Entropy based DDoS Detection and Mitigation in Software Defined Networks

Sanjay M. Vidhani [1*], Amarsinh V. Vidhate [2]

[1] Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, 400706, Navi-Mumbai, India.

*Corresponding author

[2] Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul, 400706 , Navi-Mumbai, India.

***Abstract*: 5G networks handle innovative technical concepts like ultra-high bandwidth, ultra-reliability ultra-low latency and ultra-massive device access in addition to meeting the constantly growing needs of a wide range of applications. Software-defined networking, mobile-access edge computing, network slicing and network function virtualization are examples of developing technologies that could lead to a new class of security vulnerabilities due to Network Softwarization. The security issues that 5G would bring up are highlighted in this paper, which also calls for immediate security solutions. SDN permits networks to monitor the traffic and identify vulnerabilities more effectively.DDoS assaults, Man-in-the-Middle attacks, Saturation attacks and other security risks are introduced when control and data planes are separated. One of the most severe online threat is distributed denial of service (DDoS) attacks. An entropy-based detection method is used in software-defined networks to identify and mitigate DDoS attacks, hence improving network security.**

Keywords:* *5G Networks, Security, Network Softwarization , SDN, NFV, MEC , NS and Entropy.

I. Introduction

The rapid advancement of information technologies has led to the creation of numerous new applications, such as the Mobile Internet, Internet of Things, and Internet of Vehicles. Wireless communications are frequently utilised for these purposes. The number of mobile devices in the world is expected to increase from 8.6 billion in 2017 to 12.3 billion by 2022, resulting in a monthly data flow of 77.5 exabytes from wireless and mobile devices [3]. Future needs will be more than what 4th Generation and older wireless networks can handle, especially when it comes to large Internet of things (IoT) devices, heavy app traffic, and a large number of mobile devices. Currently in use, the 5th Generation network is a crucial component of the upcoming wireless technology and mobile communication. The 5G network has approved a number of novel technologies to support a variety of applications and services, with the aim of attaining ultra-low latency, ultra-reliability, ultra-high bandwidth and ultra-massive device access [3]. The deployment of 5G wireless networks will cause security attack vectors to rapidly increase in number. Beyond the security of 5G networks, there are three main facets to 5G [1]. Firstly , almost every security requirement and challenge outlined above for pre-5G mobile generations equally applies to 5G and later mobile generations. Second, because 5G will require more IoT and mission-critical apps, it will create new security challenges because of its growing user base, a wide range of connected devices, unique network services, growing user privacy concerns, and extra stakeholders. Third, as cutting-edge technologies like software defined networks (SDN), network function virtualization (NFV), mobile-access edge computing (MEC) and network slicing (NS) are introduced and networks become more softwarized, new security issues will arise [1] and [2]. In this paper, we analyse the problems in terms of security and the security solutions that may be used to overcome such issues. The primary aim of the SDN paradigm is to simplify network operations, improve network administration and offer reliability, scalability, and security. Distributed denial of service(DDoS) attacks pose a significant security risk to SDN [22], mostly because they are caused by an attacker sending an excessive amount of traffic packets to the target, which lowers or stops the victim's service and prevents it from being accessible from later connections. Often, these incoming packets source addresses are faked. Entropy is a statistic that is used to assess the randomness or unpredictability of network traffic patterns in SDN for the purpose of DDoS discovery and mitigation. By monitoring and assessing entropy levels, glitches revealing of DDoS attacks can be detected and appropriate mitigation strategies can be employed. The remaining paper is organized as follows. Section II provides a detailed literature review on 5G component security issues. Section III contains 5G components security issues and probable security solutions were examined and analysed. Section IV implements Entropy based DDoS attacks detection and mitigation in SDN. Section V discussed the simulation of detection and mitigation methods in SDN. Section VI explain the results and analysis of security issues and the solutions. Conclusion and future work are drawn in Section VII.

