Security-as-a-Function in 5G Network: Implementation and Performance Evaluation

Shivank Malik
Department of Computer Science and Engineering
Indian Institute of Technology Jammu, 181221, India
Email: 2022pis0074@iitjammu.ac.in

Samaresh Bera, *Senior Member, IEEE*
Department of Computer Science and Engineering
Indian Institute of Technology Jammu, 181221, India
Email: s.bera.1989@ieee.org

***Abstract*—The service-based architecture of 5G allows network operators to place softwarized network functions on commodity hardware with the help of software-defined networking (SDN) and network function virtualization (NFV) technologies. While several existing works focused on network function placement and service routing in a 5G network theoretically, more investigation is required to study the performance of the softwarized network functions when placed on commodity hardware. In this paper, we study the softwarized network security function placement in a 5G network and its impact on the network performance. Specifically, we focus on the implementation of primary network security functions, such as intrusion detection and prevention systems (IDS/IPS) and network address translation (NAT), in a 5G network using open-source tools. We present a comprehensive method for the function placement, network configuration, and performance evaluation in the presence of synthetic network traffic. The extensive experiment results show that softwarized network security functions can be used to meet the quality-of-service requirements of specific applications in 5G. In contrast, dedicated hardware-based network functions may be required to support applications with stringent QoS requirements.**

***Index Terms*—5G core network, Performance evaluation, Network security, Intrusion detection and prevention system, Network function virtualization**

I. Introduction

The recent advancement of mobile communications (such as 5G and beyond networks) is expected to support modern applications with stringent quality-of-service (QoS) requirements. The applications are categorized into three broad areas – enhanced mobile broadband (eMBB), ultra-reliable and low-latency communications (uRLLC), and massive machine-type communications (mMTC) [1], [2]. The QoS requirements of these applications range from high bandwidth to high reliability to low latency [3]. Fulfilling such diverse QoS requirements of the applications using traditional vendor-specific networking architecture and devices is cost-expensive [4].

The service-based architecture of 5G [5], [6], as shown in Figure 1, allows the network operators to place application-specific softwarized network functions in the 5G network to alleviate the issues with vendor-specific dependencies. This is enabled by the software-defined networking (SDN) and network function virtualization (NFV) technologies [7]–[9]. The SDN provides flexible networking for traffic forwarding by separating the control and data planes. Whereas NFV enables network operators to place the user-plane functions (UPFs) as virtual network functions (VNFs) as per application-specific requirements.

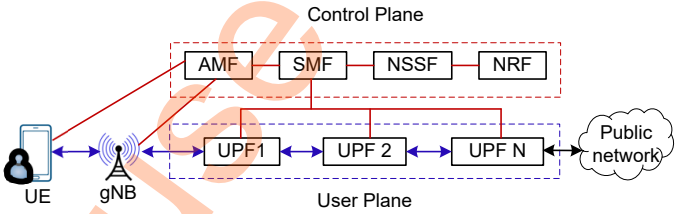


Fig. 1: 5G network architecture with control and user planes

In this paper, we consider the UPF as a network security function and its placement in the 5G network. Specifically, we focus on two primary security functions: intrusion detection and prevention system (IDS/IPS) and network address translation (NAT). We present a systematic approach to configure the UPF as a network security function using open-source software tools. Furthermore, we generate synthetic traffic in the 5G network to evaluate the performance of the network security function when placed on commodity hardware. This is important to analyze whether the softwarized network security functions are capable of meeting the QoS requirements of 5G applications [3]. We note that our objective is to study the performance of the aforementioned softwarized network security functions, not to compare them with physical network functions. In short, we aim to answer the following questions:

- How do we configure and implement a UPF as a network security function and place it in the 5G network?
- What is the impact of the softwarized network security function on the network performance in terms of throughput, latency, and packet drop?

The rest of the paper is organized as follows. Section II presents the state-of-the-art 5G network enabled with virtualized network functions. Section III presents the detailed softwarized 5G network setup, and configuration and deployment of the network security functions. Section IV presents the results on the network performance. Finally, Section V concludes the paper with future research directions.

