IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 October 2023, accepted 4 November 2023, date of publication 13 November 2023,
date of current version 16 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3332119

RESEARCH ARTICLE

Attacks Notification of Differentiated Services Code Point (DSCP) Values Modifications

ALA ABDULSALAM ALAROOD[1], ADAMU ABUBAKAR IBRAHIM[2], AND FAISAL S. ALSUBAEI[3], (Member, IEEE)

[1]College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia
[2]Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia
[3]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia

Corresponding author: Ala Abdulsalam Alarood (aasoleman@uj.edu.sa)

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number MoE-IF-UJ-22-4220746-1.

ABSTRACT The DSCP is an integral component within the Internet Protocol (IP) header of a packet, serving the purpose of categorizing and administering network traffic, as well as facilitating the provision of Quality of Service (QoS) on IP networks. In the context of network communication, it is feasible for an adversary to transmit packets with a DSCP value of ''x,'' which represents a high priority. This action aims to prioritize the specified packet over other network traffic packets without triggering any notifications during the transmission session. It is possible to use identical DSCP values for both offensive and defensive purposes. This study therefore proposed a method for generating attack notifications in response to changes in DSCP values by using binary vectors to represent entries that detect attacks and those that do not. The method returns a list of Boolean values, each of which indicates whether or not the corresponding packet was classified as an attack. The study employed an experimental research methodology to generate transmission scenarios in which an attacker would attempt to transmit packets with a malicious DSCP value so that they would be prioritized over other traffic. A function was developed to detect deviation from normal and modification values involving DSCP value operations of normal traffic and generate alert. The finding of the experimental analysis indicates the vector, represents normal traffic because it does not have a DSCP value associated with an attack. The vectors representing spoofed, Assured Forwarding (AF), Class Selector (CS) and Expedited Forwarding (EF) respectively and generate an alert based on their values. This has contributed in detecting when an attacker tries to send packets with modified DSCP value in order to get them prioritized over the other packet on the normal traffic.

INDEX TERMS Assured forwarding, class selector, differentiated services, expedited forwarding, vector space.

I. INTRODUCTION

This paper outlines the process of generating attack alerts when there are changes in the DSCP values. The understanding of DSCP operation is closely linked to the principle of QoS. This principle starts with the establishment of a ''Type of Service'' (TOS) header field in IP networks, a field is responsible for determining the priority of each packet in a network transmission session [1]. At the time, there was a lack of consideration for security attacks on TOS operation. There were no known security attacks or vulnerabilities publicly associated with the TOS on IP networks. The TOS field in the IP header was initially created to assign priority levels to various types of network traffic. TOS is only allocated to an octet that comprised of three least significant bits for the initial field, referred to as ''Precedence,'' which serves the purpose of indicating the significance or priority of the IP Packet. This solves issue of managing unfairness that arises when a network is handling multiple types of traffic with varying requirements [2]. However, TOS has been replaced by the

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

DSCP field in both IPv4 and IPv6 headers [3]. The process of distinguishing and prioritizing different types of network traffic involves instructing network devices on how to recognize and differentiate between them. In order to accomplish this task from the practical point of view, Modular QoS Command Line Interface (MQC) was provided by Cisco [4]. The MQC offers a set of commands that enable administrator to instruct Cisco routers and switches on how to identify various types of network traffic and assign a hierarchical tag to each packet in the traffic. However, it is important to note that the criteria used for distinguishing between different types of traffic can be quite detailed without regards security consequences. For instance, an administrator can specify that a particular type of traffic should be recognized based on its priority and the resources it requires, when it is destined for a specific operation, security function is crucial. Similarly, by implementing priority instructions and security operations, a network administrator can appropriately handle any complicated network traffic easily.

This study dwells on two research problems that could not be easily separated, concerning the Inspection of DSCP values in relation to network performance, and the examination of DSCP values in relation to security attacks. While, the study focus on security attacks, when addressing the issue of network performance, it is important to consider the security operation as well as DSCP in relation to QoS. As DSCP is a 6-bit field in the IP header that is used to classify traffic for QoS purposes, those bits can be manipulates in transmission session [5]. If DSCP values are not inspected from the source to the destination, then traffic may not be treated as intended at same time, the values can be modified [6]. For example, voice traffic that is marked with a high DSCP value may be treated as low priority traffic maliciously if it is not inspected by all routers along the path. This can lead to poor QoS for the traffic, and also lead to performing unintended function. In some cases, it can even lead to dropped packets or other performance problems. The emergence of security vulnerabilities can be attributed to the absence of inspection of DSCP values [7]. A primary issue revolves around the challenge of distinguishing between legitimate and malicious forms of network traffic. The absence of thorough inspection can be exploited by malicious individuals to circumvent security measures through the concealment of their activities within seemingly harmless traffic. The absence of DSCP value inspection can also result in the evasion of detection for malicious traffic, thereby presenting a substantial threat to both the network infrastructure and the preservation of the confidentiality of sensitive data.

This study has established that the examination of the security issue pertaining to the omission of inspection of DSCP values during transmission between the origin and destination holds significant importance within the contemporary context of a globally interconnected and data-centric society. When DSCP value checking is skipped, the network opens itself to many different attacks such as DoS attacks [8]. On another perspective, lack of prioritization can be used by attackers to flood the network with unnecessary packets, reducing performance and possibly disrupting services if the DSCP settings aren't checked. Furthermore, this research also established that an improved performance for certain types of traffic could be possible by DSCP values that can be used to prioritize certain types of traffic, such as voice and video traffic. This can improve the performance of these types of traffic, which is important for applications such as VoIP and video streaming. That is why this ongoing research is deemed highly essential, thus the potential contributions that it offers can be outlined as follows:

- Taking into account the highlighted research problems and motivations. In order to monitor the number of DSCP values present in the packet headers of a transmission session, a Boolean vector is created and associated with these values. The vector is maintained to ensure that the count of DSCP values is accurately recorded. This approach can also be employed to mitigate the identification of specific traffic of interest and to monitor it continuously during its transmission session. By assigning higher priority to specific types of traffic, routers can effectively safeguard these types of traffic from being impacted by abnormal operation.
- A list of Boolean values is created to indicate the classification of packets as attacks. The list includes entries that detect attacks as well as entries that do not detect attacks. The generation of appended DSCP values is a method employed to designate sensitive traffic, thereby enhancing its security against potential attacks. The lack of universal support for DSCP values among routers results in potential inconsistencies in the utilization of DSCP values across a network. Consequently, the act of adding a vector with associated DSCP values will facilitate the monitoring and management of the entire transmission session.
- This study addresses the challenge of configuring DSCP values, which can be complicated due to the existence of numerous values, each carrying a distinct significance. To overcome this difficulty, the study establishes associations between each DSCP value and its corresponding meaning. To safeguard DSCP values from potential tampering by attackers who may modify the IP header of packets, it is possible to establish tag values that can effectively fortify a network against such attacks.

The remaining part of the paper is presented as follows: Section II describe the DSCP values operation in IP networks, while Section III Discusses the research conceptualization and the development of algorithms. Section IV present an experimental analysis and section V discuss the result of the research while section VI present the implication of the research.

II. DSCP VALUES OPERATION IN NETWORK

The DSCP value within the IP header is employed to facilitate QoS and prioritize network traffic. The utilization of DSCP values enables routers and network devices to implement

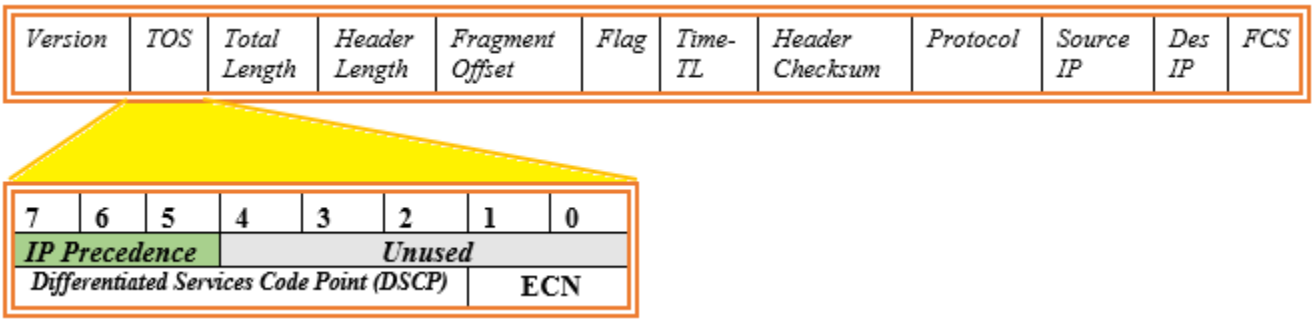

FIGURE 1. The IP packet header protruding TOS.

distinct packet handling strategies [9]. However, the maintenance of consistent link control necessitates the continuous monitoring and management of latency fluctuations in order to guarantee a network performance that is both stable and dependable [10]. These two concepts hold significant importance in contemporary networking as they aim to enhance traffic management and improve user experience throughout the network. Their implementation dwell on routers and other network devices that use the DSCP value to determine how to handle the packet [11]. As an illustration, network administrators may assign greater precedence to packets with elevated DSCP values, or alternatively, they may direct packets with lower DSCP values along less congested routes. The packet is subsequently conveyed to the destination device, where speed is also of paramount significance. There are many previous research studies within DSCP values operation in IP Network, however before elaborating on such studies, there is a need to describe the operation of DSCP Values in IP Network first.

Figure 1 illustrates an IP header packet that aims to depict the emergence trend of DSCP. At the onset DSCP originated from TOS. The ToS data field consists of a total of 8 bits. The priority control (Precedence) is represented by the first three bits. The implementation of precedence control enables expedited routing of datagrams with high urgency by bypassing the router queue [12]. The Precedence field encompasses a range of values, although only a subset of these values are commonly employed in practical applications. Specifically, the value "000" is used to represent IP packets originating from endpoints, while the values "110" or "111" are utilized for controlling IP packets exchanged between routers.

The parameters of TOS weren't sufficiently granular to reliably categorize traffic into different classes [13]. The DSCP was thus established as a new norm [14]. To accommodatedate this standard, an additional three bits were allocated.

