The Forensics of DDoS Attacks in the Fifth Generation Mobile Networks Based on Software-Defined Networks

Shahrzad Sedaghat

(Corresponding author: Shahrzad Sedaghat)

Faculty of Engineering Department, Jahrom University
Jahrom 7413188941, Iran
(Email: shsedaghat@jahromu.ac.ir)

(Received Apr. 3, 2018; Revised and Accepted Apr. 4, 2019; First Online Sept. 21, 2019)

Abstract

The number of devices connected to the Internet has been increasing with the emergence of the Internet of things technology. Although it has many advantages, the weak configuration of Internet of things devices and the higher number of such devices provide a good potential for DDoS (Distributed Denial-of-Service) attacks. In this study, an approach based on SDN (Software Defined Network) and NFV (Network Functions Virtualization) technologies were presented for the purpose of network forensics and DDoS attack detection. In this approach, the entropy-based methods were used as a warning for DDoS attacks. The methods of detecting the fake IP address of the message source and a method based on correlation coefficient were used for separating the legal traffic from allowed traffic from non-allowed traffic. In addition, NFV technology was used for allocating more resources dynamically.

Keywords: 5G; DDoS Attack; Forensic; SDN

1 Introduction

The emergence of the Internet of things has caused the communication range of mobile to spread from personal communications to smart communications among different things and people. The bursty growth of data traffic due to applications such as a smart house, smart vehicles, smart environmental monitoring, and the like require a huge number of devices connected to the Internet and continuous emergence of new services, requirements, and capacity beyond the presented facilities in the current generation of mobile networks. The fifth generation of mobile networks was aimed at removing the time and place limitation and providing an interactive user experience.

The bursty growth of data size caused some problems to their management. Thus, changing the architecture of traditional mobile networks to the fifth generation of software-defined mobile networks is a new technology, which is expected to meet the needs of users in the future. This type of network is designed by integrating the software-defined network and network functionality virtualization. These two technologies can complete each other, keep the network servicing at the busy time of network, control and manage the network, and remove the exclusive problem of network solutions. Thus, their application is highly significant for future networks.

Despite such new technologies and concepts, network security is considered as a big challenge for future networks. Network threats can be related to mobile networks and potential technologies, which should be used in the fifth generation of mobile networks. By considering the bursty size of data and a high number of the devices connected to the network, detecting the suspicious activities and making a decision about whether this activity is malicious on behalf of the attacker or has another reason is very difficult. If the occurred suspicious activity is a type of attack, detecting the attacker and his tool and method is problematic. Computer forensics is a service in the area of computer collecting data from computer equipment and digital media processing the collected data.

Thus, network forensics can be highly useful as detecting the attacks in the early steps is regarded as a very important factor for preventing action in the early steps and detecting the cause of attack, On the other hand, even if this issue cannot be effective in preventing the attack, having some evidence on the attack can be useful for the future allowed pursuits and the design of a mechanism to cope with similar attacks in the future [15].

Despite new technologies and concepts, network security is a major challenge for future networks. Network threats can also be due to the nature of mobile networks, and also due to potential technologies that should be used in fifth-generation mobile networks [6, 19]. Distributed denial-of-service attacks are one of the real threats to these networks, which can lead to a lot of destruction in the IT infrastructure and communications. Therefore, any financial and governmental organization with vast infrastructure and information and communications resources is potentially exposed to this attack and it is necessary to find a way to respond to this type of attack by implementing a new and effective mechanism.

With this introduction, as well as considering the explosion of data volumes and the large number of devices connected to the network, it would be very difficult to detect suspicious activity and to decide whether this activity is an offensive act by an attacker or another reason. It is also difficult to determine who and by whom and with what method the crime was committed If suspicious activity is a kind of attack. Computer criminology is a science in the field of computer, in order to detect crime, collects evidence from proven scientific techniques for collecting, identifying, reviewing, combining, Correlation, analyzing and documenting evidence obtained uses processing, or Transfers digital resources [15]. Since the identifying attacks in the initial steps can be a very important factor in stopping it in the very first steps and identifying the cause of the attack, Therefore, the discovery of network crime can be very useful in this regard.

In this paper, our intention is to use criminology to detect the distributed denial-of-service attacks. The public aspect of the denial-of-service attacks (distributed) is sending large volumes of traffic to the network and saturation of its resources, which leads to the emergence of changes such as a sudden increase in traffic, delays in service delivery, excessive use of the processor and possibly reduced efficiency in the network activity pattern. Therefore, having evidence of changing the pattern of the network, analyzing this evidence and understanding its origins can be a great step to counteract or prevent this kind of attack [18]. Therefore, in the following, a solution is proposed for the purpose of the criminology of distributed denial-of-service attacks on fifth-generation mobile networks, with three general steps and follows the following goals:

1) Data collection: Detection of denial-of-service attacks be in different layers of software-based distributed networks, and therefore the processing burden resulting from this goal is not imposed on a specific layer.

2) Combine and correlate: In order to obtain the correct information, ensure the reliability of the data collection nodes.

3) Follows the analysis: More types of distributed denial-of-service attacks are covered.

This paper is organized as follows: The second section presents the significance of forensics. Section three explains the different types of DDoS attacks and the new types of attack in SDN networks. Section four explains the previous studies on discovering, preventing, and repairing the DDoS attacks. Section five describes the proposed strategy and section six presents the conclusion.

2 The Significance of Forensics and DDoS Attack

Network forensics is using the proved scientific technologies for collecting, identifying, studying, combining, analyzing, and documenting the evidence obtained from digital sources process or transfer. It is aimed at discovering the planned facts, measuring the success of allowed activities including sabotage or abuse of system components, and having sufficient information for responding to the malicious activity or improving the mechanisms and systems after each activity [15].

The present study aimed to use the forensics for DDoS attack criminology. The DDoS attack is a real threat for the network, digital, and security infrastructures, which can cause much destruction in the infrastructures of information technology and communications. These attacks are made due to financial- political benefits, or destruction. In the list of recent DDoS attacks, there are the websites of Greece bank, Ireland government, Polish Airlines, Thailand government, and Canada government. Thus, each organization including the financial and governmental with broad information and communications are potentially exposed to this attack looking for a way to respond to this type of attack by implementing a new and effective mechanism [5].

