5G Attacks and Countermeasures

Angelo Bjerre, Sebastian; Wøidemann Klæbel Blomsterberg, Mikkel; Andersen, Birger

Published in:
Proceedings of 25th International Symposium on Wireless Personal Multimedia Communications

Link to article, DOI:
10.1109/WPMC55625.2022.10014962

Publication date:
2023

Document Version
Peer reviewed version

5G Attacks and Countermeasures

Sebastian Angelo Bjerre
DTU Engineering Technology
Technical University of Denmark
Ballerup, Denmark
s163526@student.dtu.dk

Mikkel Wøidemann Klæbel Blomsterberg
DTU Engineering Technology
Technical University of Denmark
Ballerup, Denmark
s172133@student.dtu.dk

Birger Andersen
DTU Engineering Technology
Technical University of Denmark
Ballerup, Denmark
birad@dtu.dk

***Abstract*—With the arrival of fifth generation of mobile networking technology, 5G, subscribers and IoT devices can look forward to higher data transfer rates, lower latency, better reliability, and increased availability. Deploying new infrastructure in conjunction with the previous generations of networks will expand the attack surface. We explore the architecture of the 5G architecture and give an overview of the types of attack vectors and how to possibly mitigate the attacks. Through our research, we found that vulnerabilities must be addressed at every level within the infrastructure of 5G network. While 5G network has increased in complexity and separated services depend from one another, maintaining and patching a service has been made easier. From security perspective, this study emphasizes how mobile network technologies are receptive to threats and the need for mitigation methods is a high priority. We estimate exploit difficulties and they indicate how to prioritize the work forward on developing mitigation methods.**

***Index Terms*—5G, security, attack vectors, countermeasures**

I. INTRODUCTION

Since the formation of the 3rd Generation Partnership Project (3GPP) in 1998, 3GPP has developed protocols for mobile communication with the latest release of 5G in 2018. 5G is a crucial part of the future and the ever-growing tech industry. It has been forecasted that in 2025 there will be more than 75 billion Internet of Things (IoT) devices [26]. The need for high-performing networks with high bandwidth and low latency is also on the rise. Example of this is the expanse in autonomous devices such as vehicles. Autonomous vehicles must meet very stringent bandwidth and latency requirements. Such use-cases require a new network structure that can accommodate a large number of devices, whilst still being able to provide specific devices with high bandwidth, low latency, or both. 5G utilizes a range of different technologies to obtain this. The network is highly configurable, which allows the operator to prioritize certain devices in regard to their requirements. This can be done by bringing into service *Massive Machine-Type Communication*, to allow a large number of devices to be connected at the same time. Network is able to provide low latency using *Ultra-reliable Low-Latency Communications*. On top of these services, the current bandwidth of 4G is further advanced with the use of *Enhanced Mobile Broadband*, providing up to 20 times the speed of 4G with a theoretical speed of 20 Gb/s [8][9][27].

The increased complexity in the network also introduces vulnerabilities and thereby requires the network to be more focused on security. If the network is compromised it can open up to further escalation and possibly affect critical infrastructure and applications, such as medical equipment and autonomous vehicles. These are a fraction of the devices which could be affected by a compromised network, and the damages differ from the affected devices to the type of attack initiated. We cover the main components of the 5G network, and the types of vulnerabilities it can be susceptible to. We also cover methods of mitigating the attacks, in conjunction with why the components are vulnerable.

978-1-6654-7318-7/22/$31.00 ©2022 European Union

II. OVERVIEW OF 5G

A. 5G Architecture

While 5G network infrastructure was designed to be more secure than its predecessors, a misconfiguration in the SDN or flawed network components can present an opportunity for malicious actors to increase privileged access or identify weaknesses within network. When assessing the security risk of the network of a Communication Service Provider (CSP) one should not only look into the Radio Access Network (RAN) but also the Core network (CN).

One of the security risks CSPs face within CN has to do with actual implementation of 5G architecture. With the first release of 5G by 3GPP, the service had two implementations, i.e., Non-StandAlone (NSA) architecture and StandAlone (SA) architecture [15]. SA introduces lot of new features such as lower latency, increased bandwidth, and reduced power consumption. NSA could be implemented into the existing 4G LTE infrastructure, making it cheaper for CSPs to support subscribers with 5G enabled equipment. While the support for both infrastructures is desirable, the security risks from legacy protocols are also transferable between architectures. SA is without a need for the 4G network in order to operate and can be viewed as the "full 5G deployment", isolated from pre-existing technologies [10]. Fig. 1. shows differences.