The DSCP values are encoded as a 6-bit binary numeral, and they are commonly converted to decimal representation for the purpose of facilitating comprehension. Table 1 present the potential DSCP values, accompanied by their respective binary and decimal representation.

The CS is situated on the IP precedence line (see Table 2), with the distinguishing feature that the last three bits consistently hold a value of zero.

TABLE 1. The DSCP values and their serial class services.

DSCP Binary	DSCP Decimal	Class of Service	Traffic Type
0	0	Best Effort	Default / Standard
1000	8	Expedited Forwarding	Real-time Audio/Video
10000	16	Assured Forwarding	Critical Data
11000	24	Assured Forwarding	Medium Priority Data
100000	32	Assured Forwarding	Low Priority Data
101000	40	Class Selector	Reserved
110000	48	Class Selector	Reserved
111000	56	Class Selector	Reserved

EF is a distinct mechanism utilized for prioritizing EF traffic. It is consistently represented in binary as 101110, equivalent to the decimal value of 46. A device lacking the capability to distinguish between CS5 and EF, or one that solely relies on IP precedence, would face limitations in accurately discerning between the two. This would generally be considered undesirable, as EF is commonly associated with voice traffic and is typically assigned higher priority in the queue. Over-loading the priority queue with numerous items would result in a large first-in, first-out (FIFO) queue, which is not ideal. Therefore, it is crucial for this data to be accurately identified and differentiated.

AF is a QoS mechanism that ensures reliable and predictable packet delivery in computer networks. The initial three bits are utilized to assign the IP precedence value, as observed in the AF11 notation. The first number in AF11 denotes the first three bits, indicating an IP precedence value of one for these bits. However, the query remains regarding the interpretation of the second set of three bits. The final three bits are utilized in various applications, such as weighted random early detection, to determine default settings regarding drop preference. It is observed that a higher numerical value corresponds to a greater drop preference in the majority of weighted random early detection default mechanisms. If the rating is set at three, it inherently

possesses a greater preference for dropping compared to a rating of one. It is possible to modify the default set-tings, although this would involve a separate process. In the context of AF values, it is important to note that the second number of an AF value can only be one, two, or three. However, it is observed that only the first two bits of the last three bits are utilized. It is worth mentioning that the first value of an AF value pertains to the three most significant bits of the byte, while the second value pertains to the first two bits of the last three bits of the differ code point field. It is worth noting that all bits are accessible, but if there is a need to identify something that is not recognized by an AF value, it can be explicitly referred to by its binary value, such as 35. In the context of Cisco networking, it is not appropriate to refer to AF35; instead, the correct terminology is DSCP35. This distinction is particularly relevant when utilizing tools such as AUTO QoS, which heavily rely on classify-ing and marking based on these values. Therefore, it is advantageous to possess knowledge regarding the interpretation and significance of these values. As previously mentioned, DSCP35 falls between AF41 and AF42, and it does indeed exist. Consequently, it is possible to employ DSCP35 in conjunction with these elements, albeit without the convenience of utilizing an AF shortcut for recognition purposes.

TABLE 2. The DSCP values associated with ip precedence.

DSCP Name	Binary Value	Decimal	IP Precedence
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4
AF43	100 110	38	4
CS5	101 000	40	5
EF	101 110	46	5
CS6	110 000	48	6
CS7	111 000	56	7

When examining the AF values in a map, it is observed that the first number can only assume the values of one, two, three, or four. It is noteworthy that AF1 corresponds to IP precedence one, AF2 corresponds to IP precedence two, and AF3 corresponds to IP precedence three. Similarly, AF4 corresponds to IP precedence four. When considering the second number pertaining to the first two of the last three values, it is important to note that only the digits one, two, or three are permissible. The digit AF10 is not included in this set. Specifically, the second value can only be represented by the digits zero, one, or two, which correspond to the values one, two, and three, respectively. The initial digit in AF11 denotes that the first three bits correspond to IP precedence 1001, while the first two bits of the second set of three bits also resemble a value of one, indicating a lower drop preference. Conversely, if a value of AF13 is assigned, which passes through a system with weighted random early detection enabled, a higher drop preference is established by de-fault. Therefore, the first three bits align with IP precedence, while the last three bits pertain to drop preference, with only the first two bits of the latter being utilized. When considering the conversion of an AF value to decimal, it can be observed that the resulting decimal value will consistently be an even number, as the AF value never marks the one high.

III. RELATED WORK

Numerous prior research studies have been conducted to examine the operational aspects of DSCP values in IP networks. Nevertheless, it is imperative to recognize the dearth of comprehensive studies concerning the security ramifications associated with DSCP values within IP networks. This limitation hinders our comprehension of their operational dynamics in the context of network security. Among the important research works on DSCP is the study of Maswood et al. [15]. According to the study conducted by Maswood et al. [15], one of the primary obstacles faced by network providers is the development of a cost effective network that can accommodate varying QoS requirements for different types of traffic. The research established that while traditional differentiated services (DiffServ) network architecture designed for IP networks, wherein differentiation is achieved by modifying the code points in IP packet headers, lots of issue comes in their operation. The research posits that by exerting greater control over the management and organization of data flows, specifically through the implementation of differentiated QoS traffic classes, network optimization can be achieved. This study employs a software-defined network (SDN) environment to deliver differentiated QoS traffic with varying latency bounds.

Solihah et al. [16] demonstrated the significance of prioritizing QoS capability, specifically with regards to VLAN-based parameters and DSCP mapping, in order to make informed decisions for effective governance in the development of the 10-Gigabit-Capable Symmetric Passive Optical Network (XGS-PON) standardization. Similarly, Kitsuwan and Oki [17] examines a method for dividing network traffic within a software-defined network (SDN) through the utilization of a meter table. The rationale behind this approach is to leverage the DSCP number present in the packet header to classify network traffic and subsequently deliver QoS. The study utilizes the traffic splitting methodology, employing a DSCP number as the parameter for splitting. When a packet

surpasses a predetermined traffic rate, the DSCP value of the packet is modified. Packets with varying DSCP values are transmitted to neighboring switches via distinct output ports.

Cansever and Islam [18] have identified that the issue of precedence and preemption presents various challenges. One of the primary challenges is to maintain a simple overall architecture that avoids excessive complexity in network management and operations. Additionally, it is crucial to ensure that the end-to-end requirements for precedence and preemption are met across multiple autonomous domains. Hence, the research presented a methodology for utilizing the DSCPs to signify the Precedence and Preemption level, as well as the class of service linked to every packet. The architecture that relies solely on the DSCP value for Precedence and Preemption may result in suboptimal utilization of network resources during periods of network congestion. The study conducted by Daoud and Qu [19] examined the various factors that can potentially lead to a decline in the quality of voice over Internet Protocol (VoIP) phone service. Additionally, the researchers analyzed and evaluated the traffic prioritization of this service based on the DSCP markings. This study presents several configurations of DSCP markings that have been shown to significantly enhance the quality of VoIP conversations.

Rodday et al. [20] analysis explores the correlation between the values of DSCPs and the ports utilized on the transport layer. The findings of the study indicate that the majority of traffic utilizing DSCP code points is limited to default values, rather than employing values specifically intended for packet prioritization. Kniazieva and Kalchenko [21] propose an algorithmic approach to model the policy for packet handling. The methodology entails modifying the service class by altering the DSCP within the packet header, while adhering to the permissible service classes. Based on the computed results, the QoS exhibits an increase of over 3% when altering merely two out of the total 22 quality indicators. Uchida and Kimura [22] propose a novel adaptive link rate switching approach that utilizes traffic splitting through OpenFlow meter tables. The meter tables are utilized for the measurement of traffic speeds and have the capability to modify the DSCP field within IP headers in the event that the speeds surpass a predetermined threshold, such as the link bandwidth. The traffic splitting method involves the allocation of distinct routes for each DSCP value based on the corresponding traffic volume. This approach effectively divides a traffic flow into multiple routes. I

In their study, Garbin et al. [23] demonstrated that IP-based networks incorporate mechanisms to prioritize certain services, such as voice and video, by utilizing DSCPs in packet headers and Per Hop Behaviors in routers. The researchers further examined the advantages of applying additional DSCP markings to voice and video packets, as well as various router configurations. The findings indicate that the inclusion of certain elements is highly beneficial in maintaining the effectiveness of disaster response management, even in situations where there is a decline in the quality of ordinary voice and video performance due to unusual fluctuations in demand. Similarly, Cahyadi [24] conducted a study which determined that real-time applications, such as videoconferencing, are considered the highest priority service for ensuring QoS in a network. The study employs a weighted fair queuing algorithm that is based on differentiated service code point with random early detection in order to optimize the QoS performance metrics. The results indicate that the utilization of the weighted fair queuing algorithm, which is based on the differentiated service code point method, offers the most favorable outcomes, particularly in terms of the quantity of dropped packets and the ratio of sent and received packets over time.

This paper highlights a research gap in the field of DSCP security, specifically the lack of research papers addressing the security implications of DSCP values. This gap represents a missed opportunity to enhance knowledge and enhance network security practices. However, the research conducted by Li et al. [25] and Bianchi et al. [26] has emphasized the need to examine the security implications related to DSCP values. Li et al. [25] employed a 0-order TSK fuzzy model that incorporated a sparse rule base. DSCP values are generated dynamically by the TSK fuzzy model and are continuously updated in real-time. The other approach of Bianchi et al. [26] demonstrated how, the preservation of QoS is achieved through the process of assigning a distinct DSCP value to duplicated packets, prior to their transmission along the QoS pathway. In order to further from the research work of Bianchi et al. [26], this current study proposed generating attacks notification on DSCP value modifications.