II. Related Work

We categorize the existing works into two parts – a) 5G network architecture and its challenges for security, and b)

softwarized security function placement in a 5G network and performance evaluation, as discussed below.

A. 5G network architecture and security issues

Several security features in 5G are discussed in [6], [10], [11] considering the evolving 3GPP standards for 5G. Specifically, the authors discuss the information security issues and challenges in 5G with integration of internet-of-things, device-to-device communication, vehicular-to-anything communications, and network slicing. The integration of these verticals introduces a complex landscape of information security issues, necessitating innovative security solutions for protecting critical infrastructure. Furthermore, the need for dynamic and policy-driven security architecture in 5G networks is emphasized in [12]. The proposed architecture in [12], tailored for multi-tenant NFV/SDN-enabled networks, addresses the intricate security challenges posed by network slicing and resource sharing. However, enforcing stringent security requirements in 5G can limit the flexibility in its architecture. The authors in [13], [14] highlight the critical balance between network flexibility and robust security. This duality is especially pertinent in environments with varying trust-levels, where maintaining security without compromising the inherent agility of 5G is paramount.

The authors in [15] presents a comprehensive view of 5G security issues, challenges, and solutions considering OSI-layered architecture. It emphasizes that no single OSI layer can independently assure security. Instead, a collaborative and multi-layered approach is necessary. The work also discusses the vulnerabilities at the physical layer, like eavesdropping and data fabrication. Similarly, the authors in [16] present a framework for balanced QoS and security measures in the context of multimedia applications.

The above-mentioned works collectively build a robust understanding of 5G security. These works theoretically focus on the general security architecture, framework, and specific technological vulnerabilities.

B. Softwarized security function and its performance in 5G

The authors in [17] evaluated the impact of softwarized security function on latency performance with forwarding and filtering strategies. The authors evaluated the performance of the security functions in two scenarios – functions placed on the host machine and VMs. The results show that VM-based security functions impose increased latency compared to the direct placement on the host machine. Similarly, the authors in [18] present a secure 5G network framework, in which a softwarized security function is deployed. Similar to [17], the authors evaluate the network latency in the proposed framework.

It is evident that there exist a few works that focused on the deployment of security functions and their performance in a 5G network. Furthermore, while the works [17], [18] are the closest ones, this work has significant differences from them. The work in [18] focuses on a layered security architecture for 5G networks and addresses the complexity of policy management in network slicing. However, it does not delve into the direct impact of the security functions on network performance. The work in [17] presents the softwarized security function placement and shows the impact on network latency. However, considering the diverse performance requirements of 5G applications, it is required to have a comprehensive network performance analysis in the presence of heterogeneous traffic. Consequently, this work evaluates the impact of softwarized security function on the network performances such as latency, throughput, jitter, and packet drop in the virtualized 5G environment.

III. Network Setup: Software Prototype

We deploy the 5G core network using Open5GS (https://open5gs.org/open5gs/) open-source software platform. The 5G RAN is deployed using UERANSIM (https://github.com/aligungr/UERANSIM) open-source software platform. UERANSIM and Open5GS are integrated together to have an end-to-end softwarized 5G network. We setup the experiment platform in a host machine with the following hardware and software configuration: Processor: Intel i9-13th generation, 24 core; RAM: 64 GB; Ethernet: 1 Gbps; and OS: Ubuntu 20.04 LTS. We create three guest machines, one for UE and gNB placement, another for 5G core network placement with security functions, and the other acts as a server to the UE.

We configure the UPF so that it acts as either IDS or IPS along with NAT. We use Snort (https://www.snort.org/), which is another open-source software tool, to configure the UPF as IDS or IPS. We discuss the implementation of UPF in the subsequent sections.