B. Network Slicing

Network slicing is an essential part of 5G and works as virtualized networks on top of physical infrastructure. Network slicing provides different channels, with specific rules and capabilities. Within network slicing, we find three key channels; enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), and massive Machine Type Communications (mMTC).

eMMB is designed to provide high data bandwidth across a wide area. eMMB is mainly used for devices and applications, requiring high bandwidth, such as mobile phones, video streaming, and high-resolution security cameras.

URLLC is designed to meet strict and precise latency requirements and at the same time provide high reliability.

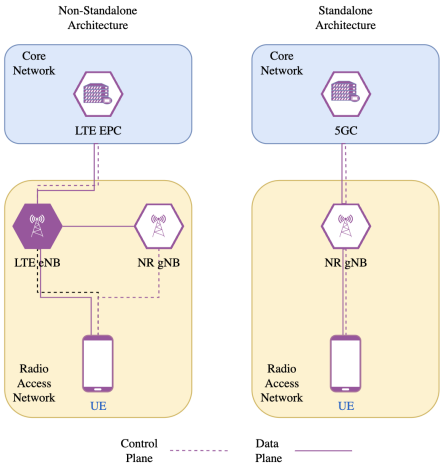

Fig. 1. Comparison of Non-Standalone and Standalone Architecture

URLLC is focused on devices in need of fast and reliable communication, such as autonomous vehicles and tasks where sensor data is critical for fast operation.

mMTC is designed to support a high volume of devices, where data is not frequent and the bandwidth at which data is transmitted is not a priority, e.g., weather stations.

Network slicing provides a tailored configuration for devices in need of specific requirements. This increases the complexity of the security needed to maintain a secure network. Each individual slice provides different security measures, depending on the use case, and the security might also differ from operator to operator. Each can include the optional security standards they find needed, and leave out other non-mandatory standards. Multiple operators having to cooperate on this, may lead to security holes and in turn expose network to a variety of different attack vectors [1].

C. Software Defined Networking

To make networks more agile and flexible, traditional way of designing networks had to be revamped. In traditional network functions like Domain Name Systems (DNS), firewalls, routing, and load-balancing are handled by individual hardware appliances. In relation to applications and content being moved to the edge of the network, the need for a more agile and flexible way of designing networks becomes important. Therefore, Software Defined Networking (SDN) in combination with Network Function Virtualization (NFV) was developed and integrated into 5G. SDN separates the network's control and forwarding planes, providing a centralized platform for managing the network. As the network control is decoupled from the forwarding function, this allows the control plane to be directly programmable. Network managers are now able to configure, manage and optimize network faster than before. This also means that configurations are less prone to errors. Whereas the traditional networking architecture was more error-prone and time-consuming to configure, SDN's quick manageability allows for faster error correction, as well as fast and more frequent security updates. NFV allows the maintainer to run multiple network functions on a single piece of hardware by virtualization of the functions. Utilizing NFV means that hardware components needed are less (cost-optimization) [9][12][24].

D. Multi-Access Edge Computing

Multi-Access Edge Computing (MEC) serves as a type of distributed computing providing high bandwidth and low latency by bringing services to edge of network and closer to end-user. In traditional network, data would be transmitted from end-user through network and to backend in a cloud. Backend would do computation and return the result to end-user. MEC moves the capabilities that backend provides to edge of network and closer to end-user. This is fundamental part of the performance gains granted through MEC used in 5G. To accommodate the user's need for particular performance requirements, the MEC plays an essential part to deliver mMTC, eMBB, and URLLC services. MEC provides ability to be in close proximity to data and thereby lowering latency to sub 10 ms. This can be crucial for certain applications that require ultra-low latency. Another benefit is continuous operation. Since edge applications are localized they are able to continue operating even when other parts of network are inaccessible [6][7].

III. ATTACKS AND COUNTERMEASURES

A. Core Network

NSA utilizes 4G's core also known as Evolved Packet Core (EPC), which consists of five components for its Control Plane (CP) and User Plane (UP), whereas SA utilizes new 5G Core (5GC). Fig. 2 compares EPC and 5GC.

