV. SDN CONTROLLER AND OPENFLOW SWITCHES

Rising the new promising network technology of the SDN supports the Internet infrastructure to be more adaptable and flexible. SDN concept depends on separating the data plane (forwarding layer) from the control plane. The forwarding layer comprises physical OpenFlow switches to deliver data efficiently. However, the control plane is served by an SDN controller to create flow tables, which has a comprehensive seen to govern forwarding data across OpenFlow switches [20], [21]. Besides, in the SDN ecosystem, the packets forwarding does not employ only the standard IP routing because it could use diverse mechanisms and algorithms to perform any task that is required to be executed by the algorithm.

OpenFlow protocol is a popular protocol that connects the SDN controller and data forwarding devices. The Open Networking Foundation (ONF) systematized the OpenFlow protocol as the southbound Application Programming Interface (API). The API is a software port and an open developing model, allowing cooperation with other software parts. The term API refers both to the implementation and specification. That means the API describes how to build or link such a connection or interface to each other. A network device that fits these rules is said to perform an API [22].

When the main OFS (OFS_m) receives a packet, it checks its flow table to send the income packet to the destination. If the OFS_m gets a match for this packet, it directly forwards it to the destination. Otherwise, the OFS_m contacts the SDN controller about this packet to determine the egress port. The SDN controller makes a decision concerning that packet based on the classified and prioritized decisions by the ADM. Then, the SDN controller modifies and updates the flow table entries according to its vision of network topology and sends the updated tables to the OFS_m and other OFSs. The OFS_m governs the data traffic priority from/to the Gateway, while the other OFSs manage the local networks' traffic priority.

Figure 4 demonstrates the fields of the flow table that the packets flow have to subject to be checked by the OFS. There are three typical fields for entries a flow table:

1) The *Matching Rules* field includes information policies to be met with those in the arrived packets header, metadata, and ingress interface. The ADM sets the DSCP bits to force the packet to get the required priority, which is implemented by the SDN controller to determine the E2E path with QoS that is defined by the ADM.
2) The *Actions* field implements a set of directions and instructions on the arrived packets through the OFSs to manage how to reroute the matched data. These actions are made by the SDN controller to order the OFS to

Algorithm 2: Forcing Priority

```
Input Classified SHE Traffic Flow
Apply Traffic Policy
Change DSCP bits(DS5-DS1)
Class 1: Set DS3 = 1
for j=1 to 3 do
    Set AF1j {Drop Probability}
end
Class 2: Set DS4 = 1
for j=1 to 3 do
    Set AF2j
end
Class 3: Set DS4 & DS3 =1
for j=1 to 3 do
    Set AF3j
end
Class 4: Set DS5 = 1
for j=1 to 3 do
    Set AF4j
end
```

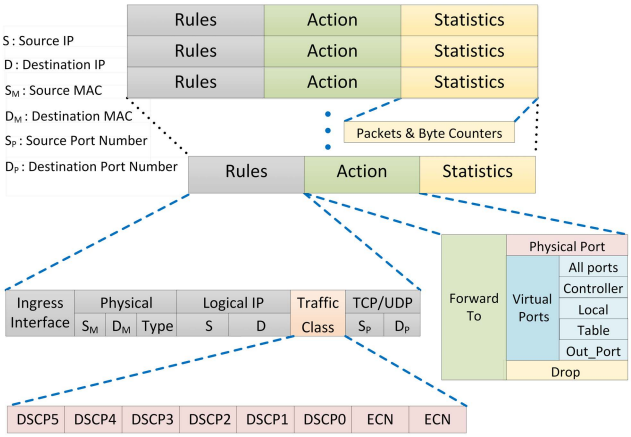

FIGURE 4. Flow table fields created by the SDN controller.

forward data traffic to the physical port, virtual port, or drop the packet.

3) The *Counters* field gets the statistics (the number of packets, number of bytes, and the period of a specific flow.