In order to better reflect the development context and latest research developments, the following reviewed research was used to analyze the weaknesses of existing solutions or systems to highlight the research motivation of this manuscript. Malikovich et al. [27] introduced a DSCP Traffic Filtering Method as a preventive measure against attacks. The authors established that the implementation of DSCP-based packet filtering can be utilized as a network filter, offering faster performance compared to alternative packet filtering programs. Regrettably, the Packet filtering function lacks the capability to tag packets that are either permitted or denied passage via the filtering device. Their solution utilizes the IP address translation function without considering reoccurrence. In their study, Yaseen et al. [28] put out the suggestion of employing DSCP for the purpose of managing health emergency traffic. The proposed methodology is based on the utilization of certain header bits extracted from the traffic class field of a packet through machine learning techniques. This enables the prioritization of traffic flows based on their respective precedence levels, which is achieved by controlling the DSCP bits in accordance with the policies set by the network administrator. Although the research includes information about the transmission session speed attribute, it does not demonstrate the effectiveness of identifying any updated DSCP values. This implies that the research fails to acknowledge the possibilities for manipulating DSCP values.

In their study, Kozuka and Okabe [29] identified the necessity of incorporating path selection in transport protocols designed for mobile devices, taking into account policy considerations for individual processes and implementing a path grouping mechanism. DSCP support is utilized to enable the allocation of audio connections and video connections, as well as screen sharing, to distinct channels based on the specific attributes of each path. This facilitates the efficient handling of typical real-time applications like Zoom and WebEX. Regrettably, the study does not provide emphasis on the occurrence of events whereby the DSCP values are altered. In those circumstances, the proposed approach would not yield favorable outcomes. In their study, Shreedhar et al. [30] introduced a technique for prioritizing DSCP at the IP layer. They demonstrated the significant effectiveness of this approach in segregating status update flows from the influence of high throughput flows within networks, particularly in scenarios where WiFi access contention is absent and all flows originate from a single WiFi client. Regrettably, the study fails to address the occurrence of DSCP value modifications. In those circumstances, the chosen strategy would not yield favorable outcomes.

The policy for traffic management, which reflects mission objectives through DSCP labeling, was devised by Refaei et al. [31]. This is the reason why an enforcement engine was employed; nevertheless, the technique does not account for the potential alteration of DSCP events. Sathyanarayana et al. [32] implemented regular examinations of queue conditions using appropriate DSCP IDs in order to consistently maintain QoS. This holds significance as it provides a comparative scale to the resource-limited scenario. Regrettably, the DSCP function lacks the capability to facilitate tracking and monitoring. Their strategy fails to take into account the potential impact of DSCP alteration on reoccurrence. In their study, Yin et al. [33] introduced a power service flow port and QoS delay indicators as the fundamental criteria for differentiation. They then utilized IP DSCP to address the communication obstacles associated with power-intensive data transmission and diverse service kinds. Regrettably, the modification of the DSCP value is a significant challenge in the implementation of the power provisioning strategy, as any alteration to this value introduces associated issues within the approach.

Zhang and Kimura [34] introduced a traffic splitting technique utilizing bypass mechanisms that leverage the DSCP field. This approach ensures that the link along the shortest path maintains a modest speed when the traffic flow reaches a ''intermediate'' rate. The findings indicate that there is a decrease in power consumption by 5.30%. In the present scenario, when there exists a departure from the standard DSCP values, an issue arises pertaining to power consumption. The study does not offer a means of ensuring the alteration of DSCP values. In their study, Solihah et al. [16] introduced a QoS capability that utilizes VLAN-based characteristics and DSCP mapping to prioritize traffic. This approach is intended to enhance the reliability and efficiency of ubiquitous networks, specifically in safeguarding the Indonesian traffic network. The study's findings indicate that although transmission is optimal, there is no consideration given to the alteration of DSCP values. Mazhar et al. [5] have demonstrated that the Next-Generation Wireless Sensor Networks will rely on DSCP in order to effectively address the varied demands of applications and provide dependable communication. The research fails to provide explicit details regarding the implementation of DSCP values, despite their critical importance.

IV. RESEARCH METHODOLOGY

This study is primarily focused on the development of algorithms and the experimental evaluation of generating attack notifications based on modifications to the DSCP values.

A. CONCEPTUALIZATION AND ALGORITHM DEVELOPMENT

The conceptual framework of this study is presented in Figure 2. Assign DSCP values'' in Figure 2 is the value that is assigned to indicate the priority level of the packet that would be transmitted when its transmission session is initiated. DSCP value inspection at the firewall indicate the region where each packet is inspected to see if the value assigned at the source is the same value after leaving the router or not.

The justification of adopting this setting lie with the following:

- It enables the monitoring of source packets as they traverse from one network to another until they reach their intended destination.
- The purpose of this mechanism is to maintain the assigned DSCP value at the source without any alterations over the entire duration of the transmission session.
- The rationale for adopting this methodology stems from the lack of clearly defined inspection status inside the DiffServ framework [26].
- The DiffServ protocol does not include techniques for node inspection to ascertain the existence of assign DSCP value on an output link in the configuration of an IP network [26].
- The underlying justification necessitates the evaluation of every packet during a dynamically joined transmission session within a DiffServ network.
- Finally, the proposed approach is necessary due to the lack of control capabilities in DiffServ networks that may evaluate the availability of resources along recently constructed channels.
- Through the analysis of DSCP values with the process of tagging, DiffServ networks would have the capability to facilitate control functions that assess the availability of resources along recently constructed routes.

1) DEVELOPMENT OF THE INSPECTION ALGORITHM

The fundamental method for inspecting DSCP values involves analyzing the DSCP field within IP packet headers

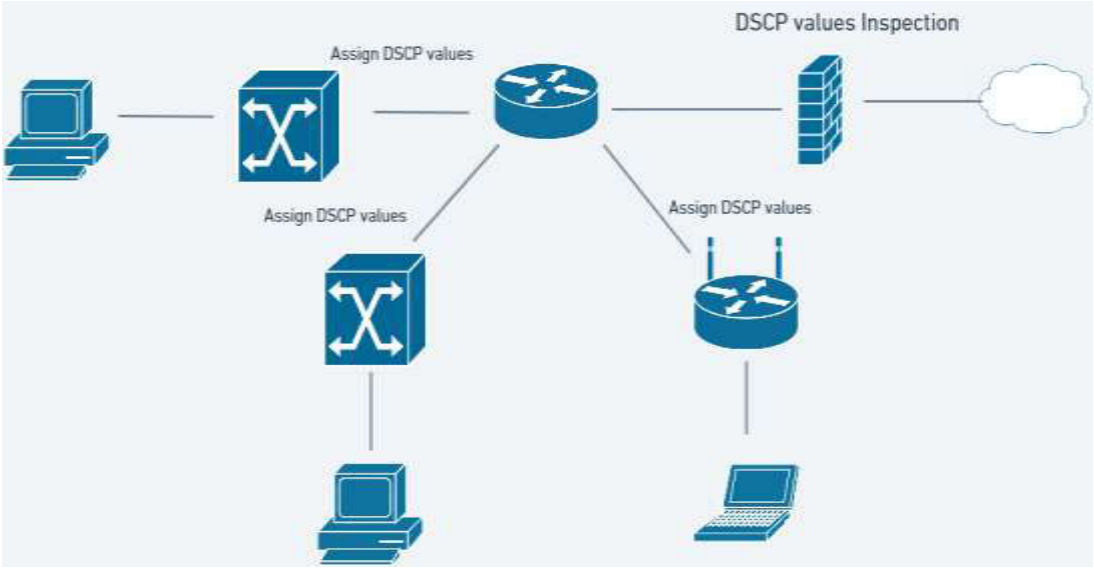

FIGURE 2. The proposed conceptual framework.

and implementing alert or notification actions according to the assigned DSCP values. The transmission session commences with the operation of transmitting a packet from the source/origin to the destination.

The task of algorithm 1 lie with collecting network packets or data flows that encompass DSCP values. The acquisition of these packets from network traffic is accomplished by the utilization of packet capture. The gathered packets are preprocessed in order to extract and isolate the DSCP values. The process relied on the analysis of packet headers in order to identify the DSCP field. Algorithm 1 has been proposed to display the general concept as follow:

- Retrieve/extract the IP packet header from incoming packet in order to assign it a tag (vector) indicating the value of DSCP that the source network assigned to that specific packet. This implies that the DSCP value extracted from the DSCP field has been stored in a designated data structure.
- The algorithm subsequently assigns the DSCP value to the corresponding service classes. This can be interpreted as a matrix-vector representation that maps the associated DSCP value to a particular service class or traffic category. The mapping can be predetermined according to the policies of the organization or the requirements of QoS, whether it is assigned as a high priority, low priority, or no priority.
- The packet proceeds to the subsequent node, which could potentially serve as the destination for a transit node. At this particular point in the algorithm, the execution of a specific action is determined by the service class that is linked to the corresponding value. In particular, it reevaluates the DSCP value and compares it with the DSCP values assigned to the source.
- Prior to transmitting the packet, the algorithm generates two Boolean vectors to indicate whether the DSCP value has remained unchanged or if it has been altered from its original values assigned at the source.
- If the notification does not indicate any modification, the algorithm will proceed to forward the packet to the next hop based on the network routing technique.
- If the notification signifies a modification, the algorithm will proceed to discard the packet and subsequently repeat the aforementioned steps for each subsequent incoming packet.

Algorithm 1 Inspecting DSCP Values

```
    Require: IP Packet header
    Ensure: DSCP value
1   RetrieveDSCP_Values(ip_packet):
2   Identify DSCP field within the DS
3   For each ip_packet
4       if ip_packet.contains("DS" == dscp_values)
5       dscp_values.add(dscp_value)
6                   dscp_vector.append(dscp_value)
7                   Label/tag (dscp_value ∪ dscp_vector)
8                   if node_value in visited_nodes
9                   visited_nodes.add(node_value)
10                  for dscp_value ∪ dscp_vector
11                  if node_value == dscp_value ∪
                      dscp_vector
12                      No modification == proceed to next
                          hop
13                  else
14                      Drop the packet & start step 1
15                  end
16f             end
17      end
18  end
```

While it is essential to recognize that the algorithm and its specific implementation particulars to different network scenarios, such as the mapping vectors and the values of

DSCP across different service, may vary depending on factors such as the network infrastructure, QoS policies, and also administrative requirements [35]. This is one of the most important things to keep in mind about the algorithm. The method serves as a thorough framework for analyzing and keeping track of DSCP values and carrying out suitable actions in accordance with the service of the network that has been determined.

