Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210218

Distributed Denial of Service Attacks Detection and Mitigation in Software Defined Mesh Networks

Santosh Mani [a, 1], Manisha J Nene [a]
[a] *Department of Computer Science and Engineering, Defence Institute of Advanced Technology (DU) Girinagar, Pune - 411025, India*

Abstract. Networks configured in Mesh topology provide Network security in the form of redundancy of communication links. But redundancy also contributes to complexity in configuration and subsequent troubleshooting. Critical networks like Backbone Networks (used in Cloud Computing) deploy the Mesh topology which provides additional security in terms of redundancy to ensure availability of services. Distributed Denial of Service attacks are one of the most prominent attacks that cause an immense amount of loss of data as well as monetary losses to service providers. This paper proposes a method by which using SDN capabilities and sFlow-RT application, Distributed Denial of Service (DDoS) attacks is detected and consequently mitigated by using REST API to implement Policy Based Flow Management through the SDN Controller which will help in ensuring uninterrupted services in scenarios of such attacks and also further simply and enhance the management of Mesh architecture-based networks.

Keywords. DDoS attacks, SDN, Attack detection and mitigation, Flow Tables, sFlow-RT, sFlow Agent, sFlow Collector, Policy Based Flow Management (PBFM).

1. Introduction

DDoS attacks on Next Generation Networks (NGNs) leads to serious consequences for critical users like Defence networks and Cloud computing networks with the Core/Backbone infrastructure in a Mesh topology for redundancy against failures to ensure uninterrupted services. Intelligent systems like Internet of Things (IoTs) use Cloud computing environments for data transmission and reception but security measures lacunae and IoT devices easy accessibility cause the Cloud network to be compromised and exploited [33]. Examples of highly impactful DDoS attacks include Estonia attack[6], Sweden Transportation network attack [6], US Department of Health and Human Services (HHS) [7] website attack, *Dyn attack* on high-profile websites such as GitHub, Twitter, Reddit, Netflix, Airbnb and many others [33].With the Covid-19 pandemic crisis, Digital Platform utilisation has skyrocketed to a new high, opening up new avenues for malicious attacks like DDoS. As of 2020, recovery from DDoS attacks takes around four hours [4]. DDoS attacks continue to grow in various dimensions like size (bandwidth), frequency of attack, complexity of attack which threaten and businesses and service providers all over the world.

[1] Santosh Mani, Department of Computer Science and Engineering, Defence Institute of Advanced Technology, Email: santorajim@gmail.com.

In this paper a method by utilizing the SDN capability of Policy Based Flow Management (PBFM) with sFlow-RT application has been proposed for detection and mitigation of DDoS attacks for Full Mesh Networks. DDoS attacks, its classification and the related literature review is given in Section 2. A description of SDN Core concept, flow table concept and sFlow-RT tool utilised is given in Section 3. Section 4 gives the description of the proposed methodology to detect and mitigate DDoS attacks. Section 5 presents the experimentation carried out and the observations. Section 6 concludes the paper and explains how SDN helps in better detection and mitigation of DDoS attack while opening up further scope for better troubleshooting of affected links. In this paper the proposed methodology using SDN capabilities has been implemented for Layer 3 and Layer 4 of the OSI layer.

2. Related work – DDoS attacks and classification, literature review

A brief description of types of DDoS attacks [8] and its classification is discussed here along with related literature review for enhancing the network security.

The DDoS attacks are classified as follows [9] [10] [11]: -

Volume based attacks – Overwhelming a resource (server's website) with a huge amount of traffic to prevent access, e.g., UDP flood/reflection attack, ICMP flood.

Protocol attack – Involves exploiting a protocol's weakness, e.g., TCP SYN attack.

Application layer attacks -Used to take down web servers. Also called Layer 7 (OSI Layer 7) or Application layer attack. In this paper, Volume based attack and Protocol attack have been utilised to demonstrate DDoS attacks detection and mitigation in SDN based Mesh Networks.

A review of literature addressing the challenges of DDoS attacks by leveraging SDN capabilities is as follows:

A proposed solution for detecting and mitigating DDoS attack for a tree architecture [11] was the main motivation for developing a DDoS Attack detection and mitigation mechanism in SDN for a Mesh Network which would prove extremely beneficial for Cloud Computing and Cloud based Services. An efficient anomaly detection and mitigation by firewall implementation in all network devices is proposed in [12]. Detection and mitigation of DDoS attacks in Legacy networks is given in [13] and for SDN environments is proposed in [16]. A comprehensive study in existing and new proposed techniques for DDoS attack detection and mitigation are discussed in [14],[15].