The Gate-Way (GW) and analytic servers are connected directly by links that transfer data from and to all the OFSs and the Internet networks. The GW serves as an access point to any IP networks placed outside the SDN network. Also, it is a traditional tool that joins the SDN network to the Internet backbone. The GW operates based on standard protocols and policies. That is, the GW is not obedient to the controls and operations of the SDN controller. The SDN network is an innovative and dynamic technique for networking management. In the SDN network infrastructure, performance depends on the SDN controller, which centrally watches the entire topology and scalability of the network [23]. In such

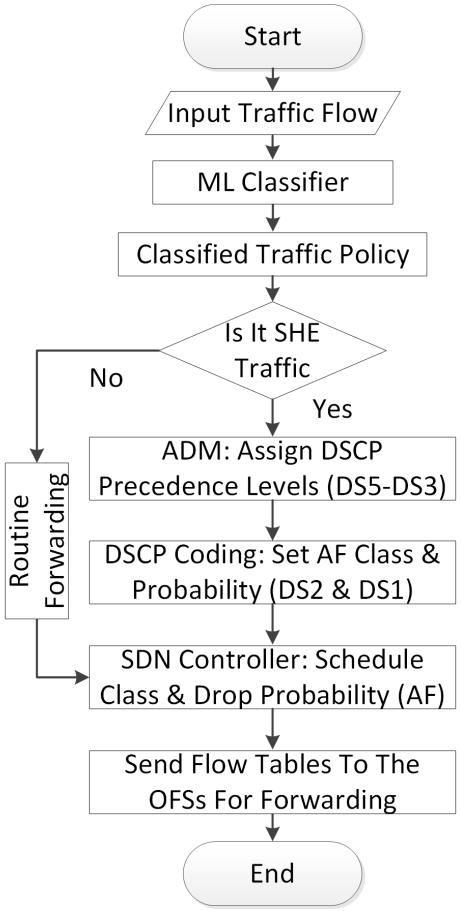

FIGURE 5. She network algorithm.

a network, when the first packet of every flow arrives at an OFS, each OFS must ask for rules for packet forwarding. The SDN controller provides and updates the rules according to ADM decisions. Moreover, the SDN controller determines the appropriate actions to forward packets depending on the priority specified by the ADM, which is governed by the network administrator. In the case of emergencies, the SDN network administrator observes and manages the network performance by giving the highest priority decision to one type of SHE traffic to pass via the network. Figure 5 summarizes our algorithm steps to classify, force the traffic priority, and forward the prioritized packets according to DSCP precedence levels.

V. FORCED FLOW CONTROL PRIORITIZING

To give the required priority to SHE traffic, we need to understand the meaning of traffic priority in a network by simple words is that *jump the waiting queue*. Figure 6 illustrates the packet queuing delay in network devices (routers or switches). Data packets are linked between network devices to forward the packets for transmission. This process requires income data packets to be queued and wait for serving by the device. In general, the communication networks suffer from several types of delay: i) *Transmission Delay*, ii) *Propagation Delay*, iii) *Queuing Delay*, and iv) *Processing Delay*. The

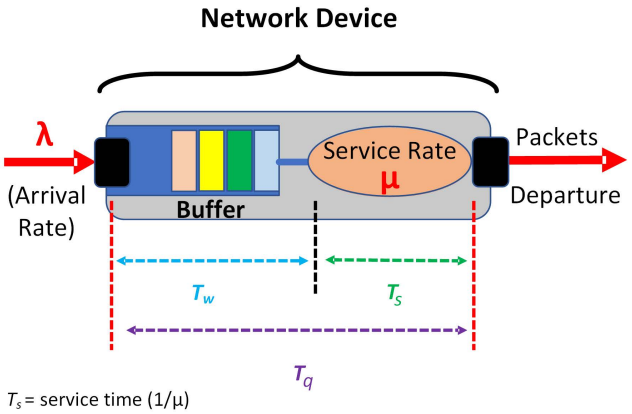

FIGURE 6. Packet queuing delay.

first two types are negligible due to their tiny values [24]. However, the processing delay concerns the hardware of the network device. The software developer cannot manage the processing delay to control or reduce it; because the processing delay depends on industrial technology. The priority is related to the packet waiting time in the queue (Queuing Delay) to forward it to its destination. In an SDN, a developer can prioritize a specific packet or flow by jumping the queue by applying the highest priority and Assured Forwarding.