The general aspect of DDoS attacks is sending a bulk size of traffic to the Internet and saturating its sources, leading to some changes such as the sudden increase of traffic, delay in service delivery, excessive use of the processor, and reduction of efficiency in the network activity pattern. Thus, having some evidence for changing the network pattern, analyzing such evidence, and understanding its origin can be considered as a big step for coping with or preventing this attack [18].

By presenting this definition, the functionality of a forensic system can be expressed in three steps: Data collection, combination and correlation, and analysis.

The forensic network is mainly introduced as an observation point to a forensic system. In other words, the forensic system uses the network nodes for observing and recording the functionality and events of the network. Thus, the complete and accurate collected data depends on the reliability of the used nodes. In other words, the unreliable nodes cannot meet the complete observation of the network, which is the primary and important step of forensic systems. Thus, this case is one of the forensic challenges in the networks. An increase in analysis methods is regarded as another challenge in forensic systems. Trusted or not network nodes that in designed architecture called the virtual explorers, using the challenge-response algorithm, the network monitoring module is located. For this purpose, the module sends packets of challenge-response packets to data-level virtual explorers randomly or at certain times. These challenges can be small requests sent to the virtual explorers. The speed of the reaction of the virtual explorers to these pack-

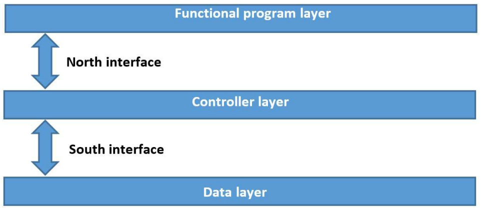

Figure 1: The layers of SDN networks

ages compared to the speed of this node to send recent reports as well as the completeness of the information received can provide an indication of the reliability of the virtual explorers.

3 Describe Different Steps of DDoS Attack and Introduce Similar Attacks

DDoS attacks prevent the access of allowed users to the computer, network, or information sources of the victim by using the distributed sources. Such distributed sources called “Zombie” are controlled by a manager and send some packets to the victim randomly or regularly when they receive an order from the manager. A type of classification for these types of attacks is displayed in Table 1.

3.1 New Types of DDoS Attack in SDN and 5G Networks

Since the software-defined networks are the inseparable parts of the fifth generation mobile networks, the attacks can use the wireless networks’ nature and potential attractions of software-defined networks for making the DDoS attacks.

By considering the different layers of software-defined networks Figure 1, the data layer, communication interfaces among the controller, the surface and the control layer are the attractive parts for attackers to make DDoS attacks. The switches in the data layer adapt the header of each packet to the available rules in their rule table when they receive a packet. In the case of adaption, the packet is processed based on that rule, otherwise, a message called “packet-in” is sent to the controller through the south interface by using the fields inside the packet header and the controller defines a new rule to send to the switch.

In a type of DDoS attack, the attacker produces many packet-INS and saturates the south interface broadband by producing the new flow (*e.g.*, by randomizing a part of fields in packets’ header) Figure 2. In addition, when the number of fake packets arrived to switch is excessive, the total switch memory is filled with the non-useful flows rule leading to discarding the new input packets.

The controller can have a special attraction for DDoS attack because it is related to other levels by using the north and south interfaces. Thus, the attacker can make the controller to define new rules by sending new flows to the data level or the functional programs can prevent the controller from addressing the important and allowed affairs by sending unnecessary feedbacks.

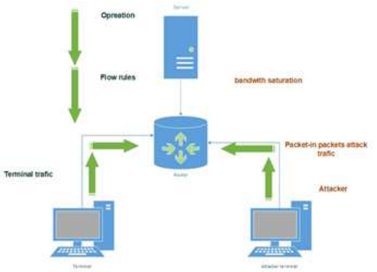

Figure 2: Broadband saturation attack in SDN

The new type of DDoS attacks in wireless networks is called “jamming” which reduces the signal rate to the noise in the receiver by sending the intervening wireless signals. The attack, which is an interventional interaction, can prevent or modify communications by intervening in the network physical equipment, network status, and network configuration.

4 Review of Literature

In this section, the mechanisms used for discovering, preventing, and restoring the DDoS attacks are explained. A review papers by Boani *et al.* [3] Classified the conducted studies into three groups of discovery, prevention, and restoration. Tables 2, 3, and 4 represent the classifications. Then, some studies were explained in more details, which may be placed in more than several groups. The review of these studies could provide us with a good perception of this subject.

4.1 Detailed Expression Some of Researches

Zhin *et al.* [8] suggested the use of TTL in the IP packets header for detecting the fake traffic. In the proposed algorithm, the number of steps between the sender and receiver was calculated by extracting the TTL field and the sender’s IP address. Then, the calculated steps were studied to see whether they are correct or not. In case of a correct number of steps, the source IP address was considered as real and in case of incorrect number, the IP address was fabricated. In this study, a challenge was guessing the initial value of the adjusted TTL in the message source, which was derived in the sender by considering some hypotheses.

Tapengam *et al.* [16] proposed a method for recognizing the DDoS attacks in allowed congested networks. Based on the results of this study, the DDoS attacks today are mainly based on botnets, which are considered as automatic or semi-automatic methods running a program and

Table 1: Different types of DDoS attacks

Flood attacks based on feedback	
attack Smurf	A large number of ICMP packets with a fake IP address move towards the network leading to traffic congestion in the network.
attack Fraggle	This attack is like Smurf, but it uses UDP traffic instead of ICMP traffic to achieve the same goal.
Flood attacks based on protocol abuse	
Attack based on SYN packets	An attacker, by setting the SYN bit, sends a packet to the attacker in the TCP handshake. The victim responds to the attacker with the SYN-ACK packet and adds a record to his memory and assigns this connection. The attacker will never respond to this packet. Repeating these communications will result in the full memory of the victim and lack of response to allowed users.
Attack based on UDP fragmentation	In this attack, the attacker sends a few large UDP packets (over 1,500 bytes) in order to add more bandwidth. The victim resources are used to rebuild and collapse packages that cannot be assembled again.
Attack based on feedback and amplification	
The attack is based on DNS amplification	In the attack, the DMS small Zombies send a fake source IP address which generates a large amount of traffic to the victim
The attack is based on NTP amplification	The attack is also like DNS amplification but the packets are sent to NTP servers instead of being sent to the DNS server

acting based on a predictable model. On the other hand, the allowed users usually spend their time responding after their first request. For example, after showing the webpage to the user, he takes some time to respond by clicking on a link. In other words, the request rate of allowed users during a time period is unpredictable.

