IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 1, November 2022

An Artificial Intelligent Mechanism for Future Networks using Mininet Wi-Fi

Prof. Shailesh Bendale[1], Kiran Pandit[2], Aswini Rathod[3], Isha Borude[4], Rutuja Chavan[5]

Professor, Department of Computer Engineering[1]

Student, Department of Computer Engineering[2,3,4,5]

NBN Sinhgad Technical Campus, Pune, Maharashtra, India

Abstract: *In this paper, Mininet Wi-Fi was used to simulate a Software Defined Network to demonstrate Mininet Wi-Fi's s ability to simulate their post and wireless dimension by assigning site to other site or access points and revoking these wireless associations which can also be integrated into the existing network. Need of networks continuously growing with more clients, more base points, and more network traffic. The security of these networks and network topologies becomes the most crucial part. The discovered mechanism will work in the network for security purposes. Mininetwi-fi will run the topology and parallellyWireshark that start capturing the network packet and protocol-like information. The extracted information will load in the CIC flow meter to make that readable. Further by processing that data using AIML algorithms data will be shuffled to avoid overfitting&underfitting then will be classified and labeled as normal data and attacked data. These results benefit modern and current networkline-up as the live network devices can also interact with the testing space for the data center, cloud, and mobile providers. The proposed framework can correctly enhance the overall performance of the synchrophasor based adaptive dependability/ security bias scheme in the course of DoS assaults and keep away from maloperation of the security devices, which enhances the strength system's balance.*

Keywords: Mininet Wi-fi, DDOS, CIC flow meter, Wire shark

I. INTRODUCTION

In today's world, computer networks have become smarter and much greater complex. At the current time, hackers internationally are designing and causing different range of attacks via the internet for exceptional reason such as information theft, system corruption and hijacking. The security of these networks and network topologies becomes the most important part. Network security is an issue that cuts across the stack. We showcase the ability of Mininet Wi-Fi to support security mechanisms combining physical and embracing real endpoints blend with virtualenvironments. Mininet Wi-Fi is a wireless network emulator that supports the user can select among multiple wireless propagations and mobility models as well as arbitrary topologies. Along with increasing the overall scalability and the fidelity of the emulated wireless channel, our roadmaps include research-friendly features towards repeatable and realistic experiments, including the ability to import packet and signal traces of the physical medium. With the help of a global group of network specialists and software developers, Wireshark continues to be updated for new network technologies and encryption methods. The network packet analyzer provides as much detail as possible about captured packets.

II. BACKGROUND AND FUTURE EXPLORATION

Previously, Networking of Named Data, networks with programmability, Hypertext Transfer Protocol as the narrow midsection, and SDN were all noted as sparkling design for enhancing the diagram of future networks. It is being hailed as the most auspicious solution for the Internet of the future. The term affectivity refers to the number performance, scalability, dependability, and safety parameters. A controller's overall performance is determined by means of a variation of elements, as well as the range of interfaces it can handle.