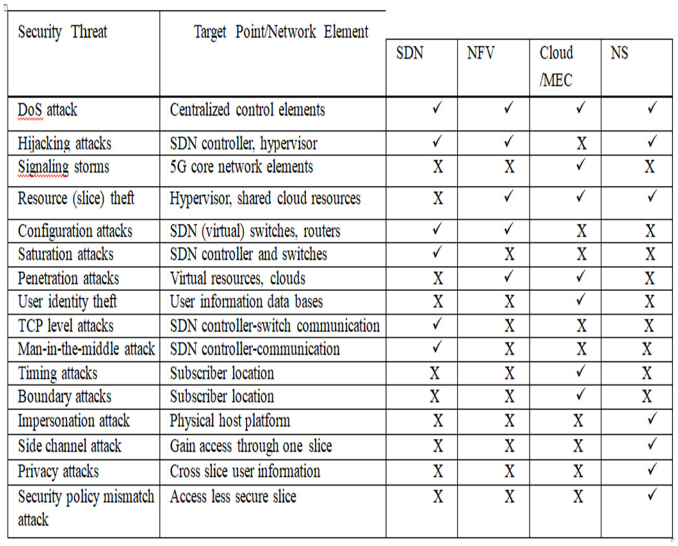
II. RELATED WORK

Rabia Khan et al. [1] explored potential remedies, ongoing developments, and possible future approaches in a survey on the security and privacy of 5G technology. Ijaz Ahmad et al. [2] explore the security solutions for the aforementioned risks as well as the security and privacy challenges of 5G technology. In order to create an automated solution framework for 5G security, Zhihong Tian et al. [3] combine the physical and logical layers to investigate 5G security from the standpoint of automated attack and defence. Jiaying Yao et al. [6] research looks at the security vulnerabilities that come with intelligence centralization in SDN. Authors suggest a strong security architecture for SDN-based 5G networks in order to get over this restriction. The key obstacles to the adoption of 5G are analysed by S. Sullivan A. Brighente et al. [10They include commercial ones like business models and ecosystem maturity, as well as technological ones like mmWave communications, backhaul technology, technical maturity, energy usage, and EMF. In order to safeguard the 5G environment, both new and old technologies are recommended and Alex Mathew [12] offers an objective review of these concerns. Juan Fernando Balarezo et al. [13] state that there are three possible assault levels for attacks that use the transmission control protocol (TCP) SYN, user datagram protocol (UDP), and hypertext transfer protocol (HTTP) : low (Q1), medium (Q2), and high (Q4). The user chooses the characteristics and severity of these attacks. The 5G threat landscape, 5G network classification criteria, and their threat taxonomy are examined by Juan Fernando Balarezo et al. [14]. They also provide a description of the security requirements of 5G systems, broken down into use cases that are specific to different domains. The security risks, difficulties, and methods present in mobile edge computing are examined by Roman [15] et al. Using a stateful SDN data plane allows Jesus Galeano-Brajones et al. [18] to describe how an entropy-based approach can be empirically evaluated for detecting and repelling DoS and DDoS attacks in online environments. For the purpose of enhancing network security in software-defined networks, Sumantra et al. [19] present an entropy-based technique for reducing distributed denial of service assaults. Mahmood Z. Abdullah et al. [20] employ POX controller to develop an entropy-based detection system. They also test the algorithm's performance in various topologies and controller counts using POX controller. Konda Srikar Goud et al. [22] discussed the security challenges and their solutions in Software defined networks. Dinh Thi Thai Mai et al. [23] discussed DDoS detection using dynamic entropy in SDN. Pradeep kumar Sharma et al [24] analyzing the SDN security issues with their countermeasures.

III. SECURITY CHALLENGES & SOLUTIONS

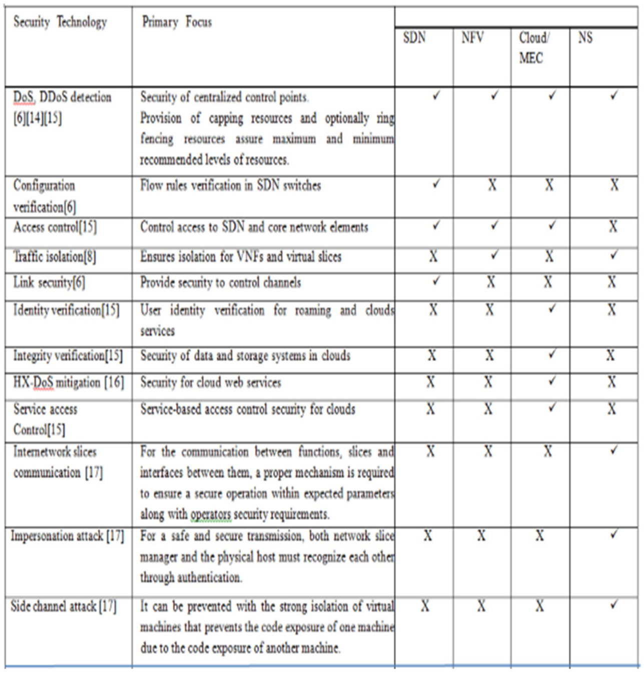
The security risks associated with 5G components and the solutions that need to be implemented were examined and analysed by Sanjay Vidhani et al. [21] in Table [1] and [2].