These studies divided the attacks into two groups of predictable and non-predictable rates. The attacks with predictable rate were divided into the constant rate, incremental rate, and periodic rate. Finally, this study tested the packet sending algorithm by using the packet receiving rate as the studied parameter and using the Pearson correlation coefficient as a mathematical model and then classified the network traffic into malicious and uncertain groups. Tapengam *et al.* studied the correlation coefficient between the packet input rate and their input time and analyzed the correlation between the packet input rates with each other. Presenting a good solution for detecting the botnets is regarded as one of the valuable aspects of this study. In addition, such a method can be used in any analytical module.

Tapengam *et al.* [17] presented an approach based on supervised machine learning which learns the behavioral pattern of the network sources by observing the input packets. The features of the data input rate were processed by using the Pearson correlation coefficient and Shannon entropy.

Then, these two features were classified by using the LDA (Linear discriminant analysis) into attack or allowed traffic groups. Accordingly, the traffic derived from the attack was filtered and the allowed attack was passed. The data provided to the LDA classifier were grouped into training data and test data. The detection power of the classifier was depended on training data. On the other hand, waiting for the training phase can cause delay and problem for using this method at real time.

Shin *et al.* [14] presented an approach called AVANT-GUARD for managing the flows in the software-defined networks based on the open flow. The communication immigration aimed to separate the sources enabling to complete the TCP handshaking protocol and the sources which could not perform it. The second module for activating without rule flow delay can be used under special conditions, which help the control level manage the network flows without delay. For this purpose, the controller specifies the conditions according which a warning should be issued and registers them in the switch. Each switch produces a warning based on this event and sends it to the controller in case of facing such conditions. By receiving this warning, the controller can change the rules of flow registered in the switches to control the current conditions. The main advantage of this study was separating the allowed traffic from the non-allowed traffic. However, in this study, only a specific type of DDoS was addressed. In addition, two additional modules should be added to SDN architecture for implementing the proposed method.

In another study, Lim *et al.* [9] presented a model for blocking the DDoS attacks, based on software-defined networks. In the architecture of this proposed model, they presented a module having a pool of IP addressed. Based on the packet-ins sent from data to the controller, this module monitored the number of flows in each switch. Simultaneously, the server monitored the parameters showing a DDoS attack. When the server found an attack, it

Table 2: DDoS discovery methods

Solution	**Discovery methods**
Entropy-based methods for detecting abnormal behavior depending on the distribution of network characteristics. Probabilistic distributions of various network feature such as the source and destination IP address and port number are used to calculate entropy. In order to determine whether current traffic behavior is normal or non-normal, a predefined threshold on entropy changes is used.	Entropy
Machine-based methods use techniques such as Bayesian networks, SOM and fuzzy logic to identify abnormal behavior. These algorithms pay attention to the different characteristics of the network and traffic to discover the abnormal behavior of the network.	Machine learning
These techniques work with the assumption that infected hosts behave differently from healthy hosts. Generally, botnets and infected machines (bats) are controlled by a single bat. The same traffic pattern is the result of sending a command to a large number of botnet host members, which results in the same behavior (sending illegal packets, starting to scan).	Traffic Pattern Analysis
These techniques are divided into two categories: 1) The successful communication rate 2) The rate of communication refers to the number of communications in a given time window.	Communication rate
These techniques use a combination of the intrusion detection system (such as SNORT) and Open Flow to detect attacks and re-configure the network dynamically. An intrusion detection system monitors network traffic to monitor suspicious activities, and Open Flow switches dynamically reconfigure the network based on real-world discoveries.	Integration of Open Flow with SNORT

Table 3: DDoS prevention methods

Solution	**Prevention methods**
In these solutions, a profile of users is kept, and the information header of each packet is checked and, and packages are prioritized to respond depending on the service previously agreed with the client.	Customizing the customer resources
In the mechanisms of this category, load balancing algorithms and virtual machines or virtual network functions are used to deal with a DDOS attack. In a number of studies, input traffic using load balancing algorithms is divided among several (virtual) factors. These virtual agents are allocated as needed and dynamically. The operating factor of the load balancing algorithm can also be a virtual factor.	Load balance
This mechanism is used to deal with DDOS attacks which generate fake traffic using fake IP addresses as the source address. In order to counteract this attack, they use the challenge-response mechanism. In this method, the server sends the packet to the originating IP address (sender of the message). If the sender is unable to respond to, it will be authorized as a fake source.	Factor detection mechanisms

Table 4: DDoS restoration methods

Solution	**Restoration methods**
Network traffic which satisfies the defined rules is sent and the rest of the traffic is discarded.	Discarding the packet
The network traffic sent by the attacked port is completely blocked.	Closing the port number
The allowed traffic changes to a new IP address.	Changing the route
The controller limits the flow rate by allocating the average bandwidth to each interface.	Controlling the broadband
The network controller changes the flow table of each switch to change the network topology.	Changing the network topology
When an attack is detected, the victim's MAC or IP address is changed, resulting in allowed traffic to the new address and the blocked traffic will be blocked.	Changing the MAC address or IP address

sent a message to the module through a secure channel and the module gave a new IP address to the server so that the server had to continue its work from that address. By using this module, the IP address of services was turned into a new address and a DDoS attack made by fabricating the source IP address failed. However, the allowed clients can search the new IP address from the server to achieve the service. In case of DDoS attacks based on bots which failed to fabricate the IP address, Lim *et al.* suggested the information message of new addresses in a form causing a huge computation to the client for understanding. For this purpose, Captcha was used in this model. However, each model causing difficulty for the bots to understanding the route change message will realize the objective. In the proposed model, it is assumed that the new addresses are all attributed to a similar physical machine by the SDN controller. When a client detects the bot or its fake IP address, a rule corresponding to the removal of current packets in the relevant flow should be sent to the switches.

This study could destroy the predetermined planning of the attacker by providing the strategy of changing the IP address. In addition, the address fabrication attacks were coped with the proposed model. These two mentioned factors could be considered as the strengths of this study.

Wang *et al.* [20] presented a model for coping with DDoS attacks to saturate the broadband between the data and controller. When the saturation attack was discovered, two new modules of flow rule analyst and data level cache were activated. All packet-ins were sent to cache in terms of attack detection, kept there temporarily, and sent gradually to the controller. The analyst module produced some rules as hyperactive based on the received packet-ins and installs them on the switches. Although this solution could help at the time of DDoS attacks, it failed to provide any solution for separating the allowed traffic from the non-allowed traffic.