Queuing delay has a considerable impact on the operation and efficiency of the network applications; it is reasonable to describe the priority based on assumptions of our proposed SHE traffic in the SDN network.The $M/M/1/\infty$ model is more suitable for our system due to its focus on the fact that packet bits enter the network device interface sequentially. Therefore, we will apply queuing theory in the communication network for priority modeling of $M/M/1/\infty : SP$, where SP is the Scheduling Policy [25]. The transmission nature of packets' arrival in a network flows Poisson process, where the arrival packet rate () defines the average number of events per unit time. The possibility of (n) arrival packets happening at the time (t) can be given by:

$$P_n(t) = \frac{\lambda t^n}{n!} e^{-\lambda t} \tag{1}$$

The size of packets in our system is Markovian distributed, with expected packet length $E[P_L]$. The system sends packets at a constant throughput rate R bps. So, the service time is exponentially distributed, which relies on the distribution of P_L. The expected service time is $E[S]$, and the parameter of the service rate is $\mu = 1/E[S]$. Let us start with a two-classes priority system for simplicity, p_{ij} is the stable system probability where i packets with priority 1 in the system and arrival rate λ_1 with service rate μ_1, and j packets with priority 2 in the system and arrival rate λ_2 with service rate μ_2. Based on these assumptions, a set of differential equations can be derived for the steady-state probabilities:

$$\begin{aligned} \lambda P_{00} &= \mu_1 P_{10} + \mu_2 P_{01} \\ (\lambda + \mu_1) P_{i0} &= \lambda_1 P_{i-1,0} + \mu_1 P_{i+1,0} \end{aligned}$$

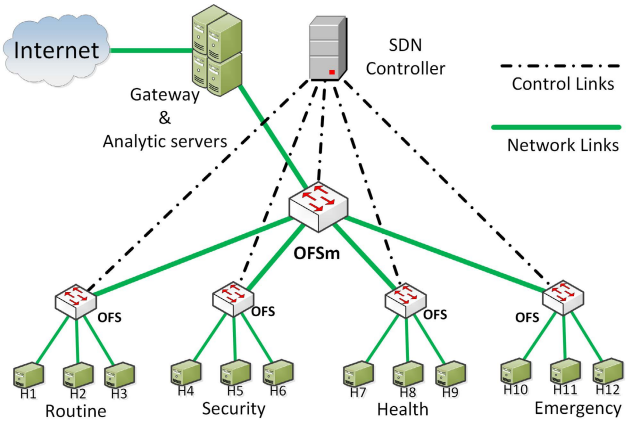

FIGURE 7. SHE network simulation setup.

$$\begin{aligned} (\lambda + \mu_2) P_{0j} &= \mu_1 P_{1,j} + \lambda_2 P_{0,j-1} + \mu_2 P_{0,j+1} \\ (\lambda + \mu_1) P_{ij} &= \lambda_1 P_{i-1,j} + \lambda_2 P_{i,j-1} + \mu_1 P_{i+1,j} \end{aligned} \tag{2}$$

where λ is the aggregation of λ_1 and λ_2. The average number of packets at the service facility (packet being served) represents the server utilization which is denoted by the symbol ρ. A good queuing system has a property that the service rate (μ) is always greater than the number of packets arrival rate (λ) and the ratio (λ/μ) must be less than 1 for the stable system, that is, $(\rho = \lambda/\mu) \leq 1$. Generally, if there are K preemptive priorities, then there are 2^K classes of priority equations. To measure the performance of such a system, we should derive distinct 2^K steady-state partisan producing functions from the equilibrium equations.