Table I. 5G Technology's Security Challenges



Security Threat	Target Point/Network Element	SDN	NFV	Cloud /MEC	NS
DoS attack	Centralized control elements	✓	✓	✓	✓
Hijacking attacks	SDN controller, hypervisor	✓	✓	X	✓
Signaling storms	5G core network elements	X	X	✓	X
Resource (slice) theft	Hypervisor, shared cloud resources	X	✓	✓	✓
Configuration attacks	SDN (virtual) switches, routers	✓	✓	X	X
Saturation attacks	SDN controller and switches	✓	X	X	X
Penetration attacks	Virtual resources, clouds	X	✓	✓	X
User identity theft	User information data bases	X	X	✓	X
TCP level attacks	SDN controller-switch communication	✓	X	X	X
Man-in-the-middle attack	SDN controller-communication	✓	X	X	X
Timing attacks	Subscriber location	X	X	✓	X
Boundary attacks	Subscriber location	X	X	✓	X
Impersonation attack	Physical host platform	X	X	X	✓
Side channel attack	Gain access through one slice	X	X	X	✓
Privacy attacks	Cross slice user information	X	X	X	✓
Security policy mismatch attack	Access less secure slice	X	X	X	✓

Table II. 5G Technology's Security Solutions



Security Technology	Primary Focus	SDN	NFV	Cloud/ MEC	NS
DoS, DDoS detection [6][14][15]	Security of centralized control points. Provision of capping resources and optionally ring fencing resources assure maximum and minimum recommended levels of resources.	✓	✓	✓	✓
Configuration verification[6]	Flow rules verification in SDN switches	✓	X	X	X
Access control[15]	Control access to SDN and core network elements	✓	✓	✓	X
Traffic isolation[8]	Ensures isolation for VNFs and virtual slices	X	✓	X	✓
Link security[6]	Provide security to control channels	✓	X	X	X
Identity verification[15]	User identity verification for roaming and clouds services	X	X	✓	X
Integrity verification[15]	Security of data and storage systems in clouds	X	X	✓	X
HX-DoS mitigation [16]	Security for cloud web services	X	X	✓	X
Service access Control[15]	Service-based access control security for clouds	X	X	✓	X
Internetwork slices communication [17]	For the communication between functions, slices and interfaces between them, a proper mechanism is required to ensure a secure operation within expected parameters along with operators security requirements.	X	X	X	✓
Impersonation attack [17]	For a safe and secure transmission, both network slice manager and the physical host must recognize each other through authentication.	X	X	X	✓
Side channel attack [17]	It can be prevented with the strong isolation of virtual machines that prevents the code exposure of one machine due to the code exposure of another machine.	X	X	X	✓

IV. IMPLEMENTATION

Many DDoS detection methods exist, including machine learning, entropy-based, traffic pattern analysis, and connection rate-based methods [19]. DDOS attacks can take many different forms, such as flooding the Transmission Control Protocol (TCP), reflection of the Domain Name System (DNS), ping of death, flooding of the Hypertext Transfer Protocol (HTTP), flooding of the Synchronise (SYN) protocol, and more. However, User Datagram Protocol (UDP), TCP SYN, ICMP, and HTTP flooding are the DDoS attacks that are most frequently employed. All of these attacks share the trait of overwhelming the victim with traffic volumes and depleting its resources.

A. *Shannon's Entropy*

Entropy is a tool to measure the network randomness. The entropy value will increase with the randomness value and vice versa. This suggests that we should consider the network to be under attack if the computed entropy value is less than a specified threshold value. A measure of an event's uncertainty or unpredictability is Shannon's entropy [19, 20]. The destination IP address is found by looking at the header of each new Packet_In message that enters the network. This information is then entered into a hash table along with the address's frequency. Equation (1) can be used to represent the hash table, where W stands for a window with n items (n = 50), x for the destination IP address, and y for the number of times it appears. Equation (2) is used to calculate the probability for each destination IP address, where P(xi) represents the likelihood of that specific IP in Window W.

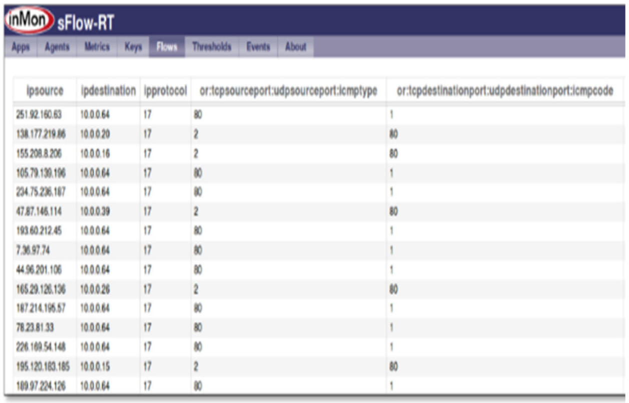
$$W = \{(x1, y1), (x2, y2), ...,(xn, yn)\} \qquad (1)$$
$$P(xi) = yi/N \qquad (2)$$
$$N = y1 + y2 + y3 + y4 +........ + yn \qquad (3)$$

Where N is the total number of requests that were made during that specific window of time. The following formula is used to determine the Entropy for each Source_IP during the specified time frame.

$$E(X) = \sum i{=}0 -P(xi)\log2P(xi) \qquad (4)$$

B. *Detection and Mitigation*

Every host on the network receives packets with spoof IP addresses during normal network traffic. The target host (H64), which has the IP (10.0.0.64), receives all packets from the spoof IP addresses when they are in the attack flow. Attack traffic is more frequent than normal traffic, and all of its packets are UDP kinds. Network traffic is tracked with the SDN traffic monitoring tool Sampled Flow-Real Time (sFlow-RT). As seen in Figure 1, all experiments will run both attack and ordinary traffic concurrently to see how the entropy detection method responds to each type of traffic.