Paydrahita *et al.* [12] presented the defensive system for DDoS attacks in software-defined networks. They identified the network traffic status by monitoring the output interfaces to inform the controller, which studied the network topography while receiving these warnings and ask the other routers to send their information. The routers responded to the controller by sending the source and destination IP addresses. Then, the controller avoided the saturation of broadband and lack of servicing the virtual flows between the attack flows by sharing the broadband fairly and fining the flows, which did not use this broadband appropriately. When the network was congested, the controller sent the necessary orders to the congested router and the routers, which were on the route of sending the packet to the congested router. In the case of non-congested routers, if the bit rate of sending the packet was less than the bit rate based on a fair system, that flow would be classified as good-behavior flow. However, if a flow used the broadband more than the specified threshold, the broadband would be less than the fair broadband and this reduced rate would be imposed as fine to this flow. This study prevented the inactivation of network services for allowed flows by sharing the broadband fairly while it failed to present any solution for separating the allowed flows from non-allowed flows. In addition, it could delay data collection and request the data from routers when the network was congested.

Turwald *et al.* [18] presented an entropy-based approach for discovering DDoS attacks in the software-defined networks of VANET (Vehicular ad-hoc networks). Entropy is a concept in the field of data flow measuring uncertainty about a random variable. If a random variable occurs more than the other variables, its entropy (uncertainty) becomes less. In this study, the investigated data were packet header. Some fields from packet header were considered as a random variable and the emergence of these variables and their entropy were calculated in a certain time period called "window". In this study, the source IP address was one of the random variables. The controller had to calculate the entropy of this variable by counting the number of sent packets towards a specific source. If the entropy exceeded the threshold, the packets would be random which can be due to a DDoS attack. Although using the entropy could be a good warning for the congested network, determining a threshold for entropy was challenging. In addition, entropy could provide us with useful information about the distribution of variables. In other words, the variables with different distribution but similar uncertainty were considered the same in this solution. This solution could separate the allowed traffic from non-allowed traffic.

In addition, Yan *et al.* [21] presented a plan for dealing with DDoS attacks, which led to excessive traffic load to switch level. In this plan, the switches of data level played a cooperative role for each other. In the proposed method, a controller monitored the status of switch flows table in terms of the used and non-used part. If the switch memory space was completely filled, the traffic sent to this switch would be guided towards other switches. Thus, the traffic was distributed throughout the network and new rules were included in the tables of networks switches flow. By this method, the empty sources of total network flow tables were used for reducing the attack.

Suggesting the status of switch memory status and guiding the traffic towards other switches can be performed by the controller at the time of studying the packet-ins. The status of switches could be studied periodically and actively in terms of memory consumption rate and then develop some rules by the controller. In addition, attempting for installing route change rules could not necessarily be made at the time of full switch memory and could be made sooner. This study kept the quality of service by distributing the sent traffic to the whole network but dealt similarly with flows including allowed or non-allowed.

Chawlo *et al.* [4] distinguished the traffic related to DDOS attacks from the huge but allowed traffic by using the Pearson correlation coefficient method. This method was composed of discovery module and the traffic separation module. In the discovery module, the input traffic was sampled and the features of source and destination IP address, the number of packets in each time period, and a number of packets sent from each IP address were extracted.

If the number of packets at a time period of T was more than a certain amount, a warning signal would be sent to the separation traffic module. Otherwise, the traffic would be considered as allowed traffic. In the traffic separation module, the traffic correlation coefficient was calculated and the created traffic was classified into two groups of DDoS attack or the congested network due to allowed users depending on the calculated value. This study introduced the instant Pearson coefficient as the best option for detecting DDoS attacks by testing different correlation coefficients.

Alhabi *et al.* [2] used the NFV technology to present a smart method for discovering the DDoS attack. The present study aimed to identify all DDoS attack and a deep investigation were used to divide the traffic into allowed traffic and attack traffic. The approach presented in the two steps mentioned the input traffic in the two steps of quick observation and deep investigation. The deep investigation was only presented when the first step showed positive results or received the message from the source allocation protocol. ARP protocol was used for allocating new sources or reducing the allocated sources. This protocol sent a message to the coordinator module when the consumed memory was more than the specified value creating a virtual machine to keep servicing. In the quick observation step, the status was recognized suspicious and the deep investigation module was activated when the input traffic was more than the threshold value or a message was sent for detecting more sources. This module detected the type of DDoS attack by receiving the data like the used protocol, packet size, destination port number, and source IP address. For this purpose, some algorithms were designed in which the attack was detected depending on the value of protocols and packet size exponentially or linear increase of the flow.

Shang *et al.* [13] presented a plan for coping with DDoS attacks imposed on data and controller. In this plan, the network status including the packet, in message rate, memory, and processor were monitored continuously and dynamically. In case of detecting the traffic in a switch, a module called table-miss module sent some flow rules to the victim switch, upon which the switch should distribute a part of table-miss traffic among its neighboring switches. Protective rules were only applied to the changed traffic due to the probability of interference between these protective rules and flow rules inside the switch. The next module filtered the message in two steps. In the first step, the flows with the frequency rate more than the defined threshold were separated. In the second filter, some features such as the number of packets in a flow within a time interval, the number of bytes of a flow within a time interval, the total number of packets in the opposite flow in an interval, and the number of bytes in the opposite flow in an interval were extracted from these data and sent to the SVM (support-vector machines) for classifying this flow into two groups of normal and attack. This learner was resistant to learning the data with high noise. Thus, all packets were divided into two groups of attack and non-attack. Based on the two described filters, some rules were defined for including in the victim switch. The two-step filter was one of the strengths in this plan and separating the traffic in the second filter added to this strength. However, one of the concerns in the proposed approach was related to SVM learning to see if it can be used timely in the real world and its error detection rate.

Further, Jakarya *et al.* [7] presented a model for coping with DDoS attacks, in which the DDoS attacks based on the fabrication of source IP address during the implementation of handshaking protocol, was prevented by using the NFV (network function virtualization) technology. In this plan, there were two main modules each one allocated dynamically by using the NFV. In the first module, the received packets were distributed among some factors (the second module) responsible for filtering the packets. In the case of high traffic, the number of such factors increased. A load balance algorithm was used for distributing the packets. These factors test the clients implementing the TCP handshaking protocol with the server by sending the challenge-response packets. The strength of this study was using NFV technology for allocating the sources dynamically. This study only dealt with a specific type of DDoS attacks.

