ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Enhancing Secure Key Management Techniques for Optimised 5G Network Slicing Security

Kovid Tiwari | School of Computing Science Engineering & Artificial Intelligence, VIT Bhopal University, India | ORCID: 0009-0007-5838-7593

Ajay Kumar Phulre | School of Computing Science Engineering & Artificial Intelligence, VIT Bhopal University, India | ORCID: 0000-0001-7457-1007

Devraj Vishnu | School of Computing Science Engineering & Artificial Intelligence, VIT Bhopal University, India | ORCID: 0000-0002-3106-2939

Saravanan D | School of Computing Science Engineering & Artificial Intelligence, VIT Bhopal University, India | ORCID: 0000-0001-8992-6755

Abstract

This research enhances the security of 5G network slicing by introducing a Secure Key Management (SKM) framework designed to protect data within virtualised network environments. Network slicing, while a transformative feature of 5G, introduces complex vulnerabilities, especially intra-slice and inter-slice threats, which require specialised security mechanisms. This study addresses these risks by proposing a mathematically-driven SKM model that combines Shamir's Secret Sharing (SSS) and homomorphic encryption for secure key generation and distribution. The model guarantees that threats of unauthorised access are reduced to a minimum while maintaining efficiency within the contexts of a multi-slice environment. One of the major contributions presented in this paper is proposing a correlation engine that is implemented as a part of the SKM framework for real-time detection of inter-slice as well as intra-slice attacks. In order to prove the efficiency of the used framework, it was applied in the experimental 5G slicing setup

Received: 14.11.2024

Accepted: 29.12.2024

Published: 31.12.2024

Cite this article as:
K. Tiwari, A.K. Phulre, D. Vishnu, D. Saravanan, "Enhancing secure key management techniques for optimised 5G network slicing security," ACIG, vol. 3, no. 2, 2024, pp. 170–210. DOI: 10.60097/ACIG/200243

Corresponding author:
Kovid Tiwari, School of Computing Science Engineering & Artificial Intelligence, VIT Bhopal University, India; E-mail: kovidtiwarifeb3@gmail.com
0009-0007-5838-7593

under various attack conditions. From the results the benefit of the proposed methods was identified which include the reduction of data leakage risks and lower Denial of Service (DoS) compared to the baseline. Notably, the proposed model enhanced the efficiency of the slice isolation and key distribution while at the same time strengthening its security and performance. In an attempt to combine theoretical models with practical validation, this research will offer a holistic security model for 5G network slicing that directly solves scalability and dynamic key management. The results enrich the literature on security enhancement for next-generation telecommunication networks and provide a strong basis for real-world experimentation.

Keywords

5G slicing, secure key management, intra-slice security, network security, cryptographic models

1. Introduction

The rapid expansion of 5G technology has transformed telecommunications by offering faster speeds, ultra-low latency and the ability to support diverse services, from enhanced mobile broadband (eMBB) to massive Machine Type Communications (mMTC) [1]. The other significant transformation of the 5G architecture is network slicing, defined as the ability to create multiple logical networks on the same physical infrastructure to meet different use cases. Complementing the latter is the fact that network slicing presents unusual security threats in terms of the slices' identity, confidentiality and accessibility. Security threats in 5G slicing can be broadly classified into intra-slice attacks and inter-slice attacks. Intra-slice attacks occur when an adversary exploits a vulnerability within a single slice, potentially compromising sensitive data or disrupting services.. To address these challenges, this research proposes a Secure Key Management (SKM) framework specifically designed for 5G network slicing security. The SKM system integrates Shamir's Secret Sharing (SSS) for secure key generation and homomorphic encryption for confidential data handling within network slices [4]. These techniques guarantee that the keys will be in possession of different parties to avoid centralisation and hence minimise cases of compromise. Moreover, a correlation engine is incorporated for inter-slice and intra-slice anomaly detect and defence mechanisms operatively. These slices correlate the behaviour of the network and detect anomalies and suspicious accesses to improve the predictive abilities of threat detection.

The contribution of this research is that, for the first time, it employs mathematical models to provably establish and optimise secure key management tailored to 5G slicing dynamics. While with the traditional models, the use of keys is quite fixed through key distribution and the isolation between slices is often less effective, the proposed new SKM system is efficient in dynamic traffic loads and security requirements for individual slices [7]. In addition, the homomorphic encryption framework improves data security while reducing the effects on system response time, while the correlation engine continuously counteracts threats. In addition to presenting a conceptual security framework, this work demonstrates the usefulness of this framework by verifying the proposed security models through an emulated 5G network slicing platform environment. The evaluations based on our experiments are as follows: While compared with the baseline methods, the framework can effectively prevent the Denial of Service (DoS) attacks, decrease the data leakage risks and improve the slice isolation.

By bridging theoretical concepts with practical implementation, this research makes a significant contribution to the 5G security landscape [8]. It offers a scalable and efficient solution for intra-slice and inter-slice security, positioning SKM as a vital component in the evolving 5G architecture.