2) INSPECTION PATH AND NOTIFICATION OF ATTACKS

Algorithm 2 primary task involves the extraction of DSCP values from individual packets and compared to preset criteria and policies that operationally defined the set of the values outlined in table 2. The task at hand involves the identification of packets that fail to meet the established criteria and choose to log or record data pertaining to non-conforming packets for the purpose of conducting audits or facilitating subsequent analysis. Thereafter determine the appropriate courses of action for packets that do not correspond to specified standards, including options such as dropping, marking, logging, or alerting.

The primary approach for inspecting the path and detecting attacks related to DSCP values is through a systematic analysis of the DSCP values assigned to packets and the accompanying vector. This analysis aims to identify any deviations from the anticipated norms. It is crucial to acknowledge that the prioritization of a packet is not solely determined by the DSCP value. The prioritization of packets is influenced by both network congestion and the policies implemented by the network administrator. However, the process of inspecting DSCP values commonly entails the assignment of DSCP values to a particular appended vector and the subsequent creation of a corresponding vector to indicate if there is modification from starting of transmission to the end. A simplified mapping function in which it associate DSCP values with vectors through the utilization of a piecewise Boolean function notifies if there is modification or not.

The process of mapping would involve the identification and preservation of each individual value at its original source. For example, when a DSCP value of 8 is considered, it will be associated with a vector of 8, resulting in the output vi (8,8). In this context, the coordinates of the point are given as (8,8). The given binary bitmask represents the retention of the 6-bit DSCP field vi (x,y), where x denotes the DSCP value and y denotes the corresponding mapped vector. The subsequent process involves the conversion of a vector into a mapping, which can be accomplished through the utilization of a mapping function. In the context of vector, A, represented as vi (8,8), its identification will trigger an alert or notification to signify its unaltered state. On the other hand, in the event that vector B, denoted as vi (8,7), is encountered, it will elicit an alert or notification to indicate that it has undergone modification. The function can be implemented using a matrix lookup approach, where each DSCP value is associated with a corresponding vector in the matrix.

Algorithm 2 makes use of a comparison between the DSCP value of each packet and its matching vector that is assigned at its source in order to determine whether or not a packet should be deemed an attack. This allows the algorithm to determine whether or not a packet should be considered an attack. When the DSCP value of a packet is different from the value that was initially assigned to it at its source, which results in the tagging or appending of the packet with an incongruous vector, this is considered to be evidence of an attack and is considered to be a successful attack. In the event that the DSCP value is the same as the value that was assigned to it when it was first created, then it is not considered to constitute an act of attack. In a nutshell, the technique necessitates the inspection of the DSCP values contained inside a predetermined quantity of data packets. When the DSCP value of a packet deviates from the value that was initially assigned to it at its source, that packet is classified as belonging to ''Set A'' because of its ability to recognize and prevent potential attacks. It is later classified as a ''Vector'' because to its inability to detect assaults when the DSCP value matches the value that was assigned to it at its source.

Algorithm 2 Inspection Path and Notification

Require: DSCPvalue_actual == DSCPvalue_expected:
Ensure: Append_vector to DSCPvalue_actual

```
Vector A: Entries that detect attacks
Vector B: Entries that do not detect attacks
For each packet in a transmission session
    if ip_packet.contains("DSCPvalue_actual)
    Alert=if(DSCPvalue_expecte≠DSCPvalue_actual)
        A = {i | real_dscp[i] = x and inspect_dscp[i] = x}
        B = {i | i not in A}
        For each packet i from 1 to n:
        If DSCP_source(i) ≠ Expected_DSCP_value:
        Mark the packet i as suspicious.
        For each packet i from 1 to n:
        If DSCP_dest(i)≠DSCP_source(i) = attack
        Vector A: A = [a1, a2, ..., an]
            ai = 1 if real_dscp[i] = x & inspect_dscp[i] = x
            ai = 0 otherwise
        Else
            Aler()
        End
        Vector B: B = [b1, b2, ..., bn]
            bi = 1 if real_dscp[i]≠y or ispect_dscp[i] ≠ y
            bi = 0 otherwise
        Else
            Alert()
        End
        DSCPvalue_expect & DSCPvalue_actua=check
        packet.contains DSCPvalue_actual ()
    All entries detected & logged
    End
End
```

If the first packet in the transmission session has the ''actual DSCP value,'' and this condition is satisfied, then the recorded value of that packet, as determined by the algorithm, should remain consistent throughout the transmission session, regardless of its location. This applies even if the packet is received later in the transmission session. In this particular instance, the technique is intended to add a vector to the DSCP value that is already in use. After that, the appended vector is saved as an entry in a collection that monitors for attacks; we'll refer to this collection as Vector A. On the other hand, if the values remain the same, the algorithm will record the added vector in a collection that does not detect assaults, and this collection will be designated as Vector B. The steps involved in this method are described in the first three lines of Algorithm 2. The process gets underway with the reception of each packet during the course of the transmission session, more especially from line 4 to line 27 of algorithm 2. In each iteration of the method, the ''n'' variable, which stands for the total number of packets sent from the source, is taken into consideration. Following that, the inspection procedure looks at each entry that was made throughout the transmission session, just like it was explained earlier

B. EXPERIMENTAL ANALYSIS

This study incorporates an experimental analysis consisting of two distinct stages. The initial stage involves the exploration of a commonly encountered experimental scenario utilizing a widely used tool capable of capturing DSCP values. Subsequently, these captured values are subjected to thorough analysis. The second step entails constructing scripts to perform tests on a transmission. This process involves manipulating network traffic by implementing policies that modify regular packets and intermix them with packets from typical transmission sessions. Subsequently, these packets are captured and subjected to examination in order to determine their ability to identify and report any instances of packet alteration. The study examined the effects of DSCP values in four distinct scenarios.

1) PRELIMINARIES

One of the most straightforward methods for capturing DSCP values is by using Wireshark. This software allows for the display and interpretation of service class information, providing an analysis of the status of each transmission between the source and destination. Figure 3 present a transmission session for which a Wireshark was used to capture the transmission session information providing a useful information for everything for which the DSCP values was also captured. Wireshark offers a comprehensive representation of service classes, facilitating the analysis of their status and presenting the outcomes pertaining to a particular transmission between the source and destination.

The designated field identifier within Wireshark for the DSCP value is denoted as ''ip.dsfield.dscp'' [36]. Figure 3 depicts the transmission sessions monitored by Wireshark, wherein each session is associated with a singular DSCP value that represents its content. The initial transmission session, denoted as DSCP 0 - ''Default,'' is depicted in Figure 3. This session illustrates a packet carrying a DSCP value of 0. The DSCP value signifies the assignment of the packet to the service class denoted as ''Default.'' In practical terms, a DSCP value of 0 indicates that this transmission does not possess any form of prioritization over other transmissions during the designated time frame. The treatment of this traffic is regarded as conventional traffic, lacking any explicit assurances of QoS.

The subsequent transmission session, designated as DSCP 10 and referred to as ''AF'' or AF11, is the focus of this discussion. The DSCP value of 10 is assigned to the second packet depicted in Figure 3. The DSCP value denotes its categorization as a service class referred to as ''AF'' (AF11). The service class known as ''AF'' is commonly classified inside the low drop precedence levels. To clarify, packets assigned with this particular DSCP value are afforded a certain level of confidence regarding its forwarding, prioritization, and reliability. However, it is important to note that this level of priority is not the highest.

The prioritization of service classes is a significant aspect in contemporary IP networks, wherein service classes such as ''AF'' are employed to offer distinct levels of forwarding assurances and prioritize the treatment of packets linked to different traffic classes. The prioritizing mechanism implemented guarantees that certain traffic categories, such as AF11 in this particular scenario, are given preferential treatment in terms of forwarding and reliability as compared to ''Default'' traffic.

The binary representation of the DSCP values is depicted in Figure 4 indicating a representation of decimal ''10'' which represent the DSCP value for ''AF''. The DSCP value is commonly represented as a 6-bit field included within the IP header [37]. The binary format is utilized to categorize packets into distinct service classes, representing a total of six bits. For the current the position of decimal 2 and 8 in the binary format of the 6 bits are 1 each respectively therefore the addition of 8 and 2 yielded 10'' The inclusion of the binary format for the DSCP values in Figure 4 serves the goal of facilitating analysis. This functionality enables researchers and network managers to analyze the discrete bits comprising the DSCP values, thereby facilitating the identification of the service class associated with each packet. The aforementioned analysis is commonly conducted subsequent to the termination of the transmission session.

The statistics and filtering capabilities of Wireshark can be utilized to analyze specific DSCP values or service classes [38]. This aids network administrators in comprehending the manner in which the network manages various types of traffic according to their prioritization. Regrettably, it is incapable of surpassing its current functionality, which is limited to determining whether the received DSCP values have been altered and providing only the captured information without any additional capabilities. Therefore, this study took into consideration the aforementioned factors

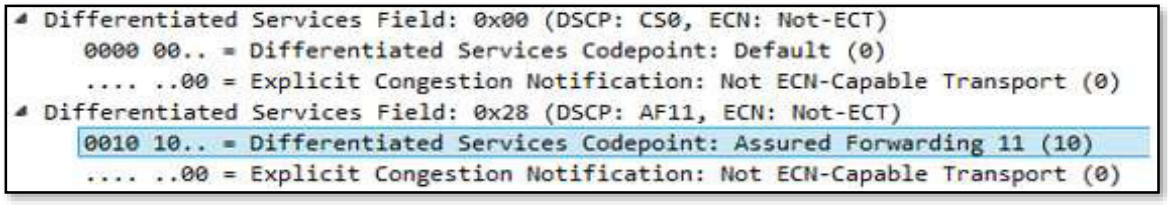

FIGURE 3. Default DSCP and AF DSCP status from a capture transmission.