Since we have an $M/M/1/\infty : SP$ queuing system, $\mathcal{E}^{(n)}$ expresses the average number of class-n packets in the system in a steady-state. In our proposal, in the case of $\mathcal{R}$ packet classes, the SDN controller will prioritize SHE traffic against the routine traffic, which is resumed re-serving from the breakpoints. The $\mathcal{R}$ packet classes can be expressed as:

$$\mathcal{E}^{(n)} = \frac{\rho_n}{1 - \sigma_{n-1}} + \frac{\lambda_n \sum_{m=1}^{n} \lambda_m E\left[S_m^2\right]}{2(1 - \sigma_{n-1})(1 - \sigma_n)} \tag{3}$$

where $\sigma_n = \sum_{m=1}^{n} \rho_n$, $\rho_n = \lambda_n E[S_n]$, and S_m is a Poisson service time of a class-m.

VI. SIMULATION ENVIRONMENT AND PERFORMANCE EVALUATION

We performed and implemented our proposal by using the Mininet simulator. Figure 7 illustrates the setup of our suggested SDN network. The simulation design consisted of one main OFS (OFSm) and four OFSs representing four network domains (Security, Health, Emergency, and Routine) traffics, each OFS with three hosts. The SDN controller connects with all OFSs as shown in Figure 7 via dotted lines as control links. While the data traffic with green links that link the OFSs to the (*GW and Analytic Servers*) which connect the proposed SDN network to the Internet networks. We applied our algorithm on three flows representing the SHE traffic to show how it controls the priority according to classes level and implicit

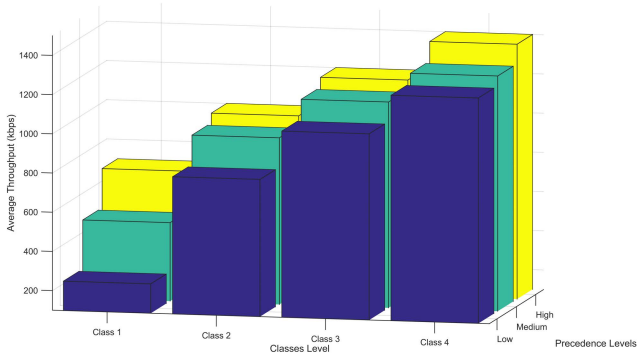

FIGURE 8. Precedence levels used in QoS classes.

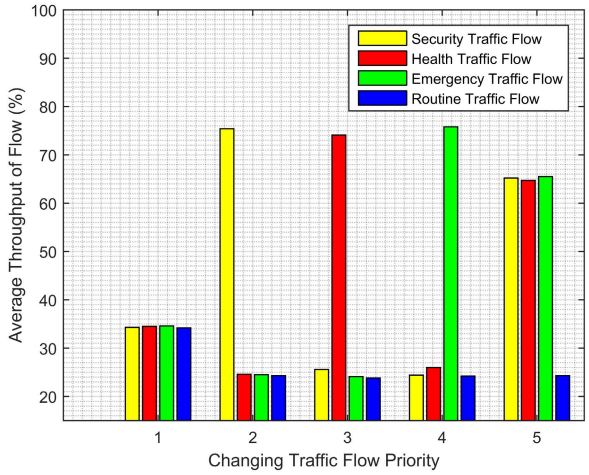

FIGURE 9. Prioritizing traffic based on selected flow.

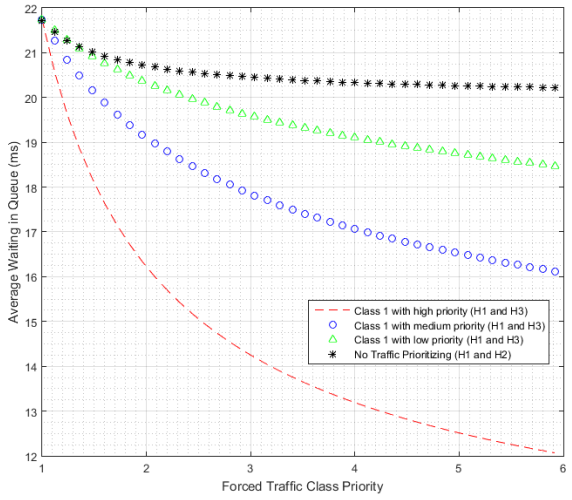

FIGURE 10. Forced traffic priority for selected local flow.