In another study, Afek *et al.* [1] evaluated a variety of methods for making fake packets and presented an approach based on the software-defined network to cope with the huge size of packets sent to the network. Verifying each packet was performed in each switch. In the proposed approach, using the total sources of the network was suggested to cope with this type of attack. For this purpose, some thresholds were defined and the network status was defined for the two parameters of rules memory capacity and processing parameter. If one or two parameters exceed the defined threshold in a switch, the controller will guide the network to the parts with fewer loads by defining the traffic rules sent to the bust part of the network. This study used the total network sources optimally by using the load balance algorithms to respond to the input traffic, which was one of the strengths of this study. However, it only dealt with a specific type of attacks and used the controller as the monitor of the network status, which was equal to imposing more processing loads to the controller.

Lyanaj *et al.* [10] presented a plan for monitoring the fifth generation mobile network based on software-defined networks. The architecture of this plan was in line with the architecture of SDN networks developing the SDN architecture at three levels for the network monitoring functionality. The monitor controller could perform the abilities of traffic monitoring, load balancing, and monitored data accumulating. Thus, it could optimize data analysis based on security needs. This monitoring controller can be implemented by P2P hierarchical model. The south interface of this controller sent the controlling messages related to monitoring the monitor explorers at the data level. The explorers were the virtual machines collecting the behavioral information of network and could be dynamically allocated. Explorers could operate passively (only for data collection) or actively (for prevention, reduction, or correction). These explorers were managed by the module, which was a part of NFV responsible for their dynamic implementation and configuration. The dashboard was a functional program considered as the functional programs of SDN networks enabling the user to specify the objectives of the monitoring system. By assuming that the 5-the generation mobile networks will be integrated with SDN architecture, the strength of this plan was that this architecture could be exclusively used for security goals. In addition, the abilities of network virtualization could cause flexibility in this plan under different network situations.

Lopez *et al.* [11] presented a plan based on network status awareness to manage and respond to the fifth generation mobile networks' events. This module which was designed as layered and could be adapted to SDN and NFV technologies monitored the low-level parameters of the network behavior by the explorers based on virtual infrastructures. Such explorers were the NFV programs, which could be personalized for monitoring and placed in different network infrastructures based on the need. The data collected from these explorers were provided to the module in the higher layer, i.e. the monitoring and correcting module. This module could collect the network traffic data precisely with low processing overhead at the real time by using the described explorers. This module could control the allocation and access to explorers. Such explorers were accessible based on two scenarios: they sent a report in case of discovering an event or the monitoring module requested the data from the explorers. The higher level module and the analysis module identified the network status by using the parameters provided by the monitoring module. In fact, this module monitored the events and extracted the risks exposed to the network by receiving the reports sent from the monitoring module. A part of this module predicted the future events by using the collected data, discarded the collected data after a time interval (defined), and used the new data for prediction for compatibility with network status dynamism. In order to detect the errors and attacks, different methods of machine learning like Bayesian networks were suggested to correct the risk detection methods. The last module was responsible for defensive measures against the probable risks such as load balance and network traffic management. This module could potentially use a big reservoir of NFV programs to operate its measures.

Furthermore, Zhang *et al.* [22] represented a plan based on packet prioritization coping with the overhead attack of rule table in the data switches in SDN architecture. In this study, the switches periodically sent the messages including the new packets input size and the number of packets in each flow to the module. In this study, the attacker sent a lot of new flows with a few packets toward the victim to reduce the attack cost. After data collection, the flows were classified into two groups of good and bad based on the number of packets sent by a client and the number of flows in this client. Then, two values of high and low threshold were considered for this parameter. The value of this parameter for each flow belonged to one of the groups of higher than the high threshold, a value between the two thresholds, and a value less than the low threshold. Accordingly, this study received services based on its label. Thus, the switches serviced some packets with high priority in the congested network and they discarded the packets with low priority in case of excessive congestion.

4.2 A Summary of Previous Studies and Presenting Some Challenges

In the previous section, some studies were stated in more details to understand the proposed solutions precisely. Furthermore, their strengths and weaknesses were mentioned at the end of each study. Some necessities of the proposed method which were considered in the fifth generation mobile networks, as explained in the weakness part of previous studies, are described below:

1) Separating the allowed traffic from the non-allowed traffic is very difficult because of too much similarity between the non-traffic traffic behavior and allowed traffic. For example, complicated botnets can pass the DDOS attacks discovery mechanisms by imitating the allowed traffic pattern when the requests are high.

2) Keeping the error detection rate low may lead to low discovery rate so that the DDoS attacks which are slow can easily pass the solution of attack prevention.

3) The proposed plans are usually software and are not integrated into the proposed solutions for DDoS attacks of interference type.

4) The proposed methods only consider the external attacks and do not regard the internal malicious factors of the network, as one of the forensic challenges in the network.

5 The Proposed Plan Architecture

The present study aimed at using the forensics to cope with DDoS attacks occurring in the future generation mobile networks. Thus, the proposed method should include three steps of data collection, analysis, and decision-making.

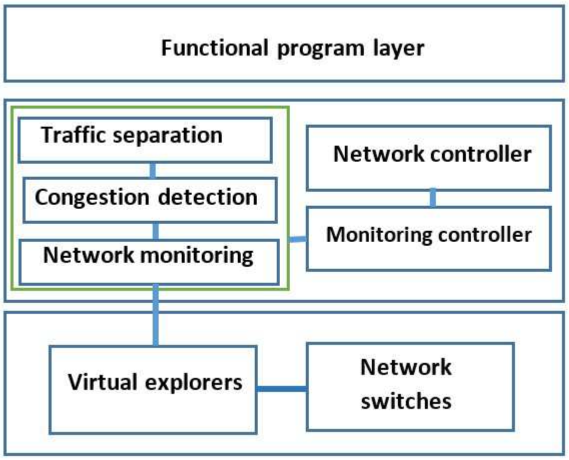

Figure 3: The proposed architecture

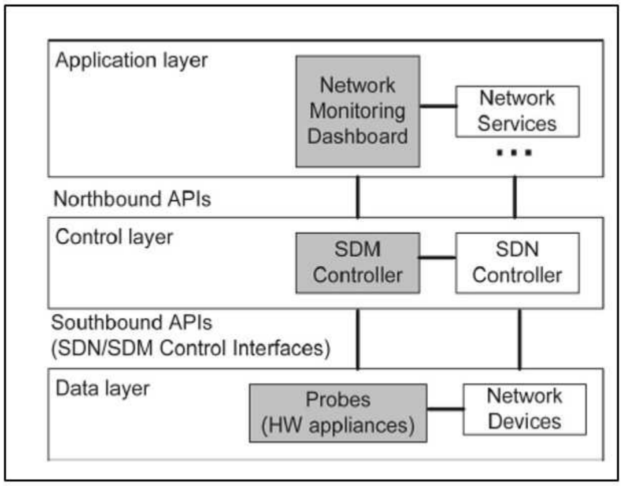

Figure 4: Research architecture

Since the SDN architecture is the inseparable part of the future generation networks, the proposed method is based on SDN and NFV technologies.