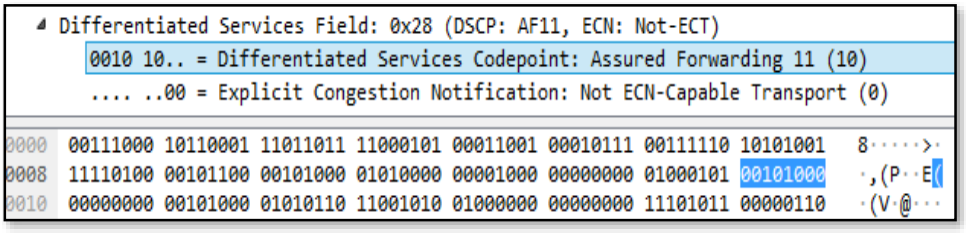

FIGURE 4. AF DSCP values in binary.

and designed a transmission session with the purpose of not only capturing and displaying the packet's state during transmission, but also examining the duration of time each packet spends in transmission based on its DSCP values. At the preliminary stage, it is also possible to transfer the data to the database for further details analysis. Figure 5 illustrates that during the initial phase of the investigation, the data obtained during the transmission session is directed towards a database. This stage entails the transfer of packet-related information, such as DSCP values and transmission duration, to a database for subsequent analysis. Figure 5 depicts the process of redirecting transmission session data, encompassing DSCP values and transmission length, to a database. The process of integrating this data into a database is a crucial component of the study, as it facilitates a more comprehensive and in-depth examination of packet behavior and network performance, specifically in relation to DiffServ and QoS.

This study proposes a close look of the various methods by which transmission session data can be captured and analyzed. Specifically, the study focuses on the relationship between DSCP values, their corresponding service classes, and the accompanying vectors throughout the entire transmission session. The objective here is to provide evidence that the DSCP values can be subject to alteration and customization either legitimately or illegitimately.

2) EXPERIMENTAL SETUP

The purpose of the experiment setup is to evaluate four different situations in the following way:

- Scenario that evaluates Traffic based on Service Class
- Scenario that evaluates a full Inspection of DSCP real value at the source and the value expected in the immediate node which returns a notification
- Scenario that inspects the service class's DSCP value and notifies
- Scenario that evaluates DSCP value linked with Vector notification after full Inspection from Source to Destination.

src_port	dst_port	src_ip	dst_ip	version_ip	ihl_ip	tos_ip ▲ 1
47632	443	10.111.213.47	142.250.199.10	4	5	0
47632	443	10.111.213.47	142.250.199.10	4	5	0
47632	443	10.111.213.47	142.250.199.10	4	5	0
443	37220	35.211.148.231	192.168.100.110	4	5	104
443	37220	35.211.148.231	192.168.100.110	4	5	104
45952	8022	192.168.100.110	38.68.135.72	4	5	8
45952	8022	192.168.100.110	38.68.135.72	4	5	8

FIGURE 5. Transmission session data that are redirected to database.

The implementation of the proposed algorithm involves the utilization of Python libraries for the purpose of sniffing and analyzing network packets. The essential libraries for this particular task include the ''scapy'' library. Python offers a robust packet manipulation library, alongside ''dpkt,'' which serves as an additional packet handling library. A research project was conducted to develop Python scripts for the purpose of sniffing and generating network traffic. The packet sniffing functionality was facilitated by the utilization of Scapy. Additionally, this research endeavor successfully achieved the creation of custom packets with modified DSCP values, thereby enabling the generation of traffic with specific characteristics.

Three different networks were utilized for the analysis. It was ensured that each of the three networks included both a sender and a receiver. The Scapy tool was employed to create customized packets containing specific DSCP values, which were subsequently transmitted from one network to another. The packets that are received will be captured and subjected to analysis.

Subsequently, the transmission was initiated with the purpose of simulating the attack through the modification of the DSCP values within the packets. The DSCP values exhibit random variation within each packet prior to their transmission. The objective is to induce an anomaly or unauthorized behavior within the network. Scapy was utilized to observe the traffic on individual network interfaces and record packet parameters pertaining to DSCP values. The filter was established to capture packets that possess particular DSCP values.

The Python scripts were capable of analyzing the captured packets and detecting any altered DSCP values. When the system identifies such alterations, it should generate notifications regarding potential attacks. The notification mechanism involves the printing of a message to the generated vector, thereby triggering an alert in a monitoring system.

V. RESULT AND DISCUSSIONS

The execution of the experimental tasks, which entailed the manipulation of network traffic, was carried out in a responsible manner within a controlled laboratory setting. Efforts were made to ensure that the activity in question does not encompass any form of unauthorized network manipulation, which is deemed both illegal and unethical. Numerous Python scripts were developed with the purpose of analyzing captured packets and assessing their ability to detect and notify the presence of any captured packet. In light of this, the initial examination pertains to comprehending the ''Impact of DSCP values.''

The utilization of DSCP values is widely recognized as a means to signify the level of priority assigned to a particular data packet, which can be categorized as high, medium, low, or no priority. These are classified as the ''service class''. Therefore, during transmission, packets are assigned DSCP values based on their priority. These values range from 0 to 30 in order of priority level, from 0 default or no priority to 30 high priorities and are categorized as follows: Best Effort (0-0), Class 1 (1-10), Class 2 (11-20), and Unknown (21-30). The initial values were defined and it was established that each of these values should remain constant, while others are subject to modification. Upon executing the script, the resulting output is capable of displaying the packet categories, as depicted in Figure 6. The analysis of the captured transmission session reveals that there is a significant abundance of packets with high priority in the distribution. The packets with low priority are situated at the lowest level within the transmission session. The packet lacking priority or default priority appears to have a higher volume than the packet with low priority during the transmission session. This indicates that the random allocation of the DSCP values was effective.

The preceding script provides an analysis of the DSCP values linked to 50 transmission sessions, as depicted in Figure 7. The initial DSCP value is recorded and appended to its vector at the source of transmission in each packet. After traversing to the next node, the record is appended to the vector, with the expectation that the value at the source will be the same. After conducting the comparison, it is necessary to generate a notification that indicates the outcome of the DSCP value comparison, specifically whether the values are identical or not. A modification signifies an act of aggression.

The script successfully captured a diverse range of DSCP values, encompassing both those within the expected range and those outside of it. This allowed for the generation of a comprehensive and realistic set of DSCP values. The script successfully identified and alerted about attacks that specifically targeted the DSCP values of packets. This finding is specific exclusively to the efficacy of the ''Recording and Appending DSCP Values'' technique. The scientific rationale underlying this discovery posits that the DSCP value of every packet is documented and added to a vector, which is a data structure, at the point of origin of transmission. This implies that the initial DSCP value remains intact and is recorded for every individual packet.

In the given context, the identification of an attack occurs when the examined DSCP value is classified as ''Unknown,'' signifying its lack of conformity with any established vector. Several instances of attacks targeting the DSCP values have been detected, including packets 13, 15, 16, 35, and 49. The script is designed to produce an alert in the event that it detects such attacks, thereby indicating the presence of potential malicious activity or a violation of established policies. It should be noted that the mapping of DSCP values to service classes and the thresholds for detecting attacks may vary in real-world scenarios, depending on the QoS policies and requirements of the network.

The subsequent script outlines the service class that is to be associated with EF, AF, and CS as the conventional method of specifying the priority level. Therefore, a comprehensive script has been developed to identify attacks that specifically target EF, AF, or CS values. The detection of an attack can be facilitated by an inspection mechanism that identifies discrepancies between the inspected DSCP value and the expected

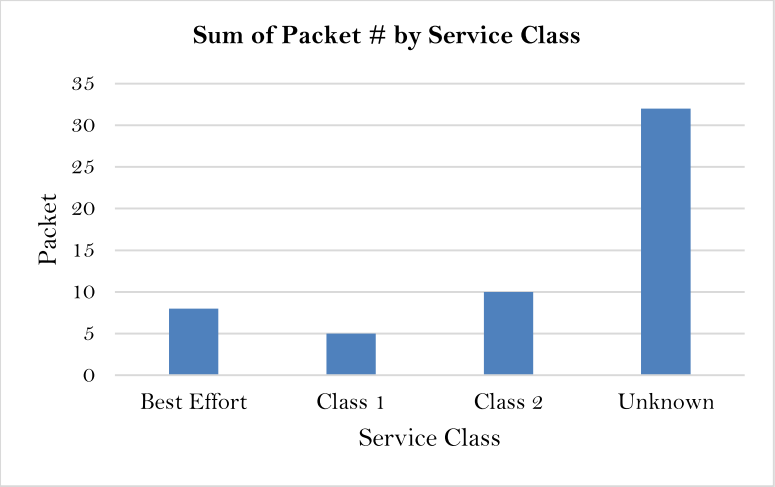

FIGURE 6. The first analyzed captured traffic based on service class.

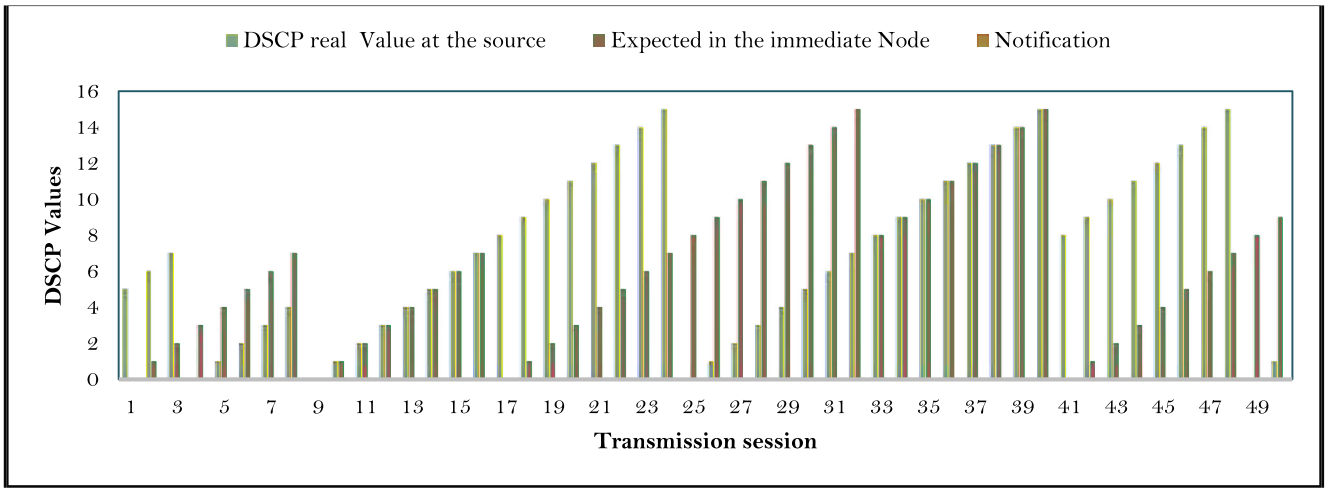

FIGURE 7. The notification generated after a full inspection.

service class. Such discrepancies may indicate a potential effort to manipulate or improperly prioritize network traffic. Table 3 displays a collection of specific vectors that were captured in relation to packets that triggered an attack notification. The table includes the corresponding service types, namely EF, AF, or CS, as well as the associated DSCP values. The entries that identify attacks directed towards EF, AF, or CS values, as well as the entries that do not detect any attacks, are disclosed. The entries that successfully identify attacks are denoted by the label ''Yes'' in the ''Notification'' column, whereas the entries that fail to detect attacks are indicated by the label ''No''. The table presents a comprehensive differentiation between the packets that exhibited signs of attacks directed at EF, AF, or CS values, and the packets that did not manifest any indications of such attacks during the inspection procedure.