A. Enabling traffic forwarding through the UPF

Figure 2 shows the network setup between the UE and server with UPF as NAT software security function. We create two IP-tunnels – one between UE and gNB (`uesimtun`) and the other between gNB and UPF (`ogstun`). The traffic gets forwarded through these two tunnels. The NAT module in UPF takes care of network address translation for incoming and outgoing traffic. The IP configurations of UE, gNB, and

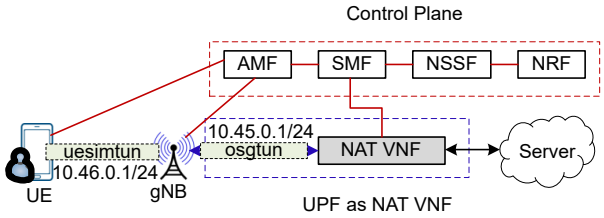


Fig. 2: UPF as NAT software security function

UPF are shown in Figure 2. The specific changes made in the network and `iptables` rules are as follows:

```
# enabled ipv4 forwarding
ipv4.forward = 1 # in /etc/sysctl.conf

# to resolve the DNS by the client
sh -c "echo nameserver 8.8.8.8 >\
```

```
/etc/resolv.conf"

# for traffic forwarding with NAT
iptables -t nat -A POSTROUTING \
-j MASQUERADE
```

B. UPF configuration as IDS

Figure 3 shows the network setup with IDS and NAT module inside the UPF. The IDS module inside the UPF listens to the 5G tunnel interface (`ogstun`) connected to the client and generates alerts based on the rules configured in IDS mode. We use customized rules in UPF to generate traffic alerts. The IDS module sends the alert messages to the NRF module at the control-plane. We note that the IDS network function silently listens to the interface and generates alert messages based on the rule-set configured in UPF. It is not involved in making packet forwarding decisions. Therefore, the network performance in IDS-NAT scenario is eventually impacted by the NAT network function. A sample set of rules used in UPF

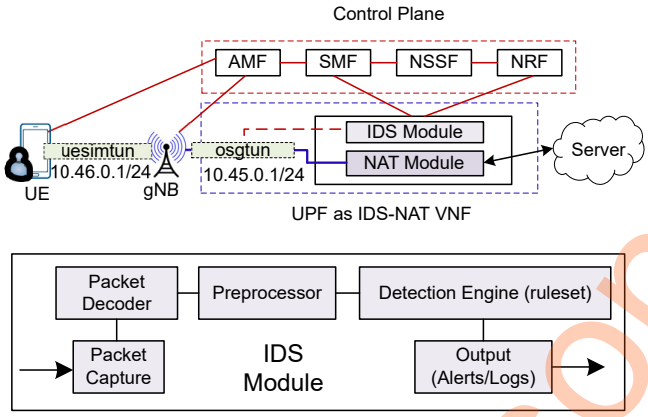


Fig. 3: UPF as IDS-NAT software security function

for IDS are as follows:

```
alert icmp any any -> \
any any (msg:"ADMIN-ALERT, ICMP traffic \
detected";sid:1000004;)

alert tcp any any -> \
$HOME_NET 80 (msg:"Possible HTTP DoS \
Attack";sid:1000002;)

alert icmp any any -> \
$HOME_NET 80 (msg:"Dos Attack suspected"; \
sid:1000001;)

alert tcp $EXTERNAL_NET any -> $HOME_NET \
445 (msg: "Exploit Detected!"; \
flow: to_server, established; classtype: \
attempted-admin; priority: 10; \
sid: 2094284; rev: 2;)
```

C. UPF configuration as IPS

Figure 4 shows the IPS scenario, where the UPF acts as an IPS. The IPS module utilizes the NFQ to process all packets sent from the client so that the packets pass through the IPS and the desired action is taken – whether to `forward` or `drop` or `send an alert`. We note that all packets are allowed through the IPS module in this experiment, as our primary objective is to study the impact on network performance while securing the network. However, any desired action can easily be integrated into the setup. The specific changes made in