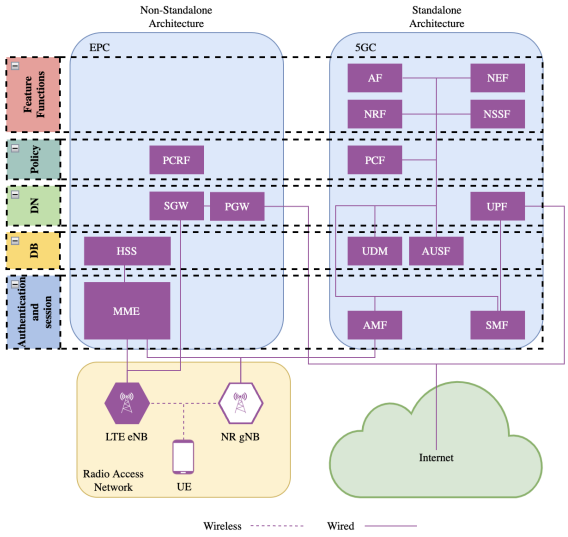

Fig. 2. Comparison of 4G and 5G Core Networks

1) Mobility Management Entity (MME): Responsible for tracking and monitoring the UEs throughout the RAN and includes also the recording of not active UEs.

2) Home Subscriber Server (HSS): The database that contains subscriber-related data.

3) Policy & Charging Rules Function (PCRF): Within this component, tracking and management of policy rules and billing data are held for the subscriber's traffic usage.

4) Serving Gateway (SGW): Forwards IP packets to and from RAN, anchoring the UE to the Core Network. Component is also involved in handovers to next base stations.

5) Packet Gateway (PGW): This component is in charge of connecting the Core Network to the external data network (more commonly referred to as the Internet). In its rawest form, it is basically an IP router.

If we compare NSA to SA we find that there are some similarities. Main difference can be found in the design approach where 5GC adopts a microservice-like architecture. By separation of functionality for each component, dependencies between CN and RAN are minimized and therefore concurrent access can be achieved. Where EPC consists of five components, 5GC consists of ten [15].

1) Access and Mobility Management Function (AMF): Responsible for user authentication, location, and mobility services and is comparable to EPCs MME service. However, unlike MME, AMF does not concern itself with session management.

2) Session Management Function (SMF): As name implies this service is in charge of user sessions and allocates IP addresses much like DHCP. Roughly it corresponds to EPCs MME and PGW (control-related aspect).

3) User Plane Function (UPF): Forwards packets between 5GC and Internet. Furthermore, service is also in charge of policy enforcement and traffic usage reporting. Corresponding the equivalency of the EPCs SGW and PGW.

4) Unified Data Management (UDM): Generating authentication credentials and managing user identity. To a certain degree resembles EPCs HSS.

5) Authentication Server Function (AUSF): Authenticates user by processing credentials generated by UDM. Together, UDM and AUSF form what is the equivariant of the EPCs HSS.

6) Policy Control Function (PCF): : Manages the policies that every component within the 5GC enforces. Comparable to EPCs PCRF.

7) Application Function (AF): Supports traffic routing and interacts with NEF.

8) Network Repository Function (NRF): Can be thought of as a "Service discovery" function.

9) Network Exposure Function (NEF): Essentially an API exposing capabilities to third-party services.

10) Network Slice Selection Function (NSSF): New feature in the world of CSPs, serving UEs with a selected Network Slice.

With the complexity, new features and speed introduced with 5GC, protecting the network is now more than ever a priority to protect users and 5G providers. As with other support systems, having to support a larger variety of services requires more resources and can lead to neglected security concerns. It is worth noting that since much of the communication within architecture is performed by the Internet Protocols (IPv4/IPv6), exploits found here are also inherited. Below we discuss some of the security threats 5GC faces and their countermeasures [25].

1) Network configuration manipulation: Attacks such as network configuration manipulation include routing attacks, also known as routing table poisoning, DNS manipulation, or tampering with cryptographic keys and policies. These attack types are targeted against AMF, DNS server, or PCF. From perspective of EPC, attacks would be aimed at the MME and PCRF. In order to mitigate attacks, some potential solutions could be to implement a least-privilege permission design and enforce reviews of change to all users [14]. When addressing DNS manipulation, DNS Security (DNSSEC) extensions can be used for countermeasure. DNSSEC provides a public key for verification of a DNS query result.