DOI: 10.48175/IJARSCT-7388

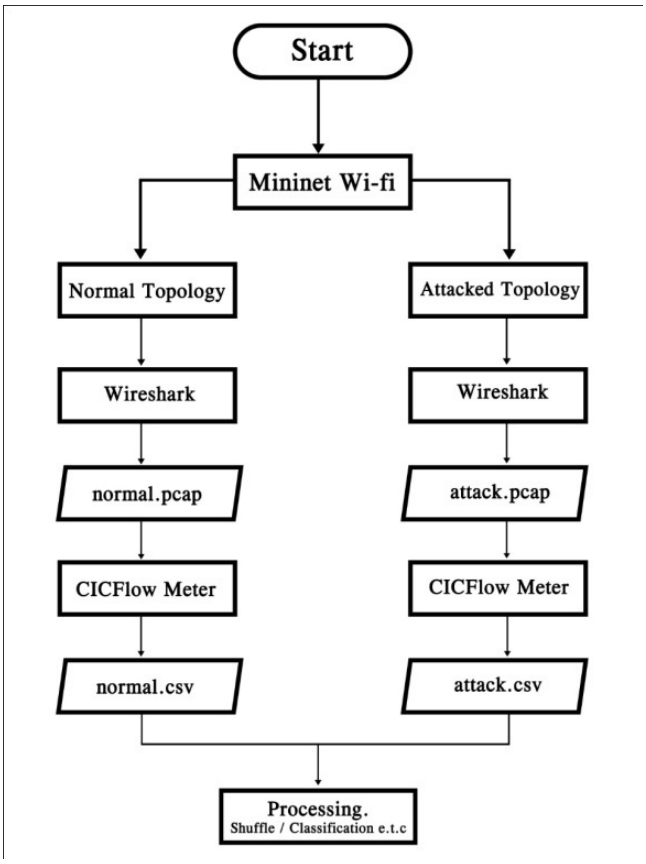


Figure 1: Block diagram

2.1 Mininet Wi-Fi

Mininet gives the platform to know how actual Software Defined Networking works by making a virtual network similar to the real network. This may utilized to run on small as well as very large-scale networks. One of the benefits of applying Mininet is that, an software that works on it can be effortlessly range to a literal network. It can be used as a tool in the process of teaching computer networks for various levels of education and addressing multiple case studies including mobility, mesh and ad hoc networks, load balancing, security, quality of Service (QoS), Multi Path TCP (MP-TCP), vehicular networks, IoT, P4, among others.

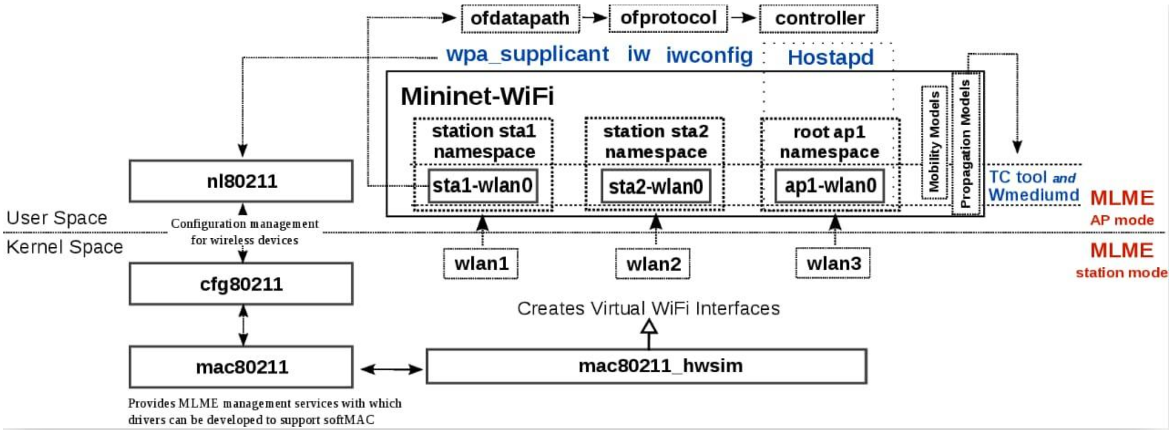
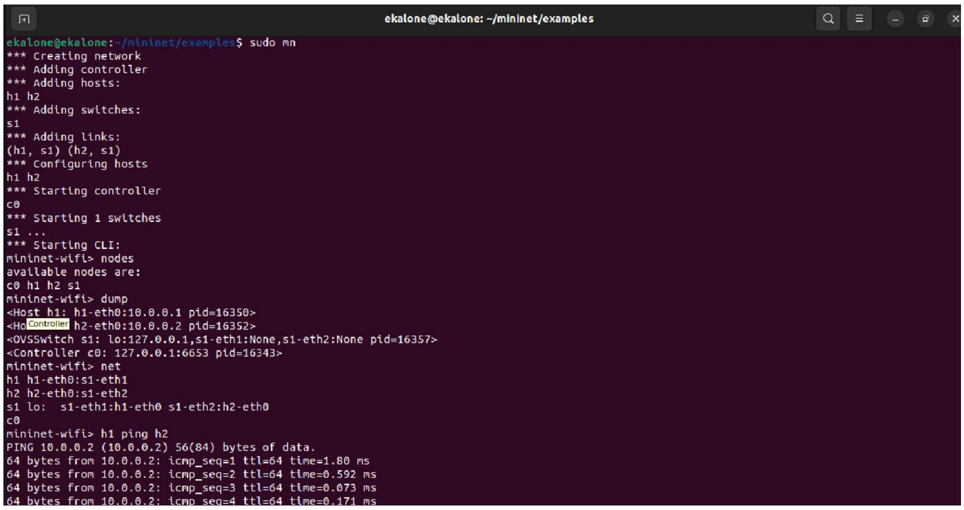


Figure 2: Mininet System Architecture

Mininet Wi-Fi is a part of the Mininet SDN network emulator and enlarging the performance of Mininet by adding virtualized Wi-Fi Sites and check Points based on the basic Linux wireless drivers.