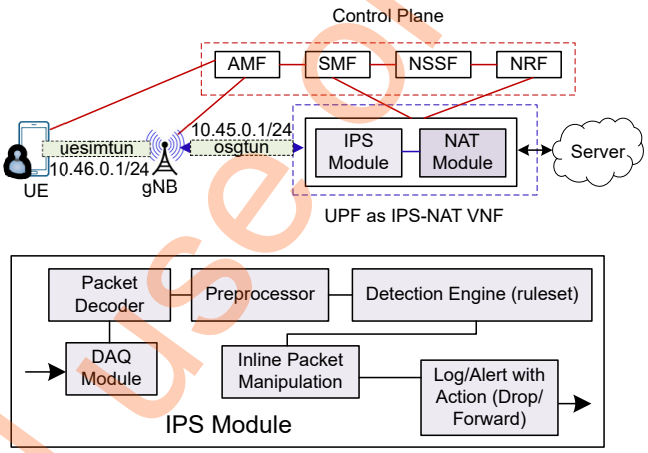


Fig. 4: UPF as IPS-NAT software security function

network and IPS configurations in addition to the IDS-NAT scenario (refer to Sec III-B) are as follows:

```
# to inspect each packet with NFQUEUE
iptables -I FORWARD -j NFQUEUE\
--queue-num=4

# Changes in snort.conf
config daq: nfq
config daq_mode: inline
config daq_var: queue=4
```

IV. Performance Evaluation

We evaluate the network performance of the 5G core network enabled with softwarized network security functions in terms of throughput, latency, jitter, and packet drop. We present the results for two scenarios – `IDS-NAT` and `IPS-NAT`. In `IDS-NAT`, the UPF is configured to send alerts to the network manager. The UPF generates alerts based on the defined rule-set considering the interests of network service providers. Therefore, the `IDS-NAT` implementation does not impact the network performance compared to the `NAT` implementation. Whereas in `IPS-NAT`, the packets get forwarded to the NFQ, and desired action is taken based on the rule-set. Therefore, `IPS-NAT` can impact the network performance. Furthermore, we generate TCP and UDP traffic using D-ITG packet generator [19] with varying number of packets for both `IDS-NAT` and `IPS-NAT` scenarios to study the network performance. Consequently, the subsequent sections present

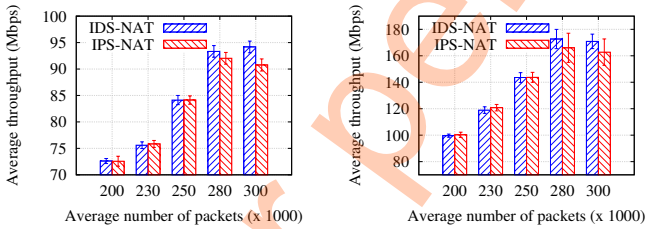
the results when the UPF is configured as IDS-NAT and IPS-NAT. Each experiment runs 20 times for 5 seconds each. We use the 95% confidence interval [20] to plot the results with a varying average number of packets with payload size 512 bytes. We note that the generated traffic follows the Poisson distribution, where mean is the average number of packets.

A. Results and Discussion

The following performance metrics are considered – average throughput, latency, and jitter for TCP and UDP applications. In contrast, the percentage of packet drop is shown only for UDP applications. This is because the TCP applications are connection-oriented, and the application-layer re-transmission happens in the presence of packet drop.

1) Throughput: Figures 5(a) and 5(b) present the average network throughput with varying number of packets for TCP and UDP applications, respectively. We see that the average throughput increases initially with less number of packets for both TCP and UDP applications. However, it gets saturated for large number of packets due to the network capacity constraint. As expected, the UDP provides higher throughput than the TCP, as shown in Figures 5(a) and 5(b). We note that the throughput is calculated at the network layer. Therefore, application layer re-transmissions are not excluded in throughput calculation.

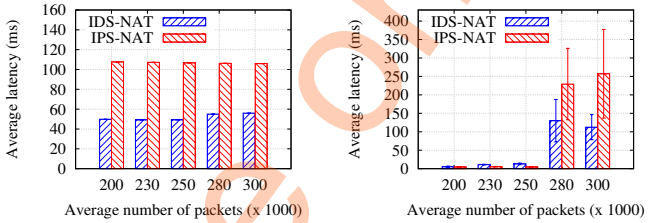
We also see that IDS-NAT and IPS-NAT yield a similar throughput for small number of packets. However, IDS-NAT yields a higher throughput than IPS-NAT with large number of packets. This is because the packets are forwarded without sending them to the NFQ module in IDS-NAT. The IDS security function only listens to the 5G tunnel interface and sends alerts based on the rule-set. In contrast, the packets are always sent to the NFQ module and analyzed before being forwarded/dropped, when the security function works as IPS-NAT. Therefore, the queue is overloaded in the presence of large number of packets, and eventually they get dropped, which, in turn, leads to decreased network throughput.