2) Malicious software: Software attacks on CN can cause unavailability of services or information destruction. Protecting against these attacks one should regularly run software updates patching vulnerabilities. Furthermore, a backup of vital data should be kept in case of data corruption.

3) Hardware manipulation: A common attack that could be used against physical hardware found in CN is known as a side-channel attack. At practical level, a side-channel attack uses current measurements from a given device to manipulate or obtain data. However, because side-channel attack is a physical attack, the exploit difficulty is high. Furthermore, protecting against side-channel attacks requires custom hardware increasing the cost of deployment. To mitigate against such attacks the hardware engineer might consider flattening the power usage to remove power peaks for the custom-designed hardware. For hardening of a processor one could randomize the pipeline, thereby messing up power and timings and for platform integrity in general, including firmware and software, a Trusted Platform Module (TPM) would be solution.

4) Information leakage: Unauthorized access to user data, cryptographic keys, and logs that are leaked. These types of attacks would be directed toward the SMF. Countermeasures could be to implement tunnel encryption with IPsec to provide privacy and integrity for IP packets.

5) Authentication abuse: The result of integrity violation by performing privilege escalation. Such attacks can be directed towards the AMF and Authentication and Key Agreement (AKA) protocol, which is a challenge-response protocol based on symmetric cryptography and a Sequence Number (SQN). Studies have found that a replay attack, which AKA defends against, can be modified with an Exclusive-OR (XOR) and a lack of randomness. To prevent this attack it is suggested that the conceal mechanism uses symmetric encryption [18].

6) Accidental: Even a well-designed and secured network can not be foolproof. Human error is inevitable and small misconfigurations may lead to security breaches. One way to mitigate these kinds of errors is to automate and remove the human aspect or to introduce a review of commits and monitoring.

B. Radio Access Network

Security for the Radio Access Network (RAN), is critical since it works as a gateway for all User Equipment (UE) and is in constant growth. With NSAs CN configured to an LTE-based Evolved Packet Core (EPC) and evolved Node B (eNB) together with next generation Node B (gNB) for the wireless network. As shown in Fig. 1 the wireless network consists of UE and base station (eNB/gNB) which together form RAN of NSA architecture. Looking at SA, RAN only consists of gNB and UEs [15][25].

1) Eavesdropping: Is an attack type whereby attacker is listening in on traffic being communicated to and from UE devices and gaining confidential information. To ensure

privacy, 5G network uses Subscriber Permanent Identifiers (SUPI), Subscriber Concealed Identifiers (SUCI), and 5G Globally Unique Temporary UE Identity (5G-GUTI). An example of a threat against the GUTI can be found with an incoming call or message, where the network pages the UE to its last known location. This page is sent in plain text without any authenticity or integrity protection over the paging channel. Exploiting paging message sent can result in location tracking. Using a strict refreshment of the GUTI can prevent such exploits [29].

2) Signaling threats: With the use of malware, signaling storms can be used to overload the RAN and the CN. In certain cases, this attack can also be used to drain the battery of a mobile device by utilizing the Power Saving Mode (PSM) introduced in 3GPP Release 12, which was meant to improve the battery life of UEs in an NSA. A malicious actor may flip this feature to drain battery life instead. A security experiment created towards this feature, reveals that it may in fact be feasible to shorten battery life. This study shows that the registration process is not interrupted even though integrity verification fails at the MME. Within this context, Tracking Area Update (TAU) message is vulnerable and can be modified to cause battery power to be drained. To mitigate this attack it is suggested that verification of the TAUs Attach Request is requested and that this feature should only be accessible after establishing security [19][20].

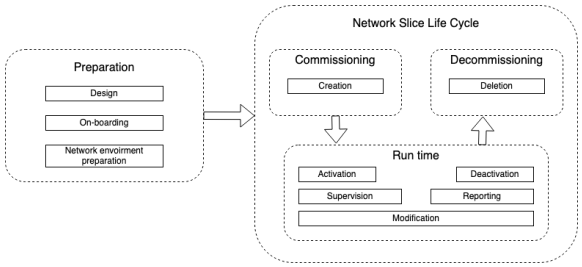

Fig. 3. Network Slice Life Cycle

C. Network Slicing

An important part of Network Slicing is the Slice Life Cycle (SLC) which consists of four phases, where each phase can be individually configured and thereby potentially be vulnerable to attacks [1][3][4].