Here are the main expectations of a comprehensive solution for discovering, preventing, or restoring this type of attack:

1) DDoS protection mechanism should not disrupt the allowed traffic activities.

2) DDoS discovery mechanism should prevent both attacks inside or outside the networks.

3) The proposed mechanism should have efficiency and scalability.

4) The proposed mechanism should be implemented at a minimum cost.

5) It should include more types of these attacks.

This solution is based on the architectures [10, 11]. This architecture is composed of four functional layers: Virtual and real explorers, monitoring, and congestion detection, and allowed and non-allowed traffic separation. The last three modules were controlled by the high level of controller. The monitor controller shared its results and decisions to the network controller. In fact, the proposed method could be implemented as a security service in SDN architecture.

In the proposed architecture Figure 3, the statistical data were collected by the explorers. These data collected by the virtual explorer includes the packet arrival rate to the network, the origin, and destination IP address, the package type. This information is sent to the monitoring module. Each of the congestion detection and traffic separation modules use some of these information items to perform their task. The statistical information was sent to network monitoring, congestion detection, and traffic analysis modules. Congestion detection module studied the congestion in the network based on the threshold-based methods. If the input traffic exceeding a certain rate or the switch memory consumption is more than a certain limit, these situations will be sent to the monitor controller as a report based on congestion (allowed or non-allowed) which can also be sent to the network controller. Traffic separation module divided the input traffic into two groups of allowed and non-allowed and sent the obtained results to the monitor controller. The network controller could develop the appropriate rules in the network switches by receiving these data.

As described in Section 3, the DDoS attacks identification and monitoring section are divided into two data layers and controllers. The intermediate module, in fact, is a monitoring controller that consists of three network monitoring stations, congestion detection and traffic separation. These three parts are initially organized in sequence and then in parallel with each other. In other words, at first, the congestion detection module waits for information from the monitoring section and the traffic separation module waiting to apply for work from the congestion detection module. But after receiving the first information and requests, all three modules can be simultaneously in operation.

Authors in [1] provide a Software-Defined Networking-based solution that includes only DDoS attacks based on fake packets. However, in this research, it is suggested that along with using the method presented in [1], the Pearson coefficient method [4] used to Detection of distributed denial of service attacks Which is done using real clients (and not fake ones). In addition, in [1], monitoring and network identification are assigned to controllers. In the present study, the monitoring and security monitoring work on network inputs is assigned to separate modules from the switch controller, thus reducing the processor load imposed on the controller. For example, the monitoring module is in the form of a separate module in the controller layer and it receives its information from the nodes of the explorer in the data layer.

Authors in [10] with aims to provide more sophisticated and dynamic management functions, an SDN-based design for monitoring Figure 4 of the fifth-generation mobile networks. In the present study, it is suggested that architecture [10] In particular, it is used to identify DDoS attacks. For this purpose, the middle section of this architecture (SDM Controller), which is called monitoring controller in the present, is composed of three monitoring modules, congestion detection and traffic separation based on its specific task, namely identification of DDoS attacks. Data surface virtual explorers are also used in both surveys to collect information and send data to the middle section. In the present study, the assumption of the inadmissibility of these virtual explorer is also proposed, and it is suggested that the mid-section of the network, using the challenge-response algorithms, measure their accuracy.

5.1 The Variables Describing the Network Status

The present study aimed at detecting the DDoS attacks. The different methods of detecting such an attack considered different features of network flows to detect DDoS attacks. In this study, the features presented in Table 5 were suggested by considering some aspects of DDoS attacks.

5.2 Data Collection and Virtual Explorers

The virtual explorers continuously collect traffic log data into the network, source IP address, package type, and packet arrival rate, and send it to the monitoring module. Explorer nodes are the virtual or real machines at data level monitoring a small limit. These machines send the features of packets or input flows to the network in the form of some reports to the monitoring module. These reports were suggested to be sent to the monitoring module after entering a certain amount of packets. The questions raised in this module are as follows:

1) Where the explorers should be placed? In other words, how should the explorers be distributed? As mentioned, these explorers can be both real and virtual. Implementing the real explorers is optimal only in congested places near the entry gates or the servers providing important or interesting services to the client. In addition, at least one virtual explorer should be used in such places to ensure the accuracy of collected data and be considered as an auxiliary source at the time of network congestion.

2) What and when should the explorer's report? These explorers must monitor the described variables in Section 5.1 and after collecting the data about a certain amount of packets, they can prepare a report and send to the monitoring module. Such reports can be on packet or deduction of flow and can be prepared after a time period or certain number and sent to the monitoring module at the controller layer. The monitoring packets sent by the explorer must include the time cache which can provide the monitoring module with updated information and reflect the dynamic changes of the network.

5.3 Network Monitoring and Data Collection

The network monitoring module sends information from virtual explores to the congestion detection module. This module also has the task of organizing the virtual explores. More precisely, the organization of the virtual explorers includes two parts of the new virtual explorers' allocation and their verification.

About task new virtual explorers' allocation, the monitoring module can Do this in each of the following conditions:

1) Declare network congestion by congestion detection module;

2) Increase the number of reports received from virtual explorers within a specified time period;

3) Specific times the network administrator guesses that traffic congestion will be higher.

Regarding the task of verifying the virtual explorer nodes, the monitoring module is organized regularly or at random times, by sending a packet to a virtual explorer node that contains a challenge based on a challenge-response algorithm and receiving a response and a review of the malice/non-malice of these nodes Makes sure. This challenge can be to send multiple small random packets to the virtual explorers and then examine the reports received by the virtual explorers from these packages.