DOI: 10.48175/IJARSCT-7388



```
ekalone@ekalone:~/mininet/examples$ sudo mn
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1)
*** Configuring hosts
h1 h2
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet-wifi> nodes
available nodes are:
c0 h1 h2 s1
mininet-wifi> dump
<Host h1: h1-eth0:10.0.0.1 pid=16350>
<Ho h2-eth0:10.0.0.2 pid=16352>
<OVSSwitch s1: lo:127.0.0.1,s1-eth1:None,s1-eth2:None pid=16357>
<Controller c0: 127.0.0.1:6653 pid=16343>
mininet-wifi> net
h1 h1-eth0:s1-eth1
h2 h2-eth0:s1-eth2
s1 lo:  s1-eth1:h1-eth0 s1-eth2:h2-eth0
c0
mininet-wifi> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.80 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.592 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.073 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.171 ms
```

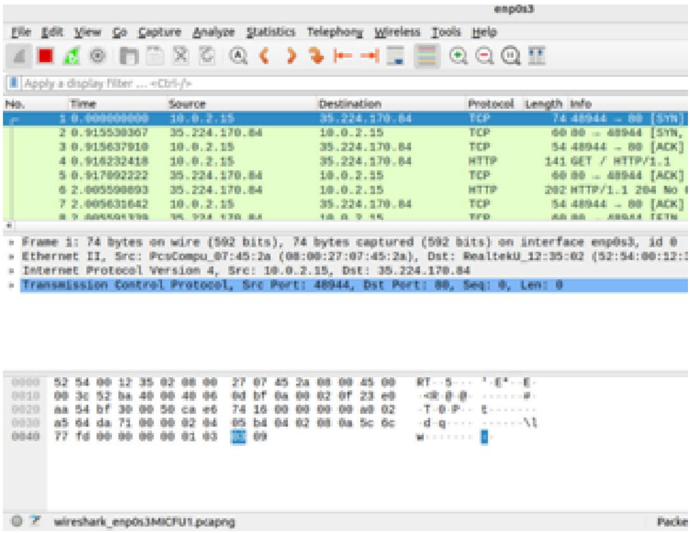
Figure 3: Mininet Wi-Fi

The outstanding value of Mininet is serving collaborative community Research studies through granting self-contained Software Defined Network prototypes, which all people with their personal computer (PC) can download, and use it. The program interface created by Mininet Wi-Fi these copy that allows all wireless traffic to all the virtual wireless interfaces in the network scenario.

The Mininet Wi-Fi Python API also provides the authorized Mininet node types of — switches, hosts, and controllers. Operating with Mininet Wi-Fi during runtime Mininet Wi-Fi python scripts can be run from the command line through running the script directly, or by providing it as part of a Python command. The only variation is how the route is stated.

2.2 Wireshark

Wireshark is the world's predominant and widely-used protocol analyzer. It lets us see what's happening in our network at a microscopic level. A network packet analyzer provides captured packet records in as many elements as possible. It can recognize many different types of encapsulation and present all the fields of a network packet. In a few respects it is, however we may effortlessly discover ways to use a number of the filters that include the software program and a way to view network specific packets. Reasons people use Wireshark: Network administrators use it to troubleshoot network problems, Network safety engineers use it to have a look at protection problems, QA engineers use it to confirm network applications, Developers use it to debug protocol implementations, People use it to learn network protocol internals.


enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
wireshark_enp0s3MICFU1.pcapng
Packe

```
No.   Time          Source           Destination      Protocol Length Info
    1 0.000000000   10.0.2.15        35.224.170.84    TCP      74 48944 → 80 [SYN]
    2 0.915530367   35.224.170.84    10.0.2.15        TCP      60 80 → 48944 [SYN,
    3 0.915637910   10.0.2.15        35.224.170.84    TCP      54 48944 → 80 [ACK]
    4 0.916232418   10.0.2.15        35.224.170.84    HTTP    141 GET / HTTP/1.1
    5 0.917092222   35.224.170.84    10.0.2.15        TCP      60 80 → 48944 [ACK]
    6 2.005500893   35.224.170.84    10.0.2.15        HTTP    202 HTTP/1.1 204 No
    7 2.005631642   10.0.2.15        35.224.170.84    TCP      54 48944 → 80 [ACK]
```

```
▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: PcsCompu_07:45:2a (08:00:27:07:45:2a), Dst: RealtekU_12:35:02 (52:54:00:12:3
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 35.224.170.84
▸ Transmission Control Protocol, Src Port: 48944, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  52 54 00 12 35 02 08 00  27 07 45 2a 08 00 45 00   RT··5··· '·E*··E·
0010  00 3c 52 ba 40 00 40 06  0d bf 0a 00 02 0f 23 e0   ·<R·@·@· ······#·
0020  aa 54 bf 30 00 50 ca e6  74 16 00 00 00 00 a0 02   ·T·0·P·· t·······
0030  a5 64 da 71 00 00 02 04  05 b4 04 02 08 0a 5c 6c   ·d·q···· ······\l
0040  77 fd 00 00 00 00 01 03  03 09                     w······· ··
```

Figure 4: Working of Wireshark

DOI: 10.48175/IJARSCT-7388

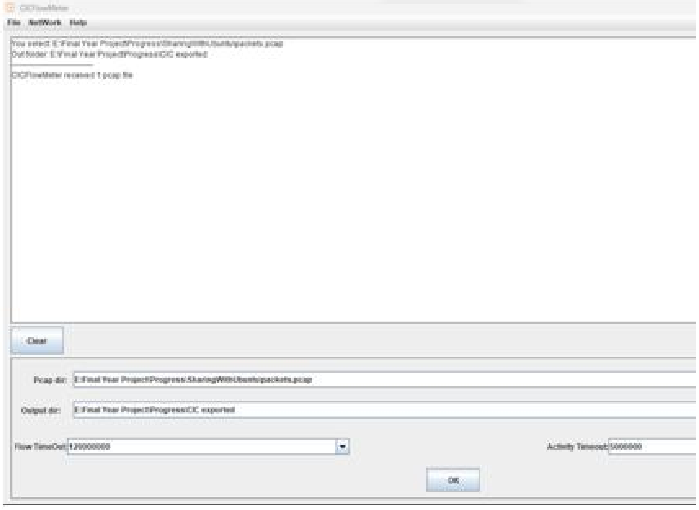
There many features as Wireshark is Available for *UNIX* and *Windows* which can *Capture* live packet data from a network interface. Wireshark Open documents containing packet records captured with tcp dump/Win Dump. Wireshark can capture site visitors from many extraordinary network media types, which include Ethernet, Wireless LAN, Bluetooth, USB, and more. The precise media types supported can be restrained with the aid of using several factors, which include your hardware and working system.

In Wireshark, TCP window replace messages can suggest that a whole lot of packets are being conveyed among the server and the client; that is the case is for downloads. Since downloads will probably purpose network visitors congestion, a few packets could probably be misplaced and need to be recommitted to make certain TCP reliability.

2.3 CIC Flowmeter

Working with big information is now a truth of lifestyles across disciplines. Digital medical files are used to construct healthcare profiles; chemistry and life sciences store vast portions of biomedical data; and the legal system machine generates an ever-increasing amount of sensitive data.

The CIC will work across disciplines to create and domesticate a country wide network of research intelligence from industry, the user sector, academia, and authorities to take a look at and address internet security, private and trust.



```
You select: E:\Final Year Project\Progress\SharingWithUbuntu\packets.pcap
Out folder: E:\Final Year Project\Progress\CIC exported
-------------------------------
CICFlowMeter received 1 pcap file
```

Pcap dir: E:\Final Year Project\Progress\SharingWithUbuntu\packets.pcap

Output dir: E:\Final Year Project\Progress\CIC exported

Flow TimeOut: 120000000

Activity Timeout: 5000000

Figure 5: CIC Flowmeter

CIC Flow Meter is a network traffic float generator allotted with the aid of using CIC to generate 84 network traffic functions. It reads .pcap file and generate a graphical document of the features extracted and also gives csv document of the file. It is an open supply application written in Java and may be downloaded from GitHub. Its supply codes may be included to a task because it gives greater flexibility in phrases of selecting the functions you need to calculate, including new ones, and additionally having a higher manage of the period of the glide timeout.