1) Preparation: Phase one, preparation, is where designing, creation, and modification of the slice template are prepared, as illustrated in the preparation box in Fig. 3. A slice is not created at this point, but configurations for the creation are made and modified here.

Main attack surface at this phase is the SLC template. These attacks can include template tampering and open up for attacks due to misconfigurations, malware injection, poor implementation, or unpatched templates. Attacks made at this phase will carry over to the next three phases, and leave them more vulnerable. Poorly configured templates might also potentially leak sensitive data about the configuration, which could open up to other attacks not mentioned here.

To mitigate template tampering, one should include authenticity checks, to verify that the templates have not been tampered with. Mitigating the unwanted disclosure of sensitive data, encryption should be implemented to ensure the protection of data. To ensure that a template is properly configured, it is important to keep up-to-date with standards and the latest security patches [3][4].

2) Commissioning: Phase two, commissioning, is where the template is used to install and create resources based on the configurations in the template, as shown in the commissioning box in Fig. 3. This creation is managed by the slice provider API.

Since API manages the creation of slices, this would be an apparent attack vector. These attacks might include the creation of fake or malicious slices, or allow for other threat actors to interfere with the creation process of slices.

A way of mitigating the threat vectors during creation is to send templates to and from the API via a secure connection, such as TLS. This would prevent clear text configurations and thereby also minimize the risk of possible man-in-the-middle attacks. The API should also log the traffic and which services invoked the API [3][4].

3) Run time: The third phase, run time, is when slice has been created, deployed, and live. This is shown in run time box in Fig. 3 where the flow between the commissioning and decommissioning phase interacts with the run time phase. At this phase, the slice is in use and is also able to receive updates and configuration changes. During this phase, devices can be connected and disconnected dynamically.

The slice is susceptible to multiple threat vectors. A common and relatively accessible attack during this stage would be a Distributed Denial of Service (DDoS) attack. A DoS attack would flood the channel with a large number of requests, and consequently, stop the channel from receiving and sending data. It is important to note, that the API is still a relevant attack vector during the third phase, as it is still open to configuration changes.

Mitigation for the API from phase two is still relevant in this phase too. Mitigation techniques for DDoS attacks can be hard to implement, but network slicing offers the ability to isolate individual slices [2]. This technique can be helpful in mitigating a DDoS attack, but will not be effective if the DDoS attack is carried out at a large scale [3][4].

4) Decommissioning: The final and fourth phase, decommissioning, is where the slice is destroyed and resources are released. This is illustrated in Fig. 3 as the run time sending a decommissioning signal, and in turn, starts the decommissioning phase. The decommissioning rules are determined by provisioning rules and can be configured as well as the other provisioning rules in the 3 latter phases.

Like with previous phases, configuration of provisioning (decommissioning) can be wrong and open up for attack vectors. Such attack vectors might include, exposure of data during decommissioning and resource consumption.

To mitigate the exposure of data during decommissioning, one must ensure the deletion of sensitive data through the provisioning rules. The same mitigation technique applies to wrongful resource consumption. It is important to monitor the resources that a slice takes up, and whether they are being freed upon decommission [3][4].

D. Legacy Communication

As we enter into the next generation of mobile technology, network operators may still want to keep the legacy technol-

ogy alive, to support legacy users who have not yet upgraded their devices. However, keeping older technologies alive and in conjunction, keeps the vulnerabilities inherent with the next generation. Legacy protocols such as GPRS Tunneling Protocol (GTP), which allow data packets to be transported to and from different wireless networks, have been used since 2G and are known for more security flaws [16][17][27].

1) Botnets: Still a vulnerability for 5G as it was for 4G. A botnet is a large group of devices infected by malware that are configured to perform malicious attacks against a network node. Countermeasures against botnets are to monitor user activity, such as failed login attempts, that might indicate suspicious behavior.

2) Bidding down: An attack type that forces devices to lower-quality network protocols, resulting in degradation in the quality of service. To protect against such attacks, 5G architecture implements a Security Edge Protection Proxy (SEPP) that protects the traffic being passed between nodes. Furthermore, SEPP also receives all application layer messages and analyses them before forwarding the messages.