In the other words, the main responsibility of the network monitoring module is related to collecting data from explorers and sending them to the data combination module. The monitoring module can organize the explorers by involving the task of allocating a new explorer and verifying the explorer nodes. Obviously, the number of packets increases at the time of network congestion and the full monitoring of the network needs more monitoring sources. Detecting the network congestion status can be announced by the congestion detection module or show the network congestion through increasing the number of reports received from explorers at a certain time period. In addition, the network manager can predict more traffic congestion at certain times, which can announce the need for more allocation to the monitoring module through the monitoring controller.

The second task of this module is related to ensuring the accuracy of virtual or real nodes of an explorer, which could be used for responding to the fourth requirements in Section 2. For this purpose, this module could send some challenge-response packets to the data level explorers randomly or at certain times. Here, because the goal is

Table 5: The variables used for describing the network status

The features describing the aspects of DDOS attack	**The considered aspect**
The amount of memory used in the rules table and the queue memory per switch, the packet-in packet rates, the traffic log rate to the network, the entropy of the origin and destination IP address, the type of packet entropy	Congestion in the network and memory overflow in the switch
The IP address and package type	Fake source IP address
Packet Entry Rate and Source IP Address	Botnets

to ensure the accuracy of the virtual explorer and to send as fast and complete information as possible beforehand, these packets can pack small packages with a random IP address and add the legal authority to report these packages to the monitoring module. Then monitoring module can conclude on the accuracy of the virtual explorers by examining the complete report of packet data as well as the speed of this report compared to recent reports. These challenges should be designed in such a way to apply low processing overhead to the explorers. These challenges include the implementation of authentication protocols or requesting a report on a switch. Comparing the new report to the current information could ensure us on the accuracy of the explorer.

5.4 Congestion Detection

The congestion detection module is a research-based [18] that uses entropy to detect congestion. For this purpose, the destination IP addresses of the packets are considered as random variables. It also obtains information about the amount of memory consumed through the monitoring controller that it receives from the network controller. If the variable entropy value of the IP address of the packet destination exceeds a specified value or the amount of memory utilized by the switch is greater than a certain amount, this situation is considered as a bust condition. In case of congestion detection, this module also informs the controller and then informs the network controller and sends the information received from the monitoring module to the traffic separation module to decide whether a DDoS attack occurs/does not occur.

Congestion detection uses two methods to examine the memory consumption of controller-level switches as well as random variable entropy using the IP address of the destination of packet inputs to the network. If the variable entropy value of the IP address of the packet destination exceeds a specified value or the amount of memory utilized by the switch is greater than a certain amount, this situation is considered as a bust condition. In case of congestion detection, this module also informs the controller and then informs the network controller and sends the information received from the monitoring module to the traffic separation module to decide whether a DDoS attack occurs/does not occur.

5.5 Traffic Separation

If requested by the congestion detection module, this module will begin its work and uses the following two methods to identify the streams associated with the DDoS attack. (The explanation of these two methods is explained in more detail below.)

1) Investigating the fakes of source IP addresses [1]: To detect DDoS attacks that are falsified by source IP addresses.

2) Using the Pearson Correlation Coefficient [4]: To detect botnet-based DDoS attacks with real clients.

Packet information is tested in two ways, and if one of the above methods detects inbound inputs, then the current stream is reported as an attack on the controller and then to the network controller.

The Traffic Separation Module will work if the congestion detection module detects congestion on the network. As described above, the congestion detection module, if the variable entropy of the source IP of the packets exceeds a certain rate, or if the use of the switch memory exceeds a certain limit, consider the network status congestion and by sending information Receiving a traffic separation module from the monitoring module to the traffic separation module requires a breakdown of traffic.

The method of examining the falsification of source IP addresses in a handshaking phase by sending a cookie that is not kept on the server side and after completing the handshaking phase by sending specific messages to the client and examining his reaction to these two challenges about the actual or fake address origin of IP decisions. Pearson's method also examines features such as the origin and destination IP address, the number of packets per time interval, and the number of packets sent from each IP address, and if the volume of traffic sent in a stream exceeds the threshold value for a normal traffic flow, this flow is considered a suspicious flow. Then, the correlation coefficient between the currents is calculated and if this value is greater than the threshold of the expected difference for the currents, it is concluded that the denial of the distribution service has occurred and that the flows x and y are due to the similarity of each other among the strikes they take.

Fake checking method for source IP addresses: This research uses the SYN Cookie method with one of the following ways to ensure the authenticity of the source IP address. In the SYN Cookie, server or client-interacting device, in the SYN-ACK response message in the TCP handwriting process, a challenge that is not kept on the server side encodes in the sequence number section. If the client succeeds with an ACK response message containing the correct ACK number, then the server will continue to communicate with the client. After successfully completing this step, the server verifies that the client is the one who is in the following ways (Of course, in the original research, there are four methods out of them, two methods below are ours).

HTTP Redirect: In this way, during the TCP handshaking process, the client request receiver records the client IP address as a legitimate address, but in the response message, the header activates the redirect server address and then terminates the connection. Sending a response packet with the redirect header to the client will cause the real client to re-connect to the server, in which case it will communicate directly with the server. Sending a response packet with the redirect header to the client will cause the real client to re-connect to the server, in which case it will communicate directly with the server.

TCP Reset: This method is similar to the HTTP-Redirect method, with the difference that the server responds to the client with an RST packet, and thus the real client starts a new connection when the connection is disconnected, in which case the real client is detected.

Method of using the pearson correlation] coefficient: The research, using the Pearson correlation coefficient, attempts to detect the traffic associated with distributed denial-of-service denials from high-traffic but legal traffic. The strategy of this research consists of two detection modules and a traffic separation module. In the discovery module, the input traffic is sampled and features such as the origin and destination IP address, the number of packets per time interval, and the number of packets sent from each IP address are extracted. If the number of packets in a T interval is greater than a specified value, an alert signal will be sent to the traffic separation module. Otherwise, traffic is considered legal traffic. In the traffic separation module, the traffic correlation coefficient is calculated and, depending on the calculated value, the traffic generated in the two categories of DDoS attack or the bustle of legal users is divided. This study, by examining different correlation coefficients, introduced the momentary Pearson coefficient as the best option for detecting distributed denial-of-service attacks.