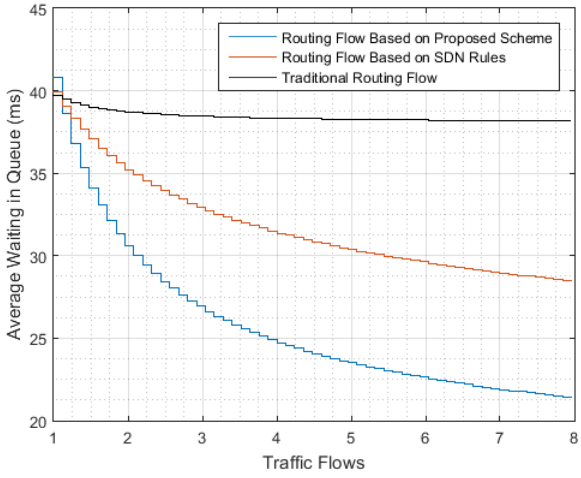

FIGURE 11. Traffic flows routing comparison based on priority.

class stages [26]. Figure 8 illustrates the precedence classes from the lowest to the highest priority (Class 1, Class 2, Class 3, and Class 4). Each class has three priority stages Low, Medium, and High. We injected four traffics representing SHE and Routine traffics to prove that the Low stage of a next class is assigned more throughput than the High stage of the previous class. For example, if we assign the Low stage of Class 2 to Security traffic that will have greater priority than all stages of Class 1, that if assigned to Health traffic. Whereas, if we set any level of Class 3 to Emergency traffic will take the highest priority than the Health and Security traffics. That means all stages of Class 3 have higher priority than all stages of Class 1 and Class 2.

Figure 9 shows the result of the forced packet priority for different flows pass through OFS_m. Initially, all the income traffic is non-prioritized, where the throughput of the four flows has been got almost equal bandwidth portions. However, when a selected flow for specific data traffic is forced to have the highest priority, the throughput for this flow had around 75% of the total throughput. While, when we assigned equal and the highest priority for multi SHE flows, the OFS_m will forward data packets for these flows with equal bandwidth. The OFS_m allocated approximately 65% of the total throughput, due to OFS_m handles packets fairly in terms of queuing and serving time.

Figure 10 gives an example of forcing priority for selected local flows of one network traffic (Security, Health, or Emergency). We selected a Health traffic network as local traffic flows to perform forcing priority within this network that consists of an OFS and three users (H7, H8, and H9). Initially, OFS (OFS of Health) received the generated traffic by H7 to be forwarded to H8 and H9 without forcing priority. Then, we applied our proposed approach to force the OFS to prioritize Class 1 traffic flow between H7 and H9 (High, Medium, and Low) based on the DSCP bits. As can be seen from Figure 10, the waiting time delay in the queue has been reduced to around 55% by forcing the OFS to assign the highest priority for selected traffic flow. This scenario can be applied to the other local networks to prioritize their traffic as desired.

Figure 11 compares the routing flows prioritizing based on our proposed scheme, SDN routing rules, and standard

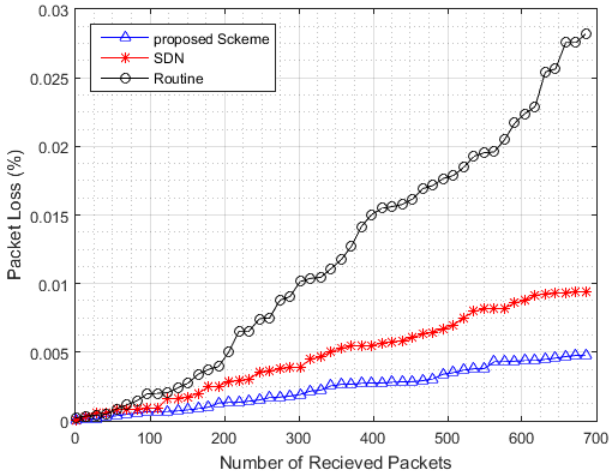

FIGURE 12. Packet loss comparison.