ipsource	ipdestination	ipprotocol	or:tcpsourceport:udpsourceport:icmptype	or:tcpdestinationport:udpdestinationport:icmpcode
251.92.160.63	10.0.0.64	17	80	1
138.177.219.86	10.0.0.20	17	2	80
155.208.8.206	10.0.0.16	17	2	80
105.79.139.196	10.0.0.64	17	80	1
234.75.236.187	10.0.0.64	17	80	1
47.87.146.114	10.0.0.39	17	2	80
193.60.212.45	10.0.0.64	17	80	1
7.36.97.74	10.0.0.64	17	80	1
44.96.201.106	10.0.0.64	17	80	1
165.29.126.136	10.0.0.26	17	2	80
187.214.195.57	10.0.0.64	17	80	1
78.23.81.33	10.0.0.64	17	80	1
226.169.54.148	10.0.0.64	17	80	1
195.120.183.185	10.0.0.15	17	2	80
189.97.224.126	10.0.0.64	17	80	1

Figure 1. Normal and attack traffic flow

As mentioned above, in order to detect any unusual activity, the entropy for packets within a given time period is calculated. The following fields Source_IP address, TCP flags, and the quantity of packets and requests sent per second are used in our suggested methods to compute entropy. Entropy falls dramatically during an attack because, in contrast to a non-attack scenario, there is less randomness. The entropy of each time window is continuously calculated and shown in Table [3] by the system, and if a certain Source's entropy is determined to be below the threshold for three consecutive time windows, it is isolated and designated as a botnet host. The rate drop of entropy also indicates that the higher the attack rate, the lower the entropy value [23].

Table III. Entropy Calculation

Sr. No.	Random variables and their occurrence	Probability	Entropy Value
1	Suppose 5 sources are attacking on destination IP address 10.0.0.64 window size 50. xi=yi/N =5/50=0.1	P(xi)=0.1	E(x) =∑i=0 −P(xi)log2P(xi) Where log2(0.1)=-3.32 E(x)=-0.1*-3.32=0.332
2.	Suppose 10 sources IP address are attacking on destination IP address 10.0.0.64 window size 50. xi=yi/N =10/50=0.2	P(xi)=0.2	E(x) =∑i=0 −P(xi)log2P(xi) Where log2(0.2)=-2.32 E(x)=-0.2*-2.32=0.464
3.	If 49 sources attacking on single destination IP address 10.0.0.64 window size 50. xi=yi/N =49/50=0.98	P(xi)=0.98	E(x) =∑i=0 −P(xi)log2P(xi) Where log2(0.98)=-0.029 E(x)=-0.98*-0.029=0.028
4.	If all sources attacking on single destination IP address 10.0.0.64 window size 50. xi=yi/N =50/50=1	P(xi)=1	E(x) =∑i=0 −P(xi)log2P(xi) Where log2(1)=0 E(x)=-1*0=0

A suitable mitigation approach is implemented as soon as a botnet host is identified. The goal of this study is to permanently block the IP addresses of the hosts within the identified botnet. The effect of the distributed denial of service attack on the network will be reduced as a result of their inability to communicate with the server in the future. The suggested Distributed Denial of Service attack discovery and reduction strategy is carried out by the controller, as shown by the flowchart in Figure 2.

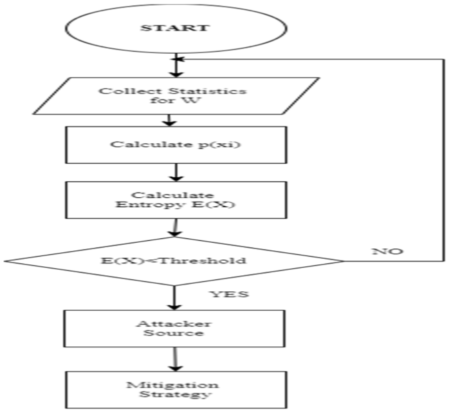


Figure 2. Process inside the controller

V. SIMULATION

To evaluate our approaches, the topology is replicated using the Mininet Simulator. Several experiments have been carried out to verify the Entropy detection technique. The network configuration utilized in the first experiment is depicted in Figure 3, where a single topology consisting of 64 hosts (H1-H64) and one switch (S1) was connected to the POX controller (C0).