The script that follows applies to the entries that successfully identify attacks, as well as those that do not successfully identify attacks when utilizing vector space notation. The binary vector A is depicted in Figure 8. A value of 1 indicates that an attack has been detected for the associated packet, whereas a value of 0 indicates that there has not been an attack detected. The binary representation of the vector that is signified by the notation ''No Attack Detected'' is the vector B. In this representation, an attack has not been detected for the corresponding packet if the value is 1, and it has been detected if the value is 0, and this is indicated by the presence of an attack if the value is 0.

Moving on to the next script is a crucial part of the experiment since it is in this script that the entries that detect attacks and those that don't detect attacks after being examined are determined. These entries are based on four different vectors, each of which represents a different kind of traffic. Those entries that don't detect attacks after being examined don't show up in the results. An unchanged packet is indicated by the initial vector, which is written as (1, 0, 0), and this indicates that there have been no changes made to the DSCP values. The second vector, which is represented by the

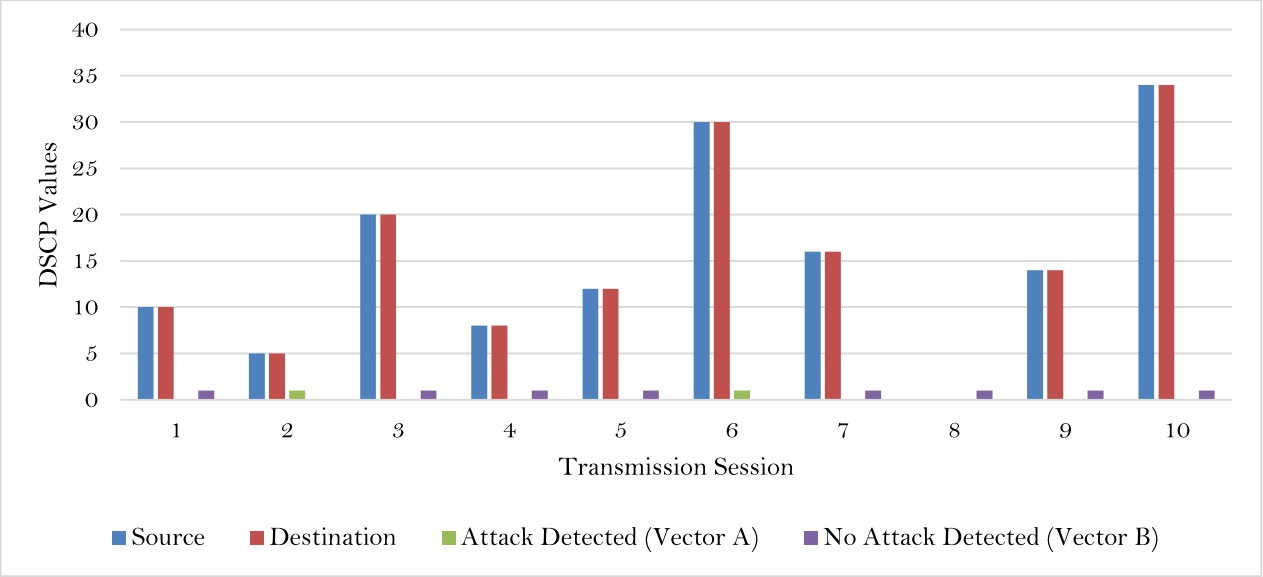

FIGURE 8. The vector notification after a full inspection from source to the destination.

TABLE 3. The service class associated to notification.

ID	Source	Next hop	Service Class	Notification
1	10 (AF21)	10 (AF21)	AF21	No
2	5 (EF)	5 (EF)	EF	Yes
7	16 (AF31)	16 (AF31)	AF31	No
8	0 (BE)	0 (BE)	BE (Best Effort)	No
14	46 (AF43)	46 (AF43)	AF43	Yes
21	5 (EF)	5 (EF)	EF	Yes
22	8 (CS1)	8 (CS1)	CS1	Yes
32	36 (AF42)	36 (AF42)	AF42	No
33	5 (EF)	5 (EF)	EF	Yes
34	42 (AF42)	42 (AF42)	AF42	No
35	0 (BE)	0 (BE)	BE (Best Effort)	No
39	5 (EF)	5 (EF)	EF	Yes
40	10 (AF21)	10 (AF21)	AF21	No
42	30 (AF41)	30 (AF41)	AF41	Yes
45	5 (EF)	5 (EF)	EF	Yes
50	40 (AF42)	40 (AF42)	AF42	No

coordinates (0, 1, 0), indicates an offensive maneuver that was carried out within the scope of the AF system's capabilities.

The third vector, which has the values (0, 0, 1), represents attacks that are considered to be within the parameters of the value range that is associated with computer science (CS). The fourth vector, which is represented by the notation (1, 1, 0), indicates an assault that takes place inside the EF value range. The quantification of the quantity of vectors recognized by the system can serve as an indicator of how effectively a connection between DSCP value and vector was established. This is accomplished by counting the number of vectors. The fact that there were more vectors found during the trial is indicative of the fact that it was more successful in identifying attacks.

The potential scientific basis for the finding of this research lie with three instances: ''Malicious Traffic Manipulation'', ''QoS Policy Violation'', and ''Traffic Engineering Adjustment''.

The phenomenon of malicious traffic manipulation refers to the deliberate and harmful alteration of network traffic for malicious purposes. In the given context, a malicious actor endeavors to manipulate the DSCP values of a packet with the intention of acquiring preferential treatment and elevated priority within the network. The potential attacker has the capability to modify the DSCP value of a packet to a value that signifies high priority upon its initial ingress into the network. During the transmission of the packet through the firewall, it undergoes a process of inspecting the DSCP value and identifying any unauthorized modifications. Subsequently, the firewall transmits an alert notification to the network administrator, signifying a plausible occurrence of a security breach or an effort to manipulate network traffic.

In the event of the violation of QoS policy. Network Administrators within a network may have implemented QoS policies to allocate priority to specific categories of network traffic. An instance of prioritization in network traffic management involves the allocation of a high-priority DSCP value to VoIP traffic. In the given context, it is possible for a user or application to deliberately or inadvertently alter the DSCP value of their packets with the goal of circumventing

QoS policies or obtaining unwarranted priority. The firewall actively monitors the packets, detecting any alterations in the DSCP values, and afterwards creates an alert to promptly inform network administrators about the violation of the established policy.

In the event of the modification of traffic engineering practices. Network operators have the ability to make dynamic adjustments to DSCP values in order to optimize traffic engineering. During periods of high demand, it is possible for network administrators to reclassify specific types of traffic as low priority in order to mitigate network congestion. In the above scenario, upon detecting a modification in the DSCP values as network traffic traverses, the firewall initiates an alert mechanism to notify network managers regarding the traffic engineering adaptation. This enables individuals to properly monitor and exercise control over network resources.

VI. IMPLICATION OF THE FINDING

The primary focus of this study relate to the need to conduct a study on transmission session and assess the potential modifications of DSCP values within each session. Experimental procedures of the study provide the means of manipulation of network traffic, forward the traffic and analyzed it through the implementation of a packet capture mechanism during transmission sessions. Python scripts were employed in accordance with its provision of flexible policy for network configuration [39]. Traffic analysis tool (Wireshark) was used for preliminary evaluation. Scripted traffic analysis tool was also developed and equipped with comprehensive policies to examine the packets that are transmitted during each transmission sessions of a network scenarios created. Subsequently, each packet that is captured is subjected to an assessment to determine whether the scripted tools used possess the ability to identify and report the existence of any tampered captured data packets. Hence, the entirety of the experimental task was centered around acquiring knowledge regarding the ''Impact of DSCP values.''

The finding of the study proof that a comprehensive network scenario created with the intension to demonstrate DSCP values status is possible with Python scripts. Furthermore, the finding reveal that the inspection process successfully identified any alterations and recorded the analysis of the report of modifications, providing information on the status of each packet during transmission through notifications. The analysis of the information extracted has revealed that the recorded transmission session exhibits a distribution characterized by a higher proportion of high priority packets. This observation implies the importance of recognizing that packets within a traffic flow during a transmission session do not conform to a normal distribution. The findings of the study indicate that the distribution of packets demonstrates stochastic characteristics. The present study was unable to establish a comparative analysis with prior relevant research due to the absence of any directly related studies at the time of writing this paper.

This study has additionally determined that it is possible to track and monitor the initial DSCP value of each packet as it progresses through the transmission session. Furthermore, it has been determined that the vector at the point of transmission exhibits significant potential for effectively monitoring the transmission process. Both normal and abnormal DSCP values were successfully identified. This development facilitated the generation of a comprehensive and reliable DSCP data compilation. The detection and flagging of attacks targeting the DSCP values in packets has become more straightforward. The occurrence of abrupt or unauthorized alterations to DSCP values may suggest the presence of potential security breaches or unauthorized endeavors to modify traffic prioritization.