Then, the key variables of the network status, which could be a sign of DDoS attacks, were detected and the tasks of each layer were explained. We will also make suggestions to meet any of the requirements described in this section. The strengths of the suggested solution include:

1) In order to Separate legal traffic from illegal traffic has been used in two different ways in the Traffic Separation module. With the goal, identifying fake packages from real traffic, identifying botnets by examining the pattern of packet access to the network, have been used the proposed methods in [1,4]. Using these two methods simultaneously can cover a variety of attacks.

2) The nodes that work for data-level monitoring are validated using the challenge-response solutions by the monitoring module. By doing so, you can identify malicious internal agents and ensure the accuracy of the information collected.

3) The use of entropy-based methods in the congestion detection Module is much faster than traffic separation methods, and are considered as good alerts for the likelihood of an attack.

6 Conclusion

In the present study, a solution based on SDN and NFV technologies was presented to perform network forensic and detect the DDoS attacks. In this strategy, the entropy-based methods were used as a warning for DDoS attacks and the two methods presented in previous studies were used for separating the allowed traffic from the non-allowed traffic. In addition, NFV technology was used for allocating more sources dynamically. These sources were used for monitoring the network activities and extracting the data for congestion detection and traffic separation modules.

References

[1] Y. Afek, A. Bremler-Barr and L. Shafir, "Network anti-spoofing with SDN data plane," in *Proceedings of IEEE Conference on Computer Communications*, 2017. (`http://www.deepness-lab.org/pubs/infocom17_spoofing.pdf`)

[2] T. Alharbi, A. Aljuhani, H. Liu, "Smart and lightweight DDoS detection using NFV," in *Proceedings of ICCDA*, 2017.

[3] N. Bawany, J. Shamsi and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," *Computer Engineering and Computer Science*, vol. 42, no. 2, pp. 425-441, 2017.

[4] S. Chawla, M. Sachdeva and S. Behal, "Discrimination of DDoS attacks and flash events using pearson's

product moment correlation methods," *International Journal of Computer Science and Information Security*, vol. 19, no. 5, pp. 734-741, 2016.

[5] M. S. Hwang, S. K. Chong and T. Yu. Chen, "DoS-resistant ID-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, pp. 163-172, Jan. 2010.

[6] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[7] A. Jakar, B. Rashidi, M. Rahman, C. Fung and W. Yang, "Dynamic DDoS defense resource allocation using network function virtualization," in *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, 2017. DOI: 10.1145/3040992.3041000.

[8] C. Jin, H. Wang and K. Shang, "Hop-count filtering: An effective defense against spoofed traffic," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 30-41, 2003.

[9] S. Lim, J. Ha, H. Kim, Y. Kim and S. Yang, "A SDN-Oriented DDoS blocking scheme for botnet-based attacks," in *Proceedings of Sixth International Conference on Ubiquitous and Future Networks*, 2014. DOI: 10.1109/ICUFN.2014.6876752.

[10] M. Liyanage, J. Okwuibe, I. Ahmed and M. Ylianttila, "Software defined monitoring (SDM) for 5G mobile backhaul networks," in *Proceedings of IEEE International Symposium on Local and Metropolitan Area Networks*, 2017. (`http://jultika.oulu.fi/files/nbnfi-fe2018080733468.pdf`)

[11] L. López, A. Caraguay, J. Vida, M. Monge and L. Villalba, "Towards incidence management in 5G based on situational awarness," *Future Internet*, vol. 9, no. 1, pp. 3, 2017.

[12] A. Piedrahita, S. Rueda, D. Mattos and O. Carlos, "Flowfence: A denial of service defense system for software defined networking," in *Proceedings of Global Information Infrastructure and Networking Symposium*, 2015. DOI :10.1109/GIIS.2015.7347185.

[13] G. Shang, P. Zhe, X. Bin, H. Aiqun and R. Ku, "FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks," in *Proceedings of IEEE Conference on Computer Communications*, 2017. DOI: 10.1109/INFOCOM.2017.8057009.

[14] S. Shin, V. Yegneswaran, P. Porras and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security*, 2013. (`http://faculty.cs.tamu.edu/guofei/paper/AvantGuard-CCS13.pdf`)

[15] D. Spiekermann and T. Eggendorfer, *Challenges of Network Forensic Investigation in Virtual Networks*, 2017. DOI: 10.13052/jcsm2245-1439.522.

[16] T. Thapngam, S. Yu, W. Zhou and G. Beliakov, "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns," in *Proceedings of IEEE Conference on Computer Communications Workshops*, 2011. (`http://cse.unl.edu/~byrav/INFOCOM2011/workshops/papers/p969-thapngam.pdf`)

[17] T. Thapngam, S. Yu and W. Zhou, "DDoS discrimination by linear discriminant analysis (LDA)," in *International Conference on Computing, Networking and Communications (ICNC'12)*, 2012. DOI: 10.1109/ICCNC.2012.6167480.

[18] M. Todorova and S. Tomova, *DDoS Attack Detection in SDN-based VANET*, 2016. (`https://projekter.aau.dk/projekter/en/studentthesis/ddos-attack-detection-in-sdnbased-vanet-architectures(11020a55-4287-4d8c-a603-b85c8969d9ca).html`)

[19] A. Tayal, N. Mishra and S. Sharma, "Active monitoring & postmortem forensic analysis of network threats: A survey," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 49–59, 2017.

[20] H. Wang, L. Xu and G. Gu, "FloodGuard: A DoS attack prevention extension in software-defined Networks," in *Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2015. DOI: 10.1109/DSN.2015.27.

[21] B. Yuan, D. Zou and S. Yu, "Defending against flow table overloading attack in software-defined networks," *IEEE Transactions on Services Computing*, pp. 231-246, 2016.

[22] M. Zhang, J. Bi, J. Bai, Z. Dong, Y. Li and Z. Li, "FTGuard: A priority-aware strategy against the flow table overflow attack in SDN," in *Proceedings of the SIGCOMM Posters and Demos*, 2017. (`http://netarchlab.tsinghua.edu.cn/~junbi/SIGCOMM2017-3.pdf`)

Biography

Shahrzad Sedaghat received her B.Sc. and M.Sc. degrees in Computer and Information Technology engineering from Yazd University, Iran in 2008 and 2010 respectively, and is currently pursuing her Ph.D. in computer engineering in Sharif University of Technology, Iran. In 2011, she joined the department of computer and information technology engineering, Jahrom University. Her research interests are computer network and security, quality of service and reliability modeling.