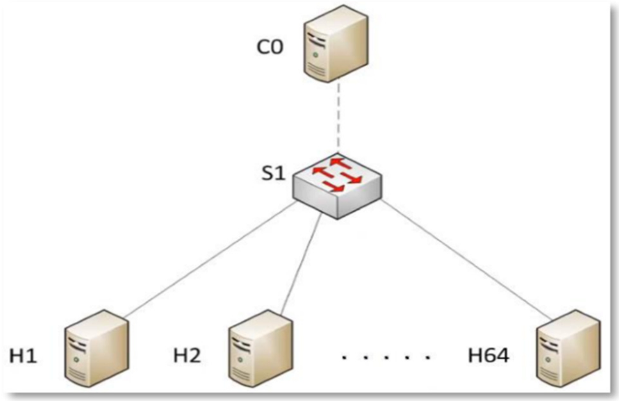
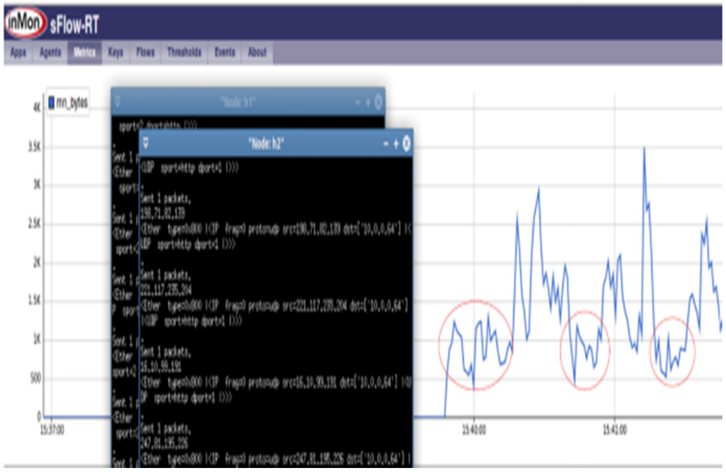


Figure 3. Mininet Topology

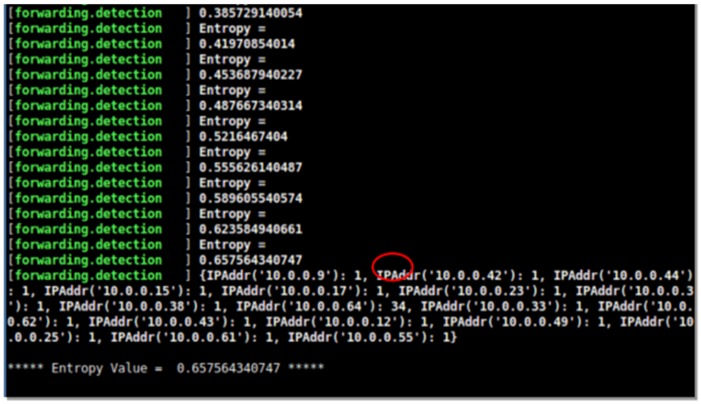
This section displays the findings from several experiments conducted on the POX controller using the entropy detection approach. The entropy value in these tests will drop while both normal and attack traffic is occurring because destination IP 10.0.0.64 is more common than other destination IPs during the course of the duration. Only regular traffic from H1 is permitted to go, while the packets from H2 are blocked when it drops below the threshold three times in a row, which is considered an attack. The window's entropy value will be zero if there are more attack packets than regular traffic. This is due to the fact that there will be 50 packets in the timeframe that have the same destination IP (10.0.0.64). Since the probability of that IP is (50/50), or 1, there will be zero entropy in this scenario, which is below the threshold and will result in the port being blocked. Figure 4 displays the combined attack and normal traffic that sFlow-RT was able to capture. The amount of bytes resumes its usual traffic rate once the algorithm has detected the assault flow.



```
<UDP  sport=http dport=1 |>>>
.
Sent 1 packets,
198.71.82.139
<Ether  type=0x800 |<IP  frag=0 proto=udp src=198.71.82.139 dst=['10.0.0.64'] |<
UDP  sport=http dport=1 |>>>
.
Sent 1 packets,
221.117.235.204
<Ether  type=0x800 |<IP  frag=0 proto=udp src=221.117.235.204 dst=['10.0.0.64']
|<UDP  sport=http dport=1 |>>>
.
Sent 1 packets,
16.10.99.191
<Ether  type=0x800 |<IP  frag=0 proto=udp src=16.10.99.191 dst=['10.0.0.64'] |<U
DP  sport=http dport=1 |>>>
.
Sent 1 packets,
247.81.135.226
<Ether  type=0x800 |<IP  frag=0 proto=udp src=247.81.135.226 dst=['10.0.0.64'] |
```