3) Protocol-based attack: GTP is a protocol with well-known flaws, that can be used to spoof user information. One such weakness is that the GTP does not validate the user's physical location, and can be used to make a malicious actor spoof the user traffic's location. Although the transition to a "full service" 5G SA is coming, protocols such as GTP will still be used for serving text messages. The only proper way to counter the GTP will be to abolish it.

E. Software Defined Networking

When looking at security aspects of SDN, it is important to mention that control plane is placed on an SDN controller, and data plane is located on a physical, or when using NFV, a virtual switch. This is important because each plane is susceptible to different kinds of attacks. Having a centralized controller, also means that controller becomes more attractive from an attacker's standpoint. Having control over the control plane can cause a variety of attack vectors down the network chain. Attacks on control plane could be seen as message spoofing, between the APIs. Through message spoofing, attacker needs to activate a new flow. If attacker is successful in spoofing controller, attacker would be able to control flow going through the SDN and effectively disable policies allowing for further pivoting through the network. SDN is vulnerable to a wide range of attacks, as SDN handles many critical components of the network [11][13][24].

1) Address Resolution Protocol (ARP) spoofing attack: Attacker could try to generate a new node by replicating identity information of a destination device. This will allow attacker to authenticate as a replicated node. This will also assume the role and security responsibility of the node, and thereby grant unwanted access to network. To mitigate this kind of attack, there exist some proposed solutions. ARP authentication works by modifying the ARP protocol to not process ARP packets unless it contains predefined cryptographic code. S-ARP and TARP are examples. The main drawback of using a technique like this is backward compatibility. By using a modified protocol, it no longer supports devices only able to communicate through ARP. Another proposed solution is Dynamic ARP Inspection (DAI). DAI works by intercepting all ARP requests and responses, dropping packets with invalid IP-to-MAC address mappings [21][22][23].

2) Man in the Middle (MitM) attack: In context to the above-explained topic, ARP, MitM attacks leverage ARP spoofing to intercept data. MitM attacks occur in the forwarding-control link, and MitM actor will be able to sniff data between the host and a client. Mitigating this can be done by securing connection that data is transmitted through. This can be done by using TLS, which should be enabled by default, but also by securing the system against ARP spoofing [21][22][24].

3) Denial of Service (DoS) attack: The main goal of a DoS attack is to flood the host with traffic, and in turn, make host unresponsive, or slow down the traffic. This would lead to resource exhaustion and could potentially bring affected channel down, or even the host if badly configured [21][22][24].

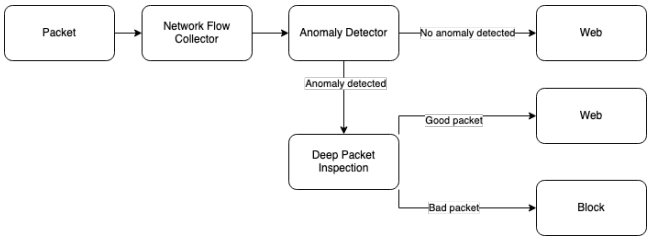

Fig. 4. Flow of a packet handled by NFA and DPI

F. Multi-Access Edge Computing

Due to the many capabilities provided by MEC, the security aspect also becomes more complex. This also means that 5G can facilitate many devices, such as IoT devices. These capabilities for a large number of connections, also expose the network to potential exploitation. The most obvious exploit involving a large number of devices is a DDoS attack. DDoS attacks in 5G can be very difficult to mitigate. The most effective way of mitigating DDoS attacks on the MEC level is through *Network Flow Analysis* (NFA) and *Deep Packet Inspection* (DPI). As shown in Fig. 4, the methods should be used in combination [6][7].

1) Network flow analysis: This method deals with anomaly detection through an analysis of the *Network Flow*. A Network Flow is defined as a collection of packets going through an observation point in the network. The packets are collected for a specific period and the *flow keys* are collected for comparing the traffic. The flow keys are just a subset of attributes for a packet, and therefore the whole packet is not analyzed at this point in time. The flow keys collected may include (but are not limited to) attributes such as: IP source address, source port, destination address, destination port, package length, and the protocol used. Network Flow Analysis serves the purpose of deciding whether given packets should be further analyzed by the DPI. If a package is selected for further inspection, the flow keys, alongside the package are collected to an external flow collector (fig. 4). The main purpose of dividing the analysis into anomaly detection and DPI is to alleviate the system's need to do full package analysis, as this operation can be very resource intensive and in turn, reduce performance. The NFA might

also benefit from the use of machine learning, to better detect possible threat vectors or anomalies [5][6].