(a) TCP application (b) UDP application

Fig. 5: Network throughput with varying number of packets

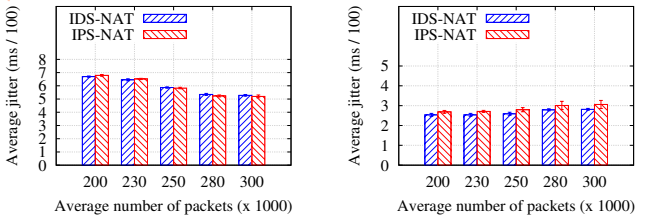
2) Latency and Jitter: Figure 6 presents the network latency with varying number of packets. Similar to the throughput, the latency experienced by TCP applications (refer to Figure 6(a)) is greater than that of the UDP applications (refer to Figure 6(b)). This is because TCP is connection oriented, which incurs additional delay compared to UDP. Furthermore, the latency experienced by TCP applications is almost constant irrespective of the number of packets in the network, as presented in Figure 6(a). This is due to the fact that TCP adaptively adjusts the congestion-window size, which eventually affects the throughput, as discussed in Section IV-A1. On the other hand, the latency experienced by UDP applications is very low for small number of packets. However, the latency increases non-linearly with large number of packets due to network congestion.



(a) TCP application (b) UDP application

Fig. 6: Latency with varying number of packets

We also measure the jitter as it is important for real-time applications, such as audio-video conferencing. Figure 7 shows the jitter for both TCP and UDP applications. For UDP applications, jitter is lower compared to TCP applications in both IDS-NAT and IPS-NAT setup. Furthermore, the IDS-NAT and IPS-NAT provide equivalent performance in terms of jitter.



(a) TCP application (b) UDP application

Fig. 7: Jitter with varying number of packets

3) Packet drop: We present the percentage of packet drop for UDP applications with varying number of packets in the network in Figure 8. We see that the percentage of packet drop is very low in the presence of small number of packets for both IDS-NAT and IPS-NAT. However, it increases non-linearly with large number of packets. This is because large number of packets creates network congestion leading to higher percentage of packet drop. Furthermore, the percentage of packet drop is higher in IPS-NAT than IDS-NAT due to the NFQ overflow.

In summary, it is evident that the softwarized security functions are capable of achieving the diverse QoS requirements in terms of throughput and latency for some of the applications, as considering their QoS requirements [3]. However, it may

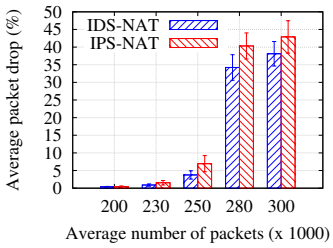


Fig. 8: Percentage of packet drop with varying number of packets for UDP application

not be suitable for applications with ultra-low latency requirements. Furthermore, redundant placement of security functions is also required to achieve high reliability. We also note that the network performances may vary depending on the commodity hardware configuration. Therefore, the performance of the softwarized security functions and QoS requirements of associated applications must be taken into consideration while placing them on commodity hardware.

V. Conclusion

In this paper, we studied the softwarized network security function placement in a 5G network and its impact on network performances, while utilizing commodity hardware. We used open-source software tools for the deployment and configuration of the 5G network with different network security functions. The experiment results showed that the softwarized network functions can meet QoS requirements of many 5G applications, while ensuring security.

We identify some future research implications as further study is required to understand different aspects of softwarized 5G networks.

Platform to place the softwarized security functions: As evident from this study and the existing works, the hardware and software platforms on which the security functions are placed also affect the network performance. Therefore, further study is required with different hardware and software platforms to have *optimized* network security function placement for application-specific service provisioning.