3. Preliminaries

3.1. Sdn Core concept and Flow table concept

SDN separates the Control Plane (network environment discovery) from Data Plane (Data/traffic flow) and places the network intelligence at a centralised location called Controller [1][2][18][19][20][21][34]. SDN utilises Flows present in Flow Tables of forwarding network devices in SDN to route packets. A Flow entry/Flow in a Flow Table is a set of packet field values (Figure 1.) which have a match (filter) criterion and a set of instructions / actions which help in formulating policies for services implemented in the Application Layer.

Figure. 1. Flow entry

3.2. sFlow-RT

sFlow is a sampling technology and can be embedded in switches and routers and continuously monitors traffic flows on all interfaces of networks devices simultaneously [3][21][22][23][24][25][26]. It has two components sFlow Collector and Analyser (Central data collector which analyses the sampled traffic sent by the sFlow Agent) and sFlow Agent (embedded in a switch/router or function as a standalone probe).The sFlow-RT analytics engine receives a continuous telemetry stream from sFlow Agents in network devices, hosts and applications and converts the raw measurements into actionable metrics, accessible through the RESTflow API to configure customized measurements, retrieve metrics, set thresholds, and receive notifications [24]. sFlow-RT detects anomalies in traffic and uses RESTflow API to inform the SDN controller to undertake the mitigation actions. [24]

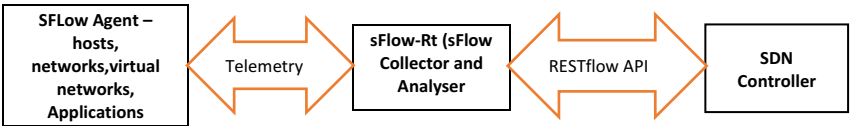

Figure. 2. Logical connectivity between sFlow-RT and SDN Controller

4. Methodology

The methodology proposes the utilization of SDN's PBFM to provide a solution for DDoS attacks detection and mitigation for Full Mesh Networks by combining sFlow-RT (sFlow Agent, sFlow Collector and Analyser) which monitors and using RESTflow API transmits the information to the Controller which then manipulates Flow Table entries in the concerned network devices in a particular flow/path.

4.1. DDoS attack scenario: Detection and mitigation methodology

The logic (Figure 3) of the DDoS Attacks detection and mitigation has been built over the underlaying base Mesh network using routing protocol Shortest Path First (SPF) with Link-failure and Link-flapping detection and mitigation incorporated [34].

First the Controller and mesh network topology are activated with Link-failure and Link-flapping detection and mitigation logic in the background. Next, the threshold is set for DDoS attacks detection on number of traffic packets being sent from a host. Then, the key parameters to classify the DDoS attack type are set. In this paper, three kinds of threat scenarios – UDP reflection, ICMP flood and TCP SYN attack are studied.

After the DDoS attack is initiated, the threshold limit is checked. If crossed, using the defined key parameters, the attack type is identified from the packet samples taken using sFlow-RT. Then based on malicious attacker connected, the router/switch is identified. Flow entries are made in the identified router/switch for that particular