The implication of this finding toward organization that uses network lies with the act of monitoring the DSCP values throughout the transmission path. This enables the detection of any potential efforts to interfere with or alter the entire network administration. Unauthorized modifications may suggest the presence of malicious activities that aim to circumvent QoS policies or gain an unfair advantage within the network. The discovery can be interpreted in order to comprehend the impact of various service classes on the flow of packets. Attackers can make packets with higher priority DSCP values, to correspond to lower numerical values, and in turn exhibit reduced or increased latency and be provided with preference in comparison to other packets with either high or lower-priority DSCP values. However, when the modification occurs, it not only impacts latency but also compromises network management and operation. In addition, it is important to refine the logic used to determine the anticipated DSCP values or incorporate more advanced analysis techniques based on the obtained results and observations. It is imperative to ensure that the experiments conducted are carried out within a controlled and authorized environment, as network analysis and monitoring often entail the handling of sensitive data and configurations.

Another implication of the study lies with experimentation to acquire insights into the network's handling of various service classes, as determined by their DSCP values, and to identify any potential issues or areas that could be enhanced. This is proven with the provision of the notifications that generates alerts to bring attention to situations in which the behavior of the network deviates from the anticipated performance for particular service classes. This information holds significant value for network administrators and security teams as it enables them to enhance network performance and guarantee appropriate QoS for diverse applications and services. The verification of DSCP values guarantees the accurate implementation of the network's security policies. Any instances of deviating from the anticipated conduct can be promptly examined and rectified.

VII. LIMITATION AND RECOMMENDATION

Although the generation of attack notifications through modifications of DSCP values proves pertinent and valuable

within a controlled research setting, its implementation within real-world networks may present challenges. Numerous contemporary networks utilize intricate QoS policies and traffic management mechanisms that may exhibit varying interactions with DSCP values. Furthermore, while the scope of the research is limited to examining specific attack scenarios that are associated with modifications to the DSCP values. Although this analysis offers valuable insights, it may not encompass the full range of potential attacks that specifically circumventing DSCP values or other attacks related to QoS. Another limitation of the study lies with the potential impact of network scenarios and scale on the study's findings. The replication of small scale laboratory setups may not faithfully capture the behavior and complexities encountered in large scale production networks. Finally, the study may fail to account for dynamic fluctuations in network conditions or the consequences of fluctuating levels of network traffic. Fluctuations in traffic are a common occurrence in realworld networks, and it is imperative to take into account the behavior of attacks in such dynamic conditions. The efficacy and feasibility of attack detection through exclusive reliance on modifications to the DSCP values may have certain limitations in practical situations, it is possible for attacks to exhibit greater complexity and present a heightened level of difficulty in terms of detection solely through the analysis of DSCP alterations.

Some key recommendation for future work lies with empirical investigation on the practical implementation of the viability and efficacy of producing attack notifications through modifications of DSCP values in operational networks. This may entail engaging in collaborative efforts with network administrators and implementing the proposed solution in real-world deployment scenarios. Furthermore, the scope of the attack analysis should be expanded to encompass a wider array of attack scenarios. This expansion should include attacks that exploit various aspects of QoS mechanisms, as well as application layer attacks and attacks based on traffic analysis. Finally, future research can investigate attack mitigation techniques, specifically focusing on the development of countermeasures and mitigation strategies to effectively respond to attacks based on DSCP values. The objective is to enhance network resilience and robustness in the face of such attacks.

The pros of this research proposed scheme is safeguarding against different network-based threats by identifying and mitigating illegal or malicious alterations to DSCP values. DSCP values play a crucial role in the effective administration of QoS, as a result preserving DSCP values is essential for upholding the appropriate prioritizing of network traffic, particularly in the context of time-sensitive applications Furthermore, the proposed scheme is capable of enabling network administrators to assign priority to specific forms of traffic, to mitigated any potential congestion and facilitating the uninterrupted delivery of essential services. Finally, in certain instances, the safeguarding of DSCP values may be compelled by regulatory obligations or industry norms in order to fulfill particular security goals. The adherence to these requirements can be considered advantageous when considering the implementation of this strategy.

The cons associated to the proposed scheme lie with computational complexity. The implementation of a technique aimed at detecting and addressing alterations to DSCP values might introduce intricacy to network settings and maintenance. The successful implementation of this task may necessitate the acquisition of supplementary equipment, software, and the allocation of ongoing resources for maintenance purposes. Furthermore, the occurrence of false positives and false negatives is contingent upon the sensitivity of the detection systems. False positives refer to the erroneous identification of legitimate changes as attacks, while false negatives pertain to the failure to identify actual assaults. Achieving an optimal equilibrium can be a formidable task.

The necessity of proposing a scheme for addressing attacks on DSCP values modifications stems from the importance of maintaining a secure and efficient network infrastructure. Malicious entities may endeavor to modify DSCP values with the intention of attaining unauthorized entry, evading detection, or causing disruption to network services. Safeguarding against such potential risks is crucial for ensuring the integrity of network security. Ensuring the integrity of DSCP values is crucial for preserving the uninterrupted functionality of essential services, including emergency communication, video conferencing, and telemedicine, which heavily depend on accurate traffic prioritization.

A. ALGORITHM PERFORMANCE

In the context of the algorithm developed for ''modifications of attacks notification of DSCP Values'' an examination of the associated detection performance revealed some important results.

Detection accuracy in identifying attacks or anomalies or the ratio of accurately detected in the given context is 100% accuracy for notifications. This is attributed to the fact that all modification has been labeled and tag and also being detected at the destination.

he detection delay on interval required for an algorithm to identify and acknowledge the presence of an attack or anomaly subsequent to its occurrence was zero. Since the packet need to be de-encapsulated in order to identify the present of modification or not.

A false positive (FP) refers to the erroneous identification of regular or authorized DSCP value modification. This phenomenon can be categorized as a misclassification error. In this research whenever a notification is make, detection happens, this suggests that the false positive rate is comparatively zero.

A false negative (FN) arises when the algorithm fails to correctly detect a legitimate attack or anomaly in the DSCP values. In contrast, the findings of this research do not align with this assertion.

A true positive (TP) refers to the accurate identification of genuine attack or abnormalities by the algorithm

on DSCP values. This is similar to the accuracy and for this research 100% detection has been found.

B. OPEN RESEARCH ISSUES

The subject matter of ''Modifications to Attacks Notification of DSCP Values'' pertains to the overarching realm including network security and QoS management. There exist numerous unresolved research matters and obstacles within this field that warrant investigation by scholars and professionals. Such endeavors aim to enhance the security and efficacy of network traffic management. Several open research issues can be identified. There are still issue associated to enhancing the effectiveness of DSCP spoofing detection methods by developing more advanced and resilient methodologies. DSCP spoofing attacks involve the manipulation of DSCP values by malevolent individuals with the intention of evading detection or obtaining unauthorized access. Furthermore, there is still issue on whether the application of machine learning and artificial intelligence (AI) techniques in order to improve the analysis of DSCP values, as well as the detection of anomalous traffic patterns or anomalies is feasible.

For the fact that this study explores techniques for the dynamic adjustment of QoS parameters and associated to DSCP values in response to real-time network conditions and traffic demands. There is still issues in enhancing network performance through the optimization of QoS adaptation strategies. Similarly, security measures employed to safeguard the configuration and allocation of DSCP values within network devices remain an open avenue for research explorations, with the aim of preventing unauthorized alterations or improper utilization. While this study serves as a countermeasure to minimize the adverse effects of attacks that involve alterations to the DSCP values, there are a lot opportunity that can encompass traffic filtering, rate restriction, and policy enforcement as means to address them from different views. This is an open avenue for research to consider. The involvement in the establishment of industry standards and best practices pertaining to DSCP value management, security, and monitoring is emphasized is also another open research issue.

There are other open research issues associated to awareness among network administrators and users regarding the significance of effectively managing secure DSCP values and the potential risks associated with modifying these values. This is also associated to ethical considerations, where critical examination of the ethical implications of DSCP value Inspection and Notification, with a specific focus on user privacy and consent be established.

VIII. CONCLUSION

The purpose of this study has been to investigate the complications of successful data transmission during network sessions and to investigate the potential implications of DSCP value alterations in the sphere of internetwork communication. The aim of this study has been to delve into the specifics of successful data transmission during network sessions. It has come to light that adversaries are able to abuse network security policies by changing DSCP values to indicate high priority in order to get around established protocols. This information has been brought to light.

During the course of our analysis, we carefully analyzed the traffic based on the service class and compared the actual DSCP values at the source with their anticipated values at intermediate nodes. This caused notifications to be sent as a result. In addition to this, we devised scenarios for a comprehensive investigation of the DSCP values connected to the various service classes. The end result of these analyses was an in-depth look into the DSCP values contained within the vector alert, which was carried out in a direction from the source to the destination.

Our findings highlight scenarios in which attackers seek to acquire priority over other network traffic by inserting packets with malicious DSCP values. These scenarios were brought to light by our recent research. It is important to note that these behaviors are easily detectable and may be monitored. This suggests that any change in DSCP values can be identified without impacting the performance of the network.

In addition, the results of our research show that vector representations are useful for assessing the degree to which packets may be distinguished from one another. This study makes an essential addition to improving network security and sustaining fair traffic management techniques by giving a number of different scenarios for detecting cases in which attackers attempt to alter DSCP values in order to acquire priority over regular network traffic. Their goal is to get priority over the regular network traffic.

REFERENCES

[1] T. Janevski, *QoS for Fixed and Mobile Ultra-Broadband*. Hoboken, NJ, USA: Wiley, Jun. 2019.

[2] B. Varastan, S. Jamali, and R. Fotohi, ''Hardening of the Internet of Things by using an intrusion detection system based on deep learning,'' *Cluster Comput.*, vol. 9, pp. 1–24, Jul. 2023.

[3] C. A. M. Alayón, D. López, J. J. R. Ochoa, and R. D. G. Tovar, ''Performance assessment of DIFFSERV and INTSERV services in QOS on an academic network using NS2,'' *Tecciencia*, vol. 7, no. 14, pp. 65–75, Feb. 2013.

[4] F. Hauser, M. Häberle, and M. Menth, ''P4sec: Automated deployment of 802.1 X, IPsec, and MACsec network protection in P4-based SDN,'' *IEEE Access*, vol. 11, pp. 56300–56309, 2023.