Software tools to create network security functions: In this work, we used Snort to implement IDS and IPS security functions and analyzed the impact on network performance. Other software tools, such as Suricata (https://suricata.io/), can also be used to conduct a comparative study. We note that a few works presented a comparative study between the Snort and Suricata to implement IDS. However, they mainly focused on the efficiency of the tools without considering the impact on the network performances.

Application-specific security function placement: With the introduction of network slicing, we can create multiple logical networks, each serving different applications based on their service-level agreements. Therefore, the performance of each slice needs be studied in the presence of different security functions based on QoS requirements.

VI. Acknowledgment

This work has been partially supported by the SRG research grant (grant number: SRG/2023/000569), funded by SERB, Govt. of India.

References

[1] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5G usage scenarios and traffic models," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 905–929, 2020.

[2] "Verticals uRLLC use cases and requirements," NGMN Alliance, Tech. Rep. V 2.5.4, Feb. 2020.

[3] "5G; Service requirements for the 5G system," 3GPP, Tech. Rep. TS 22.261, Version 15.9.0, Release 15, 2021.

[4] Y. Jarraya, T. Madi, and M. Debbabi, "A survey and a layered taxonomy of software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1955–1980, 2014.

[5] T. Sun and D. Wang, "Service-based architecture in 5G: Case study and deployment recommendations," NGMN Alliance, Tech. Rep., 2019.

[6] H. C. Rudolph, A. Kunz, L. L. Iacono, and H. V. Nguyen, "Security challenges of the 3GPP 5G service based architecture," *IEEE Commun. Stand. Mag.*, vol. 3, no. 1, pp. 60–65, 2019.

[7] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1617–1634, 2014.

[8] J. d. J. Gil Herrera and J. F. Botero Vega, "Network functions virtualization: A survey," *IEEE Latin America Transactions*, vol. 14, no. 2, pp. 983–997, 2016.

[9] H. Farhady, H. Lee, and A. Nakao, "Software-defined networking: A survey," *Computer Networks*, vol. 81, pp. 79–95, 2015.

[10] D. Lučić and P. Mišević, "An impact of implementation of 5G technology on information security," in *Intl. Conven. on Information, Communication and Electronic Technology*, 2021, pp. 412–416.

[11] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, Jan. 2020.

[12] M. Siddiqui, E. Escalona, E. Trouva, M. Kourtis, D. Kritharidis, K. Katsaros, S. Spirou, C. Canales, and M. Lorenzo, "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks," in *IEEE NFV-SDN*, 2016, pp. 44–49.

[13] M. Settembre, "A 5G core network challenge: Combining flexibility and security," in *AEIT International Annual Conference*, 2021, pp. 1–6.

[14] J. Yin, S. Li, G. Liu, J. Chen, J. Shen, and Q. Wang, "Customized 5G private network solution of high flexibility, security and controllability," in *IEEE Intl. Symp. on Broadband Multimedia Systems and Broadcasting*, Jun. 2022, pp. 1–6.

[15] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G security challenges and solutions: A review by OSI layers," *IEEE Access*, vol. 9, pp. 116 294–116 314, 2021.

[16] T. Shuminoski, T. Janevski, A. Risteski, and M. Bogdanoski, "Security and QoS framework for 5G and next generation mobile broadband networks," in *IEEE EUROCON*, Jul. 2017, pp. 104–109.

[17] S. Gallenmüller, J. Naab, I. Adam, and G. Carle, "5G QoS: Impact of security functions on latency," in *IEEE/IFIP NOMS*, Apr. 2020, pp. 1–9.

[18] W. M. L. Koribeche, D. Espes, and C. Morin, "Security policy architecture for 5G Networks," in *Intl. Conf. on Network of the Future*, 2023, pp. 37–41.

[19] A. Botta, A. Dainotti, and A. Pescapé, "A tool for the generation of realistic network workload for emerging networking scenarios," *Computer Networks*, vol. 56, no. 15, pp. 3531–3547, 2012.

[20] A. Hackshaw, *Statistical Formulae for Calculating Some 95% Confidence Intervals. A Concise Guide to Clinical Trials*. John Wiley & Sons, Ltd, 2009.