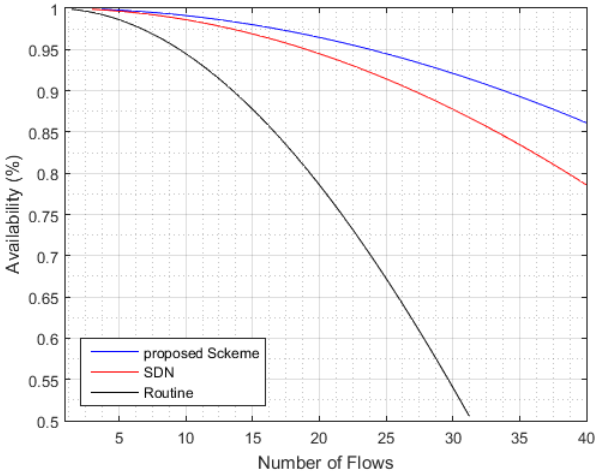

FIGURE 13. Availability of traffic flow.

routing. In this scenario, the Security network sends a traffic flow to Emergency networks via OFS_m with three traffic routing schemes:

- The traffic is routed based on ordinary routing (standards routing priority).
- The traffic is forwarded based on the SDN rules such as ingress and egress ports of the OFS_m.
- The traffic is routed according to our approach depending on the selected 8 bits of the traffic class field.

The priority has been enhanced by using SDN rules with a reasonable value of waiting delay time. Although, the SDN provided a good priority improvement over traditional traffic priority of around 30%. While our proposal doubled the performance of SDN when implemented for traffic prioritization by 61% for standard traffic and 29% for SDN.

Figure 12 compares packet loss of our proposal, SDN, and routine traffic flows. Although, the SDN provided a low packet loss rate compared with the traditional traffic. However, it still lacks optimizing and enhancing the scheduling of packet forwarding that our proposed scheme achieves with the lowest packet loss rate. The lost packet value for the SDN hits almost %0.01, while our system recorded less than %0.005. This decrease in packet loss is due to assigning the forced priority for a specific flow.

Figure 13 compares path availability for various traffic flow numbers. We generated three types of flows containing 50 packets of each, representing different network traffic. Also, this Figure exposes the improvement of our proposal against the SDN and traditional flow forwarding priority scheduling. Moreover, the path availability decreases as the number of packets increases. This degradation in the system performance is due to increasing the waiting time in the queue and the service rate of the server. Although the SDN achieves better availability performance than the traditional system, our proposed system superiors on the SDN in path availability for traffic flows.

VII. CONCLUSION

The SDN concept has provided exceptional features to the Internet networks infrastructure, such as reducing management efforts, expediting flow forwarding, and facilitating the amendment of forwarding tables. These features have led to advancements in administrating networks performance. Despite these techniques having been applied, the Internet infrastructures still require imaginative thoughts to satisfy the traffic demands of critical matters in disasters. In such cases, the special network must have the highest priority to forwarding data traffic to deal efficiently with emergencies by forcing the highest precedence levels traffic flow for these networks. Our proposal added a novel and creative touch to the SDN network infrastructure by using ML and SDN to achieve and control priority traffic flows management. The ML classifies the income traffic depending on the selected header bit statistics, which have sufficient information to recognize packets as unique identifiers for a flow. Although SDN provided acceptable performance compared to the traditional network, it lacked optimization and prioritization of scheduling forwarded packets in critical situations. Our system presented the ability to control and force traffic priority as the network administrator policy.

REFERENCES

[1] A. A. Afuwape, Y. Xu, J. H. Anajemba, and G. Srivastava, "Performance evaluation of secured network traffic classification using a machine learning approach," *Comput. Standards Interfaces*, vol. 78, Oct. 2021, Art. no. 103545.

[2] F. A. Yaseen and H. S. Al-Raweshidy, "Smart virtualization packets forwarding during handover for beyond 5G networks," *IEEE Access*, vol. 7, pp. 65766–65780, 2019.