2) Deep Packet Inspection (DPI): DPI is handled at application layer of OSI model. DPI differs from the traditional packet analysis by also including application layer. DPI analyses packets and locates identifies, classifies, reroutes, and blocks packets. In a security context, DPI would be used to analyze a packet and if it is classified as malicious or blocked content, DPI will block packet. The specific DPI configuration can differ from providers, as configuration is managed by either Internet Service Provider (ISP), enterprise or network manager [5][6].

IV. DISCUSSION

Our research has shown that 5G network can be vulnerable to a variety of different attack vectors. Mitigation is crucial to provide users with secure connections. TABLE 1 shows attack vectors we found in different components of network with an overview of attacks along with proposed mitigation. Exploit and mitigation difficulties are combination of required skills and resources as we are able to estimate. We found that each component has its own vulnerabilities, while also some share attack types. This means that there is no way to address threats with a single solution. Mitigation requires maintainer to address threats at the component level.

Component	Attack	Exploit difficulty	Mitigation difficulty	Mitigation Method
Network Slicing	Template tampering	High	Low	File integrity
Network Slicing	Slice Tampering(fake slice)	High	Low	Secure transfer of slice to and from API
Network Slicing	Data exposure	High	Low	Correctly configured slice deletion
Network Slicing	DDoS	Low	Mid	Slice isolation and traffic analysis
Software Defined Networking	ARP spoofing	Mid	Low	Implement S-ARP or TARP
Software Defined Networking	Man in the Middle	Low	Low	TLS or SSL encrypted data transfer
Software Defined Networking	DoS	Low	Mid	Traffic analysis and blocking
Multi-Acess Edge Computing	DDoS	Low	Mid	Network Flow Analysis in combination with Deep Packet Inspection
Core Network	Network configuration manipulation	High	Mid	Implement a least-priviledge permission design
Core Network	Malicious software	Mid	Low	Implement patch management
Core Network	Hardware Maniuplation	High	High	Power flattening, Pipeline randomization and TPM
Core Network	Information leakage	Low	Low	Encryption and authentication strengthening
Core Network	Authentication abuse	Mid	Mid	Hardening of protocols
Core Network	Accidential	Low	Low	Reduce handheld processes
Radio Acess Network	Eavesdropping	Low	Low	TLS or SSL encrypted data transmission
Radio Acess Network	Signaling threats	Mid	Low	Verifying requests
Legacy Communication	Botnets	High	Mid	Traffic analysis and blocking
Legacy Communication	Bidding down	Mid	Mid	Implement SEPP
Legacy Communication	Protocol-based Attack	Mid	Mid	Minimise the use of depricated protocols

TABLE I
ATTACK VECTOR OVERVIEW

V. CONCLUSION

From our research, we found that 5G comes with many new capabilities. 5G provides the ability to facilitate a large number of devices, including IoT devices, while also being able to provide ultra-low latency and high bandwidth. These features require a new network structure, which 5G is able to provide. The new structure allows for a more flexible environment through virtualisation. This means that a piece of hardware may host several services, e.g., SDN, MEC, NS.

It all leads to increased complexity within the network and larger attack surface, which opens up for more possible vulnerabilities. We found that even though the complexity of the network has increased, maintainability of each individual component was made easier. Mitigation techniques must be applied to every service, and due to virtualisation, task of maintaining and patching a service has been made easier.

In addition to the ease of configuration, it is also important to ensure correct configurations are being applied, while also securing configurations so they cannot be tampered with.

Our research covers important attack vectors within 5G and identifies directions of future research. We estimated exploit difficulties and they indicate how to prioritize. Securing 5G network is still an ongoing task, and additional threats are still to be uncovered.

REFERENCES

[1] Christopher Cox, “An Introduction to 5g, The New Radio, 5G Network and Beyond”, Vol. 1, 2021.

[2] Stan Wong, Bin Han, Hans. D Schotten, “5G Network Slice Isolation”, Network 2, No. 1, 2022.

[3] R. Dangi, A. Jadhav, G. Choudhary, N. Dragoni, M.K. Mishra, P. Lalwani, “ML-Based 5G Network Slicing Security: A Comprehensive Survey”, Future Internet 2022, 14, 116, 2022.