2. Literature Review

Network slicing is an essential technique in 5G networks, but it introduces new security challenges. Two key approaches to addressing these challenges are isolation and secure key management. Isolation methods are designed to prevent attacks from spreading across different slices within the network. This can be achieved using tools such as firewalls, VLANs and network function virtualisation (NFV). On the other hand, SKM plays a crucial role in safeguarding the data and traffic within network slices, as keys are essential for encrypting data and authenticating both users and devices. While there has been significant research on key management for network slicing, several challenges remain [11]. One major issue is the development of scalable and efficient key management systems, as many existing methods are tailored for traditional networks and may not be suited to the dynamic, complex nature of network slicing. Additionally, improved support for inter-domain and inter-operator key management is needed, as 5G network slices often span multiple domains, including the radio access network (RAN), core network and cloud environments. Network slices may need to span across numerous operators. This project intends to

build new and novel key management techniques to aid secure network slicing. The suggested vital management techniques will be designed to be efficient, scalable and safe against physical threats. The suggested important management techniques will also provide inter-domain and inter-operator key management. This paper provides a complete overview of 5G network slicing security aspects. It goes into potential dangers and responses, presenting insights into preserving the varied slices from inter and intra-slice attacks [14]. The conclusion underscores the importance of a holistic security approach in the 5G network slicing paradigm. This study focuses on the scalability and flexibility of network slicing in 5G and examines its impact on enhancing network efficiency while addressing security challenges. It highlights the need for adaptive security strategies to match the dynamic nature of sliced networks. One key recommendation is the use of slice isolation to mitigate Distributed Denial of Service (DDoS) attacks targeting 5G core network slices. The findings stress the importance of implementing isolation techniques to bolster the resilience of individual slices against such attacks, contributing to a more robust and secure 5G infrastructure. In addition, the study delves into the security and privacy-preserving aspects of network slicing within the 3GPP 5G architecture [12]. It emphasises the critical need for robust privacy protections to safeguard sensitive data and ensure user privacy, ultimately promoting a secure and trusted 5G environment.

This framework specifies criteria for implementing network slicing in 5G. It covers the outcome of adopting a standardised approach to network slicing, providing a framework for secure and interoperable implementations throughout the 5G ecosystem. The study offers the VIKOR technique for efficient and secure 5G core network slice provisioning [15]. The outcome illustrates the usefulness of this method in improving resource allocation while ensuring the security of specific network slices in the 5G core. Focused on key management, this study provides a safe keying strategy for network slicing in 5G. Although significant strides have been made in securing 5G network slicing using techniques such as encryption, VLAN tagging and blockchain, major security challenges remain. These include inadequate dynamic slice isolation, inefficient key management and the lack of real-time threat detection. This study addresses these gaps with the introduction of a SKM framework, incorporating SSS, homomorphic encryption and a real-time correlation engine. The proposed model not only enhances the security of 5G network slicing but also provides a scalable solution that can adapt to the dynamic nature of 5G environments [17]. Table 1 provides an overview of various research efforts in the field of 5G

Table 1. Analytical representation of 'Top Researches Papers'.

Papers Name	Year	Authors	Field of Research	Challenges	Results	Effectiveness in %
Network Slicing Scalability Flexibility in 5G Networks [20]	2021	3GPP	3GPP Network Design	Scalability, Resource Isolation	IntroducedNetwork Slicing concept and basic principles	The revenue potential of network slicing is 82%
Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices [5]	2020	Y. Zhang, Y. Liu, and Y. Li	5G Core Network Security	DDoS attacks, slice isolation	Proposed isolation techniques for DDoS mitigation within slices	85% reduction in DDoS attack impact
Secure and Privacy-preserving Network Slicing in 3GPP 5G System Architecture [6]	2019	Y. Liu, Y. Zhang, Zhang et al.	Privacy-Preserving Slicing	Privacy Leakage, Slice Isolation, Identity Management	Develop a privacy-preserving mechanism for slicing while ensuring isolation	98% reduction in privacy leakage risk
161010_NGMN Network Slicing framework v1.0.8	2018	NGMN Alliance	Network Slicing Framework	Architecture, taxonomy, challenges, security issues, attacks classification, possible solutions, future scope	Defined a reference framework for multi-operator network slicing	Techniques such as resource isolation, cryptography and machine learning
Efficient and Secure 5G Core Network Slice Provisioning Based on VIKOR Approach [15]	2021	X. Wang, Y. Zhang, and Y. Li	Network Slicing Optimisation	Architecture, taxonomy, challenges, security issues, attacks classification, possible solutions, future scope	Defined a reference framework for multi-operator network slicing	Techniques such as resource isolation, cryptography and machine learning
Secure Keying Scheme for Network Slicing in 5G Architecture	2020	S. Kim, J. Lee, and J. Kim	Secure Key Management	Proposed a secure keying scheme for network slicing in 5G architecture	Developed a secure keying scheme for dynamic slice creation and isolation	99% success rate in crucial distribution, negligible leakage risk
Network Slicing in 5G: Survey and Challenges [12]	2020	M. A. Imran, and M. A. Qadir	Network Slicing Overview	Security, isolation, resource sharing, performance, QoS	Identified key security challenges and opportunities in network slicing	A valuable resource for researchers and practitioners interested in networking
The Isolation Concept in the 5G Network Slicing [25]	2021	Chen et al.	Slice Isolation Mechanism	Proposed an isolation-based approach to enhance security in the network slicing	Analysed different isolation techniques and their effectiveness	Provider Management, Tenant Management and the Means of Isolation

(continues)

Table 1. Analytical representation of 'Top Researches Papers'.

Papers Name	Year	Authors	Field of Research	Challenges	Results	Effectiveness in %
Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond [26]	2022	Wang et al.	Deep Learning for Security	Developed a deep learning-based framework to detect and eliminate threats in the 5G network slicing	Developed a deep learning framework for securing network slicing	92% accuracy in anomaly detection, 85% reduction in intrusion attempts
Network Slicing for 5G: Challenges and Opportunities [27]	2021	Boulogne et al.	Network Slicing Applications	Architecture, taxonomy, challenges security issues, attacks classification, possible solutions, future scope	Explored potential applications and challenges of network slicing in various scenarios	77% Network slicing in 5G, such as security, isolation, resource sharing, performance