It can be used to generate bidirectional flows, where the first packet determines the forward (source to destination) and backward (destination to source) directions, hence more than 80 statistical network traffic functions consisting of Duration, Number of packets, Number of bytes, Length of packets, etc. may be calculated one by one in the ahead and backward directions.Additional functionalities include, choosing features from the listing of current features, including new features, and controlling the duration of flow timeout. The output of the software is the CSV format record that has six columns classified for every flow (Flow ID, Source IP, Destination IP, Source Port, Destination Port, and Protocol) with greater than 80 network traffic analysis features.

Note that TCP flows are commonly terminated upon connection teardown (through FIN packet) at the same time as UDP flows are terminated with the aid of using a flow timeout. The flow timeout value can be assigned arbitrarily by the individual scheme e.g., 600 seconds for both TCP and UDP.

DOI: 10.48175/IJARSCT-7388

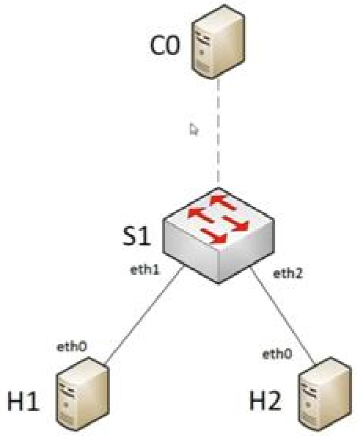


Figure 6: System Architecture

Mininet Wi-Fi standard network topology is used which is made up of a wireless access point (S1) with two Wi-Fi posts and the controller. The access point is connected to a controller (C0) using virtual connection involved and the two (H1 and H2) stations are connected to the access point (S1) using the simulated Wi-Fi interface.

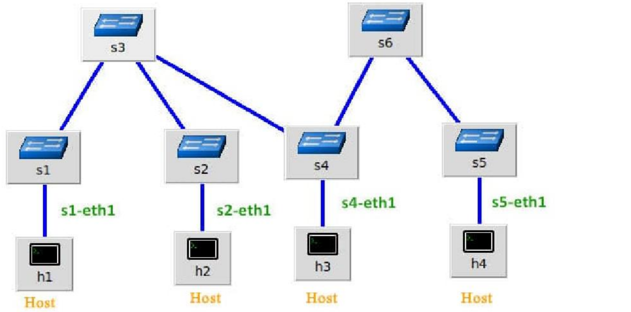


Fig.7: Normal Topology

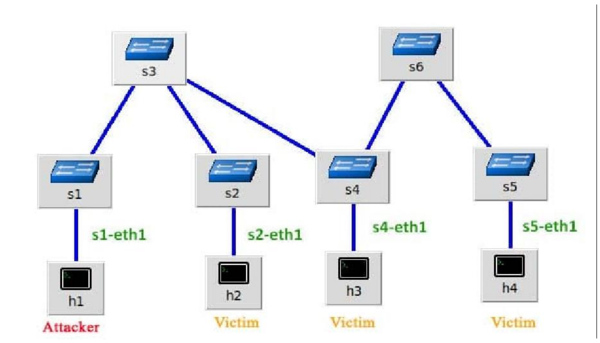


Fig.8: Attacked Topology

After performing operations using Mininet Wi-Fi with respect to Wireshark to capture data, we expect to get .pcap files in linux which is not in readable format and cannot be processed. We need to export these files to through CIC flowmeter in form of .csv files in windows, which is in readable and operational format. Again for attack files using iping-f DDOS attack and perform same operation. Then we get two files in which first file contains normal dataset while another file contains attack dataset we need to shuffle both files to avoid overfitting and underfitting errors. After importing these files in open source Platform that is Google co-laboratory shuffled files. At the end, we perform machine algorithm on those files starting with simply cleaning and processing data.

III. CONCLUSION

The environment is a very important factor when analyzing cyber security. In this paper, we proposed network based security system for future networks which will continuously capture network packets transferring between systems and Wi-Fi. Real systems are very difficult to reconfigure. Virtual machines permits easier topology changes however be suffer from scalability issues. In this paper we monitor the traffic controller and generate new and unique dataset which is in readable format that even unprofessional can read. By using existing technologies it is user-friendly system to setup and use.