Figure 4. Captured Traffic

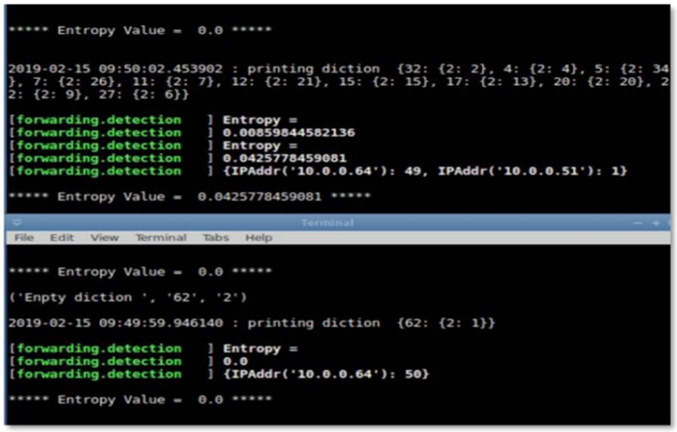
Figures 5 and 6 display a window of 50 packets. Attack traffic has caused the destination IP (10.0.0.64) to have more occurrences than usual, resulting in an entropy value below the threshold value.



```
[forwarding.detection    ] 0.385729140054
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.41970854014
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.453687940227
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.487667340314
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.5216467404
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.555626140487
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.589605540574
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.623584940661
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.657564340747
[forwarding.detection    ] {IPAddr('10.0.0.9'): 1, IPAddr('10.0.0.42'): 1, IPAddr('10.0.0.44')
: 1, IPAddr('10.0.0.15'): 1, IPAddr('10.0.0.17'): 1, IPAddr('10.0.0.23'): 1, IPAddr('10.0.0.3
'): 1, IPAddr('10.0.0.38'): 1, IPAddr('10.0.0.64'): 34, IPAddr('10.0.0.33'): 1, IPAddr('10.0.
0.62'): 1, IPAddr('10.0.0.43'): 1, IPAddr('10.0.0.12'): 1, IPAddr('10.0.0.49'): 1, IPAddr('10
.0.0.25'): 1, IPAddr('10.0.0.61'): 1, IPAddr('10.0.0.55'): 1}

***** Entropy Value =  0.657564340747 *****
```

Figure 5. Output Detection



```
***** Entropy Value =  0.0 *****


2019-02-15 09:50:02.453902 : printing diction  {32: {2: 2}, 4: {2: 4}, 5: {2: 34
}, 7: {2: 26}, 11: {2: 7}, 12: {2: 21}, 15: {2: 15}, 17: {2: 13}, 20: {2: 20}, 2
2: {2: 9}, 27: {2: 6}}

[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.00859844582136
[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.0425778459081
[forwarding.detection    ] {IPAddr('10.0.0.64'): 49, IPAddr('10.0.0.51'): 1}

***** Entropy Value =  0.0425778459081 *****
```

```
***** Entropy Value =  0.0 *****

('Enpty diction ', '62', '2')

2019-02-15 09:49:59.946140 : printing diction  {62: {2: 1}}

[forwarding.detection    ] Entropy =
[forwarding.detection    ] 0.0
[forwarding.detection    ] {IPAddr('10.0.0.64'): 50}

***** Entropy Value =  0.0 *****
```

Figure 6. Output Detection1

Figure 7 illustrates how central processing unit (CPU) utilization increased during the attack. It displays the CPU's near-maximum performance. According to the observation, the system's performance progressively degrades.

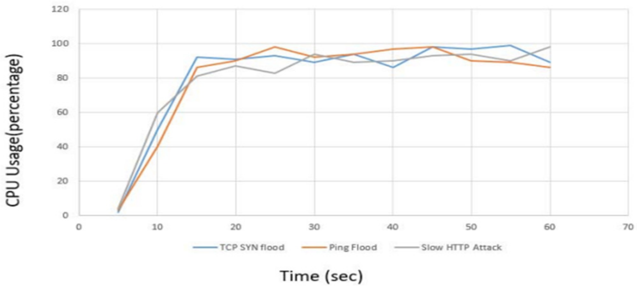


Figure 7. CPU Utilization

The entropy is calculated appropriately as soon as the controller starts collecting statistics for the specified time period. Figure 8 shows how the entropy decreased during the attack's 20-second time frame.

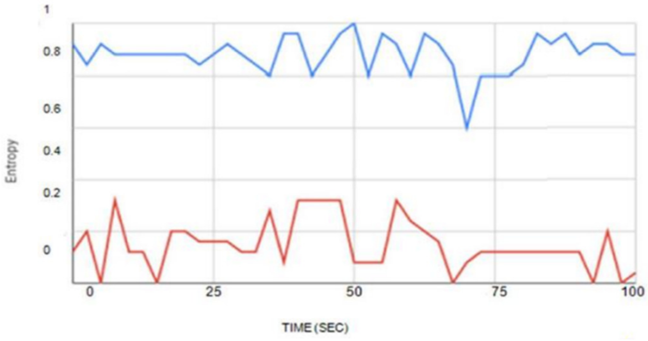


Figure 8. Entropy during attack

SDN is the foundation of many DDoS protection techniques. In SDN networks, mitigating techniques including traffic redirection, port blocking, and packet dropping are frequently utilized and extensively implemented. By installing new or editing existing flow entries and delivering flow-mod messages to its switches, SDN can enforce these strategies.