[4] GSMA “E2E Network Slicing Architecture”, Official Document NG.127-E2E Network Slicing Architecture, 2021.

[5] Marian Gusatu, Ruxandra F. Olimid, “Improved security solutions for DDoS mitigation in 5G Multi-access Edge Computing”, Department of Computer Science, University of Bucharest, 2021.

[6] Pasika Ranaweera, Anca Jurcut, “MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures”, ACM Comput. Surv., Vol. 54, No. 9, 2021.

[7] Abderrahime Filali, Amine Abouaomar, Soumaya Cherkaoui, Abdellatif, Kobanne, Mohsen Guizani, “Multi-Access Edge Computing: A Survey”, IEEE, Vol. 8, 2020.

[8] Xiaowei Zhang, Andreas Kunz, Stefan Schröder, “Overview of 5G security in 3GPP”, 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 2017.

[9] Shane Fonyi, “Overview of 5G Security and Vulnerabilities”, The Cyber Defense Review, Vol. 5, No. 1, 2019.

[10] Anand R. Prasad, Sivabalan Arumugam, Sheeba B, Alf Zugenmaier, “3GPP 5G Security”, Journal of ICT Standardization, Vol. 6, Combined Special Issue 1 & 2, 2018.

[11] S. Sullivan, A. Brighente, S.A.P. Kumar, M. Conti, “5G Security Challenges and Solutions: A Review by OSI Layers”, IEEE Access, Vol. 9, 2021.

[12] Tashi Tobgyel, Shankar Duraikannan, Vinesh Thiruchelvam Raed Abdulla, Yvette Susiapan, “SDN Based 5G Network Architecture For Latency Critical Services”, Solid State Technology, Vol. 63, 2020.

[13] J. Yao, Z. Han, M. Sohail, L. Wang, “A Robust Security Architecture for SDN-Based 5G Networks”, Future Internet MDPI, 2019.

[14] S. Park, D. Kim, Y. Park, H. Cho, D. Kim, S. Kwon, ”5G Security Threat Assessment in Real Networks”, Sensors, 2021.

[15] 3GPP, ”Release 15”, 3GPP TR 21.915 V15.0.0, 2019.

[16] H. Kim, ”5G core network security issues and attack classification from network protocol perspective”, J. Internet Serv. Inf. Secur., 2020.

[17] Roger Piqueras Jover, Vuk Marojevic, ”Security and Protocol Exploit Analysis of the 5G Specifications”, IEEE Access PP(99):1-1, 2019.

[18] R. Borgaonkar, L. Hirschi, S. Park, Shaik, ”A. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols”, Proc. Priv. Enhancing Technology, 2019.

[19] Cisco, “Power Saving Mode (PSM) in UEs”, https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21/MME/b_21_MME_Admin/b_21_MME_Admin_chapter_0111010.pdf

[20] Altaf Shaik, Ravishankar Borgaonkar, ”New Vulnerabilities in 5G Networks”, Technische Universität Berlin and Kaitiaki Labs.

[21] Anmol Mahajan, Abhinav Bhandari, “Attacks in Software-Defined Networking: A Review”, ICICCR-2020, 2022.

[22] Aayush Pradhan, Rejo Mathew, “Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)”, Procedia Computer Science 171 (2020), 2022.

[23] A.M. AbdelSalam, A.B. El-Sisi, V.R. K, “Mitigating ARP Spoofing Attacks in Software-Defined Networks”, ICCTA 2015.

[24] A.A. Barakabitze, A. Ahmad, R. Mijumbi, A. Hines, “5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges”, Computer Networks Volume 167, 2020.

[25] M.N.I. Farooqui, J. Arshad, M.M. Khan, ”A Layered Approach to Threat Modeling for 5G-Based Systems”, Electronics 2022, 11.

[26] Statista, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[27] Y. Hao, “Investigation and Technological Comparison of 4G and 5G Networks”, Journal of Computer and Communications, 9, 36-43, 2021.

[28] H. Kim, J. Lee, E. Lee, and Y. Kim, ”Touching the untouchables: Dynamic security analysis of the lte control plane”, Proc. of the 2019 IEEE Symposium on Security and Privacy (SP’19), IEEE, 2019.

[29] Tao W, Mansour G., ”Security Analysis Of 5G Mobile Networks”, Technical Paper Prepared for SCTE.ISBE, 2019.