ACKNOWLEDGMENT

We would like to express my special thanks of gratitude to my teacher Prof. Shailesh Bendale as well as our principal Dr. S.P. Patilwho gave me the golden opportunity to do this wonderful project on the topic An Artificial Intelligent Mechanism for Future Network Using Mininet Wi-Fi, which also helped us in doing a lot of Research and we came to know about so many new things we are really thankful to them.

This paper and the research behind it would not have been possible without the exceptional support of my supervisor, Prof. Shailesh Bendale sir His enthusiasm, knowledge and exacting attention to detail have been an inspiration and kept our work on track and for his valuable and constructive suggestions during the planning and development of this research work. His willingness to give his time so generously has been very much appreciated.

I am also grateful for the insightful comments offered by the anonymous peer reviewers at Books & Texts. The generosity and expertise of one and all have improved this study in innumerable ways and saved me from many errors; those that inevitably remain are entirely my own responsibility. And our project group members we really punctually worked hard.

REFERENCES

[1]. SorinBuzura, VasileDadarlat, Adrian Peculea , Hugo Bertrand, Raphaël Chevalier (2022); Simulation Framework for 6LoWPAN Networks Using Mininet-WiFi.

[2]. AanchalChaurasia, SoumyaNandan Mishra, SuchismitaChinara (2020); Performance Evaluation of Software-Defined Wireless Networks in IT-SDN and MininetWi-Fi .

[3]. Ramon Fontes, Samira Afzal, Samuel H. B. Brito (2016). MininetWi-Fi 'Emulating softwaredefined wireless networks.

[4]. G. Bagyalakshmi, G. Rajkumar, N. Arunkumar, M. Easwaran, K. Narasimhan,V.Elamaran; 'Mario Solarte (2018). Network Vulnerability Analysis on Brain Signal/Image Databases Using Nmap and WiresharkTools .

[5]. MukhtiarBano; Amir Qayyum; Rao Naveed Bin Rais; Syed Sherjeel A. Gilani (2021); SoftMesh: A Robust Routing Architecture for Hybrid SDN and Wireless Mesh Networks.

[6]. AsthaChawla,AnimeshSingh,PrakharAgrawal,BijayaKetanPanigrahi, BhaveshR.Bhalja, Kolin Paul (2021); Denial-of-service attacks Pre-emptive and detection framework for synchrophasor based wide area protection applications.

[7]. VivensNdatinya,ZhifengXiao,Vasudeva Rao Manepalli,KeMeng ,Yang Xiao(2015); Network forensics analysis using Wireshark.

[8]. BinduDodiya ,Umesh Kumar Singh (2022); Malicious traffic analysis using wireshark by collection of indicators of compromise.

[9]. NeelamGupta,MashaelS.Maashi,SarveshTanwar,SumitBadotra,MohammadAljebreen,Salilbharanay (2022);A comparative study of Software Defined Networking controllers using Mininet.

[10]. Jain, Vinit. "Getting Familiar with Wireshark." Wireshark Fundamentals. Apress, Berkeley, CA, 2022. 35-78.

[11]. Lantz B, O'Connor B. (2015). A Mininet-based Virtual Testbed for Distributed SDN Development.

[12]. Introduction to Wireshark- https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html.

[13]. Working of Wireshark-https://wiki.wireshark.org/Development/Workflow

[14]. Applications of CIC FlowMeter-https://www.unb.ca/cic/research/applications.html#CICFlowMeter

[15]. MininetWi-fi Introduction-https://hackmd.io/@akiranet/rynV3Udz5.

[16]. Lantz,B.; Handigol,N.; Heller, B.; Jeyakumar,V. Introduction to Mininet. Mininet Project,[Enlínea].2017. https://github.com/mininet/mininet/wiki/Introduction-to-Mininet .

BIOGRAPHY

- Kiran Pandit is currently pursuing Bachelor's Degree in Computer Engineering at NBN Sinhgad School of Engineering, Pune.
- Aswini Rathod is currently pursuing Bachelor's Degree in Computer Engineering at NBN Sinhgad School of Engineering, Pune.
- Isha Borude is currently pursuing Bachelor's Degree in Computer Engineering at NBN Sinhgad School of Engineering, Pune.
- Rutuja Chavan is currently pursuing Bachelor's Degree in Computer Engineering at NBN Sinhgad School of Engineering, Pune.