[3] S. Liu, D.-G. Zhang, X.-H. Liu, T. Zhang, J.-X. Gao, C.-L. Gong, and Y.-Y. Cui, "Dynamic analysis for the average shortest path length of mobile ad hoc networks under random failure scenarios," *IEEE Access*, vol. 7, pp. 21343–21358, 2019.

[4] C. Yu, J. Lan, J. Xie, and Y. Hu, "QoS-aware traffic classification architecture using machine learning and deep packet inspection in SDNs," *Proc. Comput. Sci.*, vol. 131, pp. 1209–1216, Jan. 2018.

[5] O. Salman, I. Elhajj, A. Kayssi, and C. Ali, "A review on machine learning–based approaches for internet traffic classification," *Ann. Telecommun.*, vol. 75, pp. 673–710, Jun. 2020.
[6] J. Yan and J. Yuan, "A survey of traffic classification in software defined networks," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 200–206.
[7] T. Saba, K. Haseeb, A. A. Shah, A. Rehman, U. Tariq, and Z. Mehmood, "A machine-learning-based approach for autonomous IoT security," *IT Prof.*, vol. 23, no. 3, pp. 69–75, May 2021.
[8] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6242–6251, Jul. 2020.
[9] L.-V. Le, B.-S. Lin, and S. Do, "Applying big data, machine learning, and SDN/NFV for 5G early-stage traffic classification and network QoS control," *Trans. Netw. Commun.*, vol. 6, no. 2, p. 36, 2018.
[10] Y.-F. Huang, C.-M. Chung, C.-B. Lin, Y.-B. Peng, S.-H. Liu, and H. Chen, "Traffic classification of QoS types based on machine learning combined with IP query and deep packet inspection," in *Proc. 14th Int. Conf. Signal Process. Commun. Syst. (ICSPCS)*, Dec. 2020, pp. 1–4.
[11] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 27–51, 1st Quart., 2014.
[12] J. Moeyersons, B. Farkiani, B. Bakhshi, S. A. Mirhassani, T. Wauters, B. Volckaert, and F. De Turck, "Enabling emergency flow prioritization in SDN networks," in *Proc. 15th Int. Conf. Netw. Service Manage. (CNSM)*, Oct. 2019, pp. 1–8.
[13] F. Huang, J. Zhang, J. Xu, Y. Shao, and L. Pu, "An SDN-based QoS guaranteed mechanism for geospatial flows," in *Proc. IEEE Int. Conf Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Dec. 2019, pp. 1394–1401.
[14] L.-H. Chang, T.-H. Lee, H.-C. Chu, and C. Su, "Application-based online traffic classification with deep learning models on SDN networks," *Adv. Technol. Innov*, vol. 5, pp. 216–229, 2020.
[15] J. Moeyersons, B. Farkiani, T. Wauters, B. Volckaert, and F. De Turck, "Towards distributed emergency flow prioritization in software-defined networks," *Int. J. Netw. Manag.*, vol. 31, no. 1, Jan. 2021, Art. no. e2127.
[16] N. A. Alkhalidi and F. A. Yaseen, "FDPHI: Fast deep packet header inspection for data traffic classification and management," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 4, pp. 373–383, Aug. 2021.
[17] K. Nichols, S. Blake, F. Baker, and D. Black, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, document RFC2474, 1998.
[18] T. Szigeti, C. Hattingh, R. Barton, and K. Briley, Jr., *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*. San Jose, CA, USA: Cisco, 2013.
[19] O. T. Brewer and A. Ayyagari, "Comparison and analysis of measurement and parameter based admission control methods for quality of service (QoS) provisioning," in *Proc. MILCOM Mil. Commun. Conf.*, Oct. 2010, pp. 184–188.
[20] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.
[21] E. L. Fernandes, E. Rojas, J. Alvarez-Horcajo, Z. L. Kis, D. Sanvito, N. Bonelli, C. Cascone, and C. E. Rothenberg, "The road to BOFUSS: The basic OpenFlow userspace software switch," *J. Netw. Comput. Appl.*, vol. 165, Sep. 2020, Art. no. 102685.
[22] J. Doherty, *SDN and NFV Simplified: A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization*. Reading, MA, USA: Addison-Wesley, 2016.
[23] Y. Zhang, L. Cui, W. Wang, and Y. Zhang, "A survey on software defined networking with multiple controllers," *J. Netw. Comput. Appl.*, vol. 103, pp. 101–118, Feb. 2018.
[24] Y. Wang, K. Wang, R. Zhang, G. Zhang, and Y. Wang, "The optimization of networking method for the system protection communication networks based on the delay analysis," *J. Phys., Conf. Ser.*, vol. 1187, no. 4, Apr. 2019, Art. no. 042001.
[25] J. F. Shortle, J. M. Thompson, D. Gross, and C. M. Harris, *Fundamentals of Queueing Theory*, vol. 399. Hoboken, NJ, USA: Wiley, 2018.
[26] *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(1)*, 2009.