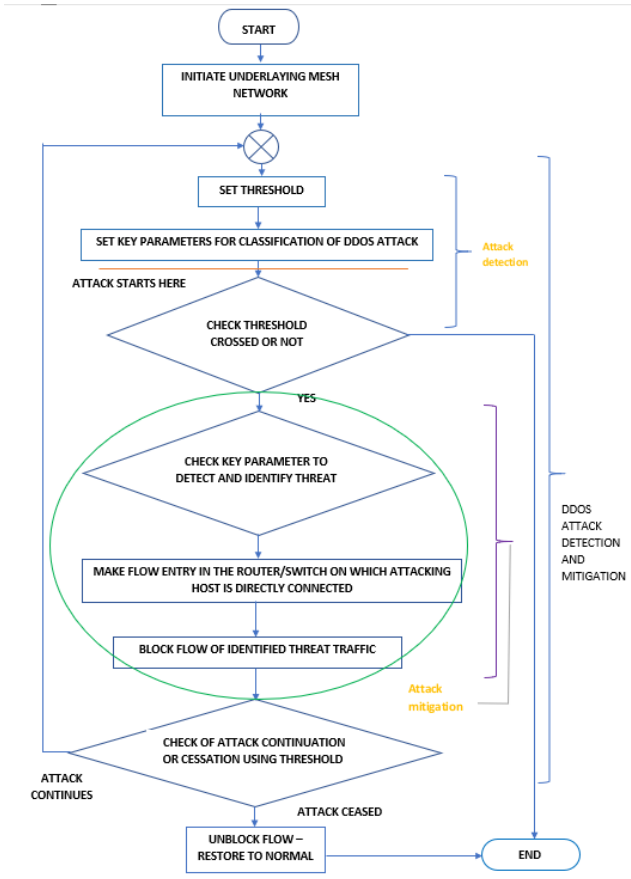

Figure. 3. Methodology for detection and mitigation of DDoS Attacks

attack type to block the flow of threat traffic. The logic applied further to distil the traffic based on each type of attack is given below in this section as test cases.

The logic for intermittent check to see whether the attack traffic is in progress or has ceased is additionally implemented so that once the attack has stopped, the flow is restored to normal, else if not, the detection and mitigation cycle will repeat.

4.2. Test cases for different types of DDoS attacks: -

The logic applied is as follows for the three cases (Figure 4): -

Case 1: UDP reflection attack detection and mitigation logic. First, threshold limit is checked for all the cases. If threshold is crossed and UDP reflection attack traffic is detected and identified based on keys ‘ip destination’ and ‘udp source port’ a flow entry with the filters as the key parameters to stop the flow of attack traffic is made to stop the UDP reflection DDoS attack. If the attack is not identified as UDP reflection attack traffic then the logic shifts to the next attack ICMP flood attack.

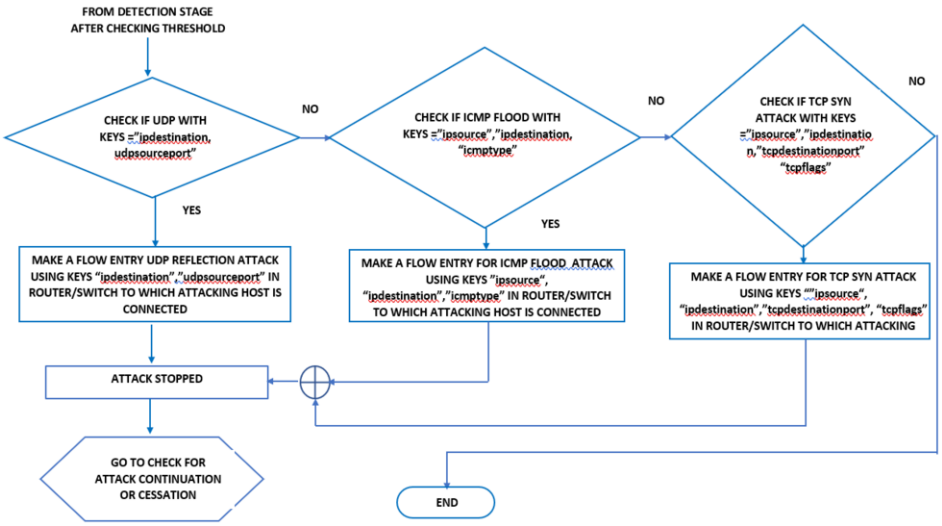

Figure. 4. Test cases for DDoS attacks

Case 2: ICMP flood attack detection and mitigation logic. If threshold is crossed and ICMP flood traffic is detected and identified based on the keys 'ip source', 'ip destination' and 'icmp type' a flow entry with the filters as the key parameters is made to stop the ICMP flood DDoS attack. If the attack is not identified as ICMP flood attack traffic then the logic shifts to the next attack TCP SYN attack.

Case 3: TCP SYN attack detection and mitigation logic. If the threshold is crossed and TCP SYN attack is detected and identified based on the keys 'ip source', 'ip destination','tcp destination port' and 'tcp flags' a flow entry with the filters as the key parameters is made to stop the TCP SYN DDoS attack. If the attack is not identified as TCP SYN attack traffic, then the logic shifts back to the next step in detection and mitigation methodology (Figure 3)

5. Experiments and Observations

This section describes the experimentation carried out to realise the proposed concepts in the previous section. The mesh topology (Figure 5) has been made in Mininet [27][31][32] and RYU controller utilised for controlling and managing the network. Underlaying routing protocol is SPF with Link-failure and Link-flapping detection and mitigation capability [34]. Attacks are carried out using packet crafter tool *hping3*. sFlow-RT detects anomalies in traffic for DDoS attack detection and uses RESTflowf API to inform the SDN controller to undertake the mitigation actions [28][29][30]. The same topology when viewed from sFlow-RT dashboard is shown in Figure 6.