The controller notifies the switch to add a new entry to stop the attack when the new item in the flow table matches the packets that are initiating the assault with the same source IP, destination IP, source port, and destination port. Dropping these packets is the directive for this flow entry. The attacker IP address and source port would be 192.168.100.101 and 40, the target IP address and port would be 10.0.0.64 and 80, and the source IP address and port values would be 192.168.100.101 and 40, respectively, in the flow rule. Figure 9 shows how this affected the attacker's traffic flow. As seen, the bandwidth used by H2 traffic is essentially nonexistent prior to the attack, but increases significantly as soon as the attack commences. After the attack is neutralized, the switch discards all packets associated with the malicious flow, resulting in nearly negligible bandwidth.

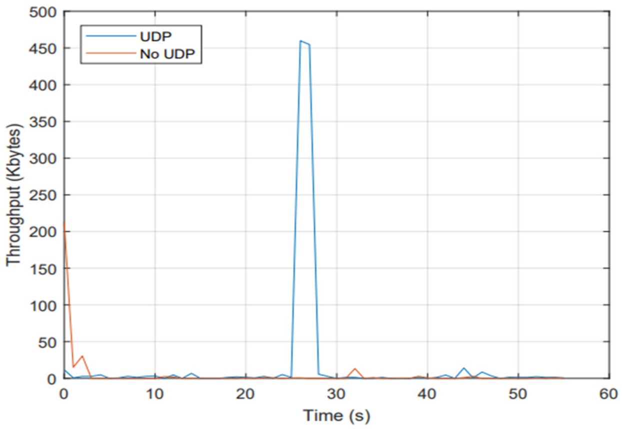


Figure 9. Throughput during attack

VI. RESULTS AND ANALYSIS

The findings of an analysis of security issues and how to resolve them for 5G components are shown in Tables No. 2 and 3 [21]. DoS and DDoS assaults are the most dangerous to counter because they disrupt the target by continuously attempting to connect for a long time, which can lead to a crash or rapid operation. For instance, several techniques are created in SDN to quickly identify and counteract DDoS attacks and to improve network security [18].

Defense strategy and statistical analysis are the foundations of the first approach. This protection needs to collect and examine samples of network data in order to identify malicious activity. Various metrics, including entropy [19, 20], standard deviation, adaptive correlation analysis, and sample chi-square statistic computation, are employed in the development of statistical algorithms to classify a flow as either legitimate or an assault. The defined policy of the switch, which indicates which flows are dangerous and which can be routed, serves as the foundation for defense. To launch a malicious DDoS assault, the second method is an excellent way to assess and classify distinct flows using machine learning algorithms. The third approach deploys services that enhance network element capabilities through the use of NFV, making it possible to identify and reduction of DDOS attacks.

VII. CONCLUSION AND FUTURE WORK

We need to understand 5G networks architecture and hierarchical structure. The 5G network aims to achieve several goals, including ultra-high bandwidth, ultra-reliability, ultra-low latency and ultra-massive device access. Several cutting-edge technologies are also authorised to offer an extensive array of services and applications. In order to solve problems with affordability, flexibility, and massive connectivity, 5G will make use of SDN, NFV, MEC and NS. These technologies offer a lot of benefits, but there are also a lot of security threats. Thus, in this research, we have concentrated on the critical security flaws that could become more harmful in 5G if they are not adequately addressed. We have talked about fixes for those problems as well as recommended security precautions. Because 5G is still being implemented both separately and in combination, it is not yet possible to completely describe the safety threat vectors. Future security difficulties can be avoided, though, if these considerations are made from the start of design until deployment. To increase network security, several SDN technologies are also taken into account for DDoS attack detection and mitigation. When an entropy value is below a threshold, an entropy detection algorithm will identify it, block attack packets, and retain only safe packets.

The capabilities of DDoS detection and mitigation in SDN can be greatly improved by future research and development by concentrating on improved entropy calculation techniques, artificial intelligence (AI) and machine learning (ML) integration, real-time DDoS detection and response, advanced mitigation techniques and Network Slicing. This will guarantee the security and reliability of next-generation networks.

REFERENCES

[1] Rabia Khan, Pardeep Kumar, Dushantha Nalin K. Jayakody and Madhsanka Liyanage," A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," IEEE Communications Surveys & Tutorials, 2020.

[2] Ijaz Ahmad, Tanesh Kumar , Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila and Andrei Gurtov , "5G Security: Analysis of Threats and Solutions," In Standards for Communications and Networking (CSCN), 2017 IEEE Conference on IEEE, 2017.

[3] Zhihong Tian, Yanbin Sun, Shen Su, Mohan Li, Xiaojiang Du and Mohsen Guizani," Automated Attack and Defense Framework for 5G Security on Physical and Logical Layers," arXiv Feb-2019.

[4] S. Zhang, "An Overview of Network Slicing for 5G," IEEE Wireless Communications, 2019.

[5] Xinsheng JI, Kaizhi HUANG, Liang JIN, Hongbo TANG, Caixia LIU, Zhou ZHONG, Wei YOU, Xiaoming XU, Hua ZHAO, Jiangxing WU and Ming YI," Overview of 5G security technology," Science China Inf Sci, 2018.