FOUAD A. YASEEN received the B.Sc. degree in electronics and communication engineering from the University of Technology, Baghdad, Iraq, in 1994, the M.Sc. degree in electronics and communication engineering from the University of Baghdad, Baghdad, in 2010, and the Ph.D. degree from Brunel University London, U.K., in 2019. He is currently a member of the Iraqi Engineers Association. He is also an Instructor Member with the CISCO Academic University of Baghdad/Computer Center. He has authored or coauthored 12 papers in international journals and referred conferences. His research interests include computer networks, wireless communication networks, mobile communication systems, SDN and cloud networks, and artificial intelligence. Besides, designing and implementing industrial electronic circuits. He was the Head of many teams for designing and installing computer networks for the Iraqi Ministry of High Education and Scientific Research and the Iraqi Ministry of Communications/The High Institution for Communications.

NAHLAH ABDULRAHMAN ALKHALIDI received the B.Sc. degree in control and computer engineering from the University of Technology, Baghdad, Iraq, in 1993, and the M.Sc. degree in control and computer engineering from the University of Baghdad, Baghdad, in 2013. She is currently an Instructor Member with the CISCO Academic University of Baghdad/College of Science. She is also a member of the Iraqi Engineers Association. She has authored or coauthored eight papers in international journals and refereed conferences. Her research interests include computer networks, wireless communication networks, fiber optics communication systems, SDN and cloud networks, and artificial intelligence.

HAMED S. AL-RAWESHIDY (Senior Member, IEEE) received the Ph.D. degree from Strathclyde University, Glasgow, U.K., in 1991. He was with the Space and Astronomy Research Centre/Iraq, PerkinElmer/USA, Carl Zeiss/Germany, British Telecom/U.K., Oxford University, Manchester Met. University, and Kent University. He is currently a Professor of communications engineering with Strathclyde University. He is also the Group Leader of the Wireless Networks and Communications Group (WNCG) and the Director of PG studies (EEE) with Brunel University London, U.K. He is also the Co-Director of the Intelligent Digital Economy and Society (IDEAS) and the New Research Centre which is part of the Institute of Digital Futures (IDF). He was the Editor of the first book *Radio over Fiber Technologies for Mobile Communications Networks*. He acts as a consultant and involved in projects with several companies and operators such as, Vodafone (U.K.), Ericsson (Sweden), Andrew (USA), NEC (Japan), Nokia (Finland), Siemens (Germany), Franc Telecom (France), Thales (U.K. and France), Tekmar (Italy), Three, Samsung, and Viavi Solutions, where he actualized several projects and publications with them. He is a Principal Investigator of several EPSRC projects and European project such as, MAGNET EU Project (IP), from 2004 to 2008. He has published more than 450 journals and conference papers. His current research interests include 6G with AI and the IoT. He is an external examiner for the Beijing University of Posts and Telecommunications (BUPT) and the Queen Mary University of London. Further, he was an external examiner for a number of the M.Sc. Communications Courses at the Kings College London, from 2011 to 2016. He had contributed to several White Papers. Specifically, he was the Editor of White Paper in Communication and Networking, which has been utilized by EU Commission for research. He has been invited to give presentations at EU Workshop and delivered two presentations at Networld2020, as well as being the Brunel representative for NetWorld2020 and WWRF for the last 15 years.