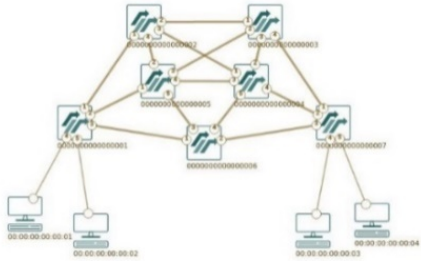

Figure. 5. Topology for experiment

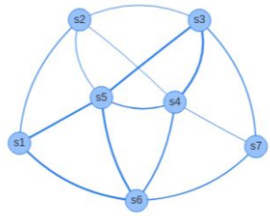

Figure. 6. Topology as seen in sFlow-RT

Following is the illustration of the sequence of events executed during the experimentation: -

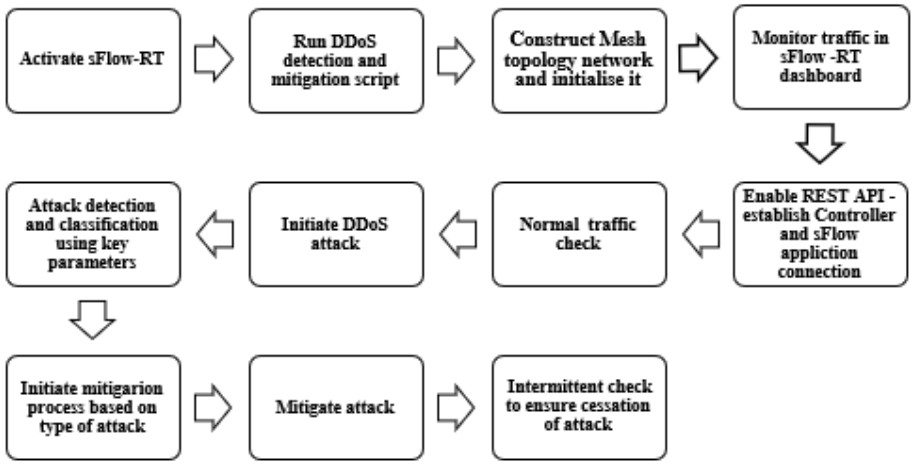

Figure. 7. Experimentation steps

First, the sFlow-RT application for monitoring and analysing the sampled data is activated. The next important step is to initialise and activate the DDoS attack detection and mitigation script. This script is responsible for Setting the threshold which is monitored by the sFlow-RT application, Setting the parameters for classifying the type of DDoS attack, Utilising the sampled data packet taken by the sFlow-RT to identify and detect the attack and Using RESTflow API to carry out DDoS attack mitigation by Policy Based Flow Management.

Next the Mesh topology is initialised and activated with SPF routing protocol and the sFlow-RT traffic monitoring dashboard is started along with enabling REST API connection between Controller and sFlow-RT application. A normal traffic check is carried out to ascertain the working of the sFlow-RT application.

Next, DDoS attack is initiated. Three different types of attacks i.e., UDP reflection attack, ICMP flood attack and TCP SYN attack are utilised for experimentation. The sFlow-RT keeps monitoring the threshold. Once the threshold is crossed, the key parameters in the packets are checked to determine the attack traffic type whether it is UDP reflection attack packets, ICMP flood attack packets or TCP SYN attack packets. After detection, then the mitigation phase is activated.

In the mitigation phase, using PBFM, a flow entry having very high priority is made in the router/switch (Figure 10) to which the attacking host is connected to stop the flow of the attacking traffic only. Following is an example for TCP SYN attack.

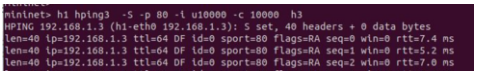

Figure. 8. TCP SYN attack initiated

Figure. 9. TCP SYN attack detected and blocked.

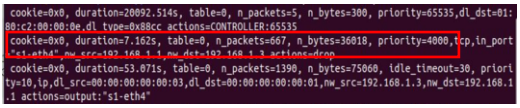

Figure. 10. Flow entry made to block the flow of TCP SYN attack traffic

Figure. 11. Unblock traffic flow

Additional functionality (Figure 11.) of periodically checking whether the attack is in progress or not is implemented. It helps to bring the status of the network devices and flows to normal by unblocking the traffic, if within threshold limits, else the traffic will be kept in blocked state only.