[6] Jiaying Yao, Zhigeng Han, Muhammad Sohail and Liangmin Wang , "A Robust Security Architecture for SDN-Based 5G Networks," MDPI/journal/ future internet, 2019.

[7] Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi and Andrew Hinesd,"5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," Elsevier, 2019 press.

[8] Andres J. Gonzalez, Jose Ordonez Lucena, Bjarne E. Helvik, Gianfranco Nencioni, Min Xie, Diego R. Lopez and Pal Gronsund," The Isolation Concept in the 5G Network Slicing," European Conference on Networks and Communications (EuCNC):Network Softwarisation (NET), 2020.

[9] Morteza Taheribakhsh, Amir Hossain Jafri and Mahdi Moazzami Peiro, "5G Implementation: Major Issues and Challenges," 25th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran, 2020.

[10] S. Sullivan A. Brighente, S. Kumar and Conti, "5G Security Challenges and Solutions: A Review by OSI Layers," IEEE Access 2021.

[11] Grant Millar, Anastasios Kafchitsas and Orestis Mavrooulos , "5G Security: Current Status and Future Trends," Inspire-5G consortium 2020.

[12] Alex Mathew, "Network Slicing in 5G and the Security Concern," ICCMC-2020, IEEE Xplore -2020.

[13] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture an Emerging Technologies," IEEE Access, vol. 3, pp. 1206–1232, 2015.

[14] Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al – Hourani and Sithamparanathan Kandeepan, "A survey on DoS / DDoS Attacks Mathematical modeling for traditional, SDN, and virtual networks," Engineering Science and Technology, an International Journal, Sept-2021.

[15] R. Roman, J. Lopez and M. Mambo, "Mobile Edge Computing, Fog: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, 2016.

[16] A. Chonka and J. Abawajy, "Detecting and Mitigating HX- DoS Attacks against Cloud Web Services," In 2012, 15th International Conference on Network-Based Information Systems, Sept 2012.

[17] Ramraj Dangi, Akshay Jadhav, Gaurav Choudhary, Nicola Dragoni Manas Kumar Mishra and Praveen Lalwani, "ML-Based 5G Network Slicing Security: A Comprehensive Survey," Future Internet-2022.

[18] Jesus Galeano-Brajones, Javier Carmona-Murillo, Juan F. Valenzuela-Valdes and Francisco Luna-Valero, "Detection and Mitigation of DoS And DDoS attacks in IoT-based stateful SDN: An experimental approach," Sensors-2020.

[19] I Sumantra, Dr. S. Indira Gandhi, "DDOS attack detection and mitigation in SDN," IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), 2020

[20] Mahmood Z. Abdullah, Nasir A. Al-awad, Fatima W. Hussein," Implementation of Entropy-based Distributed Denial of Service Attack Detection Method in Multiple POX Controllers", IIETA , Vol 6, No. 2, June 2019

[21] Sanjay M. Vidhani, Amarsinh V. Vidhate , "Security Challenges in 5G Network: A technical features and analysis," IEEE International Conference on Advances in Science and Technology (ICAST), 2022

[22] Konda Srikar Goud, Srinivasa Rao Gidituri, "Security Challenges and Related Solutions in Software Defined Networks: A Survey", International Journal of

Computer Networks and Applications (IJCNA), 9(1), PP: 22-37, 2022, DOI: 10.22247/ijcna/2022/211595.

[23] Dinh Thi Thai Mai, Nguyen Tien Dat, Pham Minh Bao, Can Quang Truong, Nguyen Thanh Tung, "DDOS ATTACKS DETECTION USING DYNAMIC ENTROPY IN SOFTWARE-DEFINED NETWORK PRACTICAL ENVIRONMENT", International Journal of Computer Networks and Communications (IJCNC), DOI:10.5121/ijcnc/2023/15307.

[24] Pradeep kumar Sharma, Dr. S.S.Tyagi, "Security enhancement in Software Defined Networking: A Thread Model", International Journal of Advanced Computer Science and Applications " , (IJACSA), Vol 12, No. 9 , 2021

Authors Profiles

Sanjay Vidhani (Research Scholar) : Received his M.E degree at Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul , Navi Mumbai. He is working as Assistant Professor in the Department of Information Technology of K.J.Somaiya College of Engineering, Vidyavihar, Mumbai . He is currently pursuing Ph.D. at Department of Computer Engineering, Ramrao Adik Institute of Technology, Nerul , Navi Mumbai, India. Research area includes Network Security, Computer Networks , Software Defined Networks and 5G applications etc

Amarsinh Vidhate (Mentor) : Prof & Head, Dept. of Computer Engineering Ramrao Adik Institute of Tech, D Y Patil University, Nerul, Navi Mumbai, India. He received Ph.D degree from Mukesh Patel School of Technology and Management at NMIMS University in Mumbai. Research interest includes Protocol Stacks, Mobile and Wireless Networking, VaNET, IOT, 5G Applications, AI and ML , Data science etc