[5] T. Mazhar, M. A. Malik, S. A. H. Mohsan, Y. Li, I. Haq, S. Ghorashi, F. K. Karim, and S. M. Mostafa, ''Quality of service (QoS) performance analysis in a traffic engineering model for next-generation wireless sensor networks,'' *Symmetry*, vol. 15, no. 2, p. 513, Feb. 2023.

[6] F. Hilal and O. Gasser, ''Yarrpbox: Detecting middleboxes at internet-scale,'' *Proc. ACM Netw.*, vol. 1, pp. 1–23, Jun. 2023.

[7] P. Zórawski, L. Caviglione, and W. Mazurczyk, ''A long-term perspective of the internet susceptibility to covert channels,'' *IEEE Commun. Mag.*, vol. 61, no. 10, pp. 171–177, Oct. 2023.

[8] S. Gao, Z. Peng, B. Xiao, A. Hu, Y. Song, and K. Ren, ''Detection and mitigation of DoS attacks in software defined networks,'' *IEEE/ACM Trans. Netw.*, vol. 28, no. 3, pp. 1419–1433, Jun. 2020.

[9] H. W. Oleiwi, N. Saeed, H. L. Al-Taie, and D. N. Mhawi, ''Evaluation of differentiated services policies in multihomed networks based on an interface-selection mechanism,'' *Sustainability*, vol. 14, no. 20, p. 13235, Oct. 2022.

[10] D. Soldani, P. Nahi, H. Bour, S. Jafarizadeh, M. F. Soliman, L. Di Giovanna, F. Monaco, G. Ognibene, and F. Risso, "EBPF: A new approach to cloud-native observability, networking and security for current (5G) and future mobile networks (6G and beyond)," *IEEE Access*, vol. 11, pp. 57174–57202, 2023.

[11] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 29, no. 1, p. 518, Jan. 2022.

[12] T. Velmurugan, H. Chandra, and S. Balaji, "Comparison of queuing disciplines for differentiated services using OPNET," in *Proc. Int. Conf. Adv. Recent Technol. Commun. Comput.*, Oct. 2009, pp. 744–746.

[13] S. Ozawa, T. Ban, N. Hashimoto, J. Nakazato, and J. Shimamura, "A study of IoT malware activities using association rule learning for darknet sensor data," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 83–92, Feb. 2020.

[14] E. A. Ozturk and C. F. Bazlamacci, "Fairness in differentiated services architecture," in *Proc. Int. Symp. Comput. Inf. Sci.* Boca Raton, FL, USA: CRC Press, pp. 264–268.

[15] M. M. S. Maswood, R. Abhishek, and D. Medhi, "Network optimization for differentiated QoS traffic in an SDN environment for PoP-data center traffic," in *Proc. IEEE 39th Sarnoff Symp.*, Sep. 2018, pp. 1–6.

[16] N. Solihah, M. I. Nashiruddin, and E. S. Sugesti, "Regulatory impact analysis for XGS-PON standardization development in Indonesia," in *Proc. 13th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Oct. 2021, pp. 246–252.

[17] N. Kitsuwan and E. Oki, "Traffic splitting technique using meter table in software-defined network," in *Proc. IEEE 17th Int. Conf. High Perform. Switching Routing (HPSR)*, Jun. 2016, pp. 108–109.

[18] D. Cansever and J. Islam, "Flow based precedence and preemption methods without a priory signaling," in *Proc. MILCOM*, Oct. 2006, pp. 1–7.

[19] S. Daoud and Y. Qu, "A comparison research on DSCP marking's impact to the QoS of VoIP-based and SS7-based phone calls," in *Proc. 7th Int. Conf. Inf., Commun. Netw. (ICICN)*, Apr. 2019, pp. 66–71.

[20] N. Roddav, K. Streit, G. D. Rodosek, and A. Pras, "On the usage of DSCP and ECN codepoints in internet backbone traffic traces for IPv4 and IPv6," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Jun. 2019, pp. 1–6.

[21] N. O. Kniazieva and A. S. Kalchenko, "Quality control of multimedia services in mining enterprises 'corporate networks," *Sci. Bull. Nat. Mining Univ.*, vol. 1, no. 2, pp. 107–113, 2018.

[22] S. Uchida and S. Kimura, "Adaptive link rate switching based on traffic splitting method for power saving," in *Proc. 8th Int. Symp. Comput. Netw. Workshops (CANDARW)*, 2020, pp. 67–73.

[23] D. A. Garbin, P. McGregor, and D. M. B. Masi, "Using event simulation to evaluate internet protocol enhancements for special services," in *Proc. Winter Simul. Conf.*, Dec. 2007, pp. 2276–2284.

[24] E. F. Cahyadi, "Assessing readiness of IP networks to support H.323 desktop videoconferencing services over various scheduling techniques using OPNET," in *Proc. Elect. Power, Electron., Communicatons, Control Inform. Seminar (EECCIS)*, 2014, pp. 105–110.

[25] J. Li, L. Yang, X. Fu, F. Chao, and Y. Qu, "Dynamic QoS solution for enterprise networks using TSK fuzzy interpolation," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, Jul. 2017, pp. 1–6.

[26] G. Bianchi, N. Blefari-Melazzi, G. Bonafede, and E. Tintinelli, "QUASI-MODO: Quality of service-aware multicasting over DiffServ and overlay networks," *IEEE Netw.*, vol. 17, no. 1, pp. 38–45, Jan. 2003.

[27] K. M. Malikovich, G. S. Rajaboevich, T. S. Sobirovna, and E. Temurmalik, "DSCP traffic filtering method to prevent attacks," in *Proc. Int. Conf. Inf. Sci. Commun. Technol. (ICISCT)*, Tashkent, Uzbekistan, 2021, pp. 1–4.

[28] F. A. Yaseen, N. A. Alkhalidi, and H. S. Al-Raweshidy, "SHE networks: Security, health, and emergency networks traffic priority management based on ML and SDN," *IEEE Access*, vol. 10, pp. 92249–92258, 2022.

[29] M. Kozuka and Y. Okabe, "A policy-based path selection mechanism in QUIC multipath extension," in *Proc. IEEE 47th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Italy, Jun. 2023, pp. 1255–1259.

[30] T. Shreedhar, S. K. Kaul, and R. D. Yates, "Coexistence of age sensitive traffic and high throughput flows: Does prioritization help?" in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, New York, NY, USA, May 2022, pp. 1–6.

[31] T. Refaei, S. Ha, R. Starr, and M. Steele, "Using NDN and P4 for effective traffic management in tactical networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, San Diego, CA, USA, Nov. 2021, pp. 1–6.

[32] S. D. Sathyanarayana, M. Sankaradas, and S. Chakradhar, "5GLoR: 5G LAN orchestration for enterprise IoT applications," in *Proc. IEEE Future Netw. World Forum (FNWF)*, Montreal, QC, Canada, Oct. 2022, pp. 28–35.

[33] X. Yin, Y. Liu, L. Yan, and D. Li, "QoS flow mapping method of multi-service 5G communication for urban energy interconnection," in *Proc. Int. Conf. Wireless Commun. Smart Grid (ICWCSG)*, Hangzhou, China, Aug. 2021, pp. 75–78.

[34] C. Zhang and S. Kimura, "ALR switching and routing strategy for multiple sites based on traffic splitting method for power saving," in *Proc. 10th Int. Symp. Comput. Netw. Workshops (CANDARW)*, Nov. 2022, pp. 33–39.

[35] I. Nassra and J. V. Capella, "Data compression techniques in IoT-enabled wireless body sensor networks: A systematic literature review and research trends for QoS improvement," *Internet Things*, vol. 23, Oct. 2023, Art. no. 100806.

[36] R. Z. N. Ahmad, S. D. Jabaspal, S. Muliani, S. Sabila, W. Sofiyah, and Y. N. Pradana, "A NMAP and wireshark application for data analysis and network security," *JComce-J. Comput. Sci.*, vol. 1, no. 1, pp. 42–51, 2023.

[37] M. A. El-Gendy and K. G. Shin, "Assured forwarding fairness using equation-based packet marking and packet separation," *Comput. Netw.*, vol. 41, no. 4, pp. 435–450, Mar. 2003.

[38] K. Cardwell, "Advanced features of wireshark," in *Tactical Wireshark: A Deep Dive Into Intrusion Analysis, Malware Incidents, and Extraction of Forensic Evidence*. Berkeley, CA, USA: Apress, 2023, pp. 183–219.

[39] P. Shrestha and T. D. Sherpa, "Dynamic host configuration protocol attacks and its detection using Python scripts," in *Proc. Int. Conf. Artif. Intell. Knowl. Discovery Concurrent Eng. (ICECONF)*, Jan. 2023, pp. 1–5.

ALA ABDULSALAM ALAROOD received the Bachelor of Computer Science and Master of Computer Science degrees and the Ph.D. degree in computer science from the University of Technology Malaysia (UTM), in 2017. He is currently an Associate Professor with the Faculty of Computer Science and Engineering, University of Jeddah. His research interests machine learning, the Internet of Things (IoT), multimedia security, and cybersecurity.

ADAMU ABUBAKAR IBRAHIM is currently an Associate Professor with the Department of Computer Science, International Islamic University Malaysia (IIUM). He is also working in many areas of computer applications with an emphasis to computer network and computer network security, artificial intelligence, blockchain, and 3D graphics.

FAISAL S. ALSUBAEI (Member, IEEE) received the B.S. (Eds.) degree in computer science from King Abdulaziz University, Saudi Arabia, the M.Sc. degree in computer science, concentrating in security in computing from RMIT University, Australia, and the Ph.D. degree in computer science from the University of Memphis, USA. He is currently the Vice-Dean of the Deanship of Scientific Research and also an Assistant Professor with the Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia. He was a Software Engineer with Shaker and Associates Pty Ltd., Australia. He is currently a Microsoft Certified Technology Specialist, a Microsoft Certified Professional, and a Cisco Certified Entry Networking Technician. His research interests include security and privacy in the IoMT and cloud computing. He is also an active member of Australian Computer Society and Linux Users of Victoria.