Following were the observations: -

Using PBFM only the malicious traffic is blocked. Normal traffic detected within the threshold is allowed without any interruptions. The methodology only stops the flow of malicious traffic and does not completely isolate the attacking host by shutting down the switch ports. It instead opens up an opportunity for the network administrators and network security experts who access the infected device and try to analyse the attack reasons while normal traffic flows through the network.

If both malicious traffic and normal legitimate traffic within threshold limits are traversing through the same path and network devices only the malicious traffic is selectively stopped and the normal legitimate traffic is not disturbed. It again provides an opportunity for troubleshooting without disturbing the network.

The mechanism of intermittent check of the event whether the attack is in progress helps to gauge the duration of the attack once the attack is ceased. After checking the traffic threshold limits, on ceasing of attack, the traffic is unblocked.

Figure 12. illustrates the graph of how the attacks started in a burst and how it is brought down using Policy Based Flow Management.

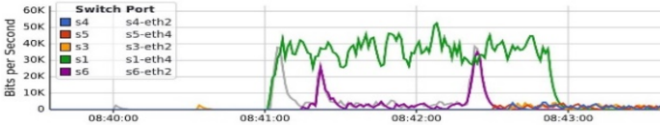

Figure. 12. Graphical representation of TCP SYN attack initiation and mitigation

The highlighted graph (green colour) shows that the attack was started by a host in router/switch s1 and sFlow recognised it as the traffic originating network device. The traffic initiated increased quickly to an average of around 45000 bps. It is detected and mitigated using PBFM and sFlow-RT, by making a flow entry using REST API, through the Controller in the identified network device and the graph dips down to zero.

6. Conclusion

In this paper the study and experimentation using SDN capabilities of PBFM with sFlow-RT application was carried out to detect and mitigate the DDoS attacks and the results found are summarised as follows: -

The network device to which the attacking host is connected is identified and pinpointed accurately and helps in detecting and mitigating the attack at the source of attack itself. Detection is carried out using a script with predefined threshold and the parameters to classify DDoS attack types defined. Mitigation of DDoS attack is realised by making a flow entry in the identified switch/router using PBFM capability of SDN.

Using predefined threshold and classification parameters, PBFM capability of SDN and sFlow-RT with RESTful API, the malicious DDoS Attack traffic is identified and isolated from the normal traffic which passes uninterrupted. With traffic isolation and affected device pinpointed, methodology adopted opens up troubleshooting opportunity without disturbing the network and network traffic for infected devices and all network devices from attacking source host to target destination host.

Intermittent checking functionality for the DDoS attack continuity or cessation helps in gauging attack duration by acting as a gatekeeper to monitor the attack. When the attack ceases, the traffic for that particular kind of flow is unblocked if within threshold limits. With the proposed methodology in the paper, the Controller enables the router/switch, to which the attacking host is connected, to function as a dynamic firewall which gets activated once a trigger in the form of threshold crossing is detected. Better control over the network will help in facing challenges like mapping of network devices and forensic artefacts for attacker tracking due to Cloud Service Utilisation by IoT devices [33].

References

[1] RFC 7426 – Software Defined Networking: Layers and Architecture Technology
[2] RFC 7149 – Software Defined Networking: A perspective from within a Service Provider Environment
[3] RFC 3176 - InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks
[4] https://www.comparitech.com/blog/information-security/ddos statistics-facts/
[5] Rajeev Singh, Department of Computer Engineering College of Technology,G. B. Pant University of Agriculture and Technology, Pantnagar, Uttarakhand, India ,rajeevpec@gmail.com T. P. Sharma Department of Computer Science & Engineering ,National Institute of Technology, Hamirpur, Himachal Pradesh, India ,teekparval@gmail.com. Present Status of Distributed Denial of service (DDoS) Attacks in Internet World. International Journal of Mathematical, Engineering and Management Sciences Vol. 4, No. 4, 1008–1017, 2019, https://dx.doi.org/10.33889/ IJMEMS.2019.4.4-080
[6] DDoS during the COVID-19 pandemic: attacks on educational and municipal websites tripled in Q1 2020 | Kaspersky
[7] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[8] https://www.indiumsoftware.com/blog/how-ddos-attack-protect-your- business
[9] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602-622, Firstquarter 2016, doi: 10.1109/COMST.2015.2487361.
[10] Christos Douligeris, Aikaterini Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art, Computer Networks, Volume 44, Issue 5, 2004, Pages 643-666, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2003.10.003.

[11] B. H. Lawal and A. T. Nuray, "Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN)," *2018 26th Signal Processing and Communications Applications Conference (SIU),* Izmir, Turkey, 2018, pp. 1-4, doi: 10.1109/SIU.2018.8404674.

[12] A. Kumar and N. K. Srinath, "Implementing a firewall functionality for mesh networks using SDN controller," *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Bengaluru, India, 2016, pp. 168-173, doi: 10.1109/CSITSS.2016.7779417.

[13] K. Giotis, G. Androulidakis and V. Maglaris, "Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks," *2014 Third European Workshop on Software Defined Networks*, Budapest, Hungary, 2014, pp. 85-90, doi: 10.1109/EWSDN.2014.24.

[14] Bawany, N.Z., Shamsi, J.A. & Salah, K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. Arab J Sci Eng 42, 425–441(2017). https://doi.org/10.1007/s13369-017-2414-5

[15] N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung and D. Choi, "Time-based DDoS detection and mitigation for SDN controller," *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Busan, Korea (South), 2015, pp. 550-553, doi: 10.1109/APNOMS.2015.7275389.

[16] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, V. Maglaris,Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments, Computer Networks, Volume 62, 2014, Pages 122-136, ISSN 1389-1286, https://doi.org/10.1016/j.bjp.2013.10.014.

[17] Software-defined network for dummies – Mykola konrad, Dan teichman with Brian Underdahl . Sonus special edition.(A Wiley brand).

[18] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[19] R. G. Rao and M. J. Nene, "SEDoS-7: A proactive mitigation approach against EDoS attacks in cloud computing," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017, pp. 965-970, doi: 10.1109/WiSPNET.2017.8299905.

[20] Brian Underdahl and Gary Kinghorn. (2015) Software Defined Networking For Dummies®, Cisco Special Edition Published by John Wiley & Sons, Inc. 111 River St.Hoboken, NJ 07030-5774 www.wiley.com

[21] https://inmon.com/products/sFlow-RT.php (Last accessed 11-06-2021)

[22] Phaal et al.(2014) Method,System and Computer Program Product for identifying common factors associated with network activity with reduced resource utilization. US Patent 8,838,774, 16 Sept 2014

[23] Phaal P. (2017) Method for asynchronous calculation of network traffic rates based on randomly sampled packets. US Patent 9,509,583, 29 Nov 2016

[24] Peter P. (2017) Distributed traffic quota measurement and enforcement. US Patent 9,712,443, 18 Jul 2017.

[25] Peter P. (2017) Method and system of large flow control in communication networks. US Patent 9,722,926, 1 Aug 2017.

[26] https://sflow-rt.com/ (Last accessed on 11-06-2021)

[27] https://github.com/mininet/mininet/wiki/Documentation (Last accessed 11-06-2021)

[28] https://sflow-rt.com/ (Last accessed on 11-06-2021)

[29] Lantz, Bob; Heller, Brandon; McKeown, Nick (2010). *[ACM Press the Ninth ACM SIGCOMM Workshop - Monterey, California (2010.10.20-2010.10.21)] Proceedings of the Ninth ACM SIGCOMM Workshop on Hot Topics in Networks - Hotnets '10 - A network in a laptop. , (), 1–6.* doi:10.1145/1868447.1868466

[30] sFlow-RT Writing Applications (sflow-rt.com)

[31] sFlow-RT Defining Flows (sflow-rt.com)

[32] sFlow-RT Reference (sflow-rt.com)

[33] Girija Devi M.S., Nene M.J. (2019) Security Breach and Forensics in Intelligent Systems. In: Satapathy S., Joshi A. (eds) Information and Communication Technology for Intelligent Systems. Smart Innovation,Systems and Technologies, vol 107. Springer, Singapore. https://doi.org/10.1007/978-981-13-1747-7_33

[34] S. Mani and M. J. Nene, "Data Loss Prevention due to Link-flapping using Software Defined Networking," *2021 6th International Conference for Convergence in Technology (I2CT)*, 2021, pp. 1-5, doi: 10.1109/I2CT51068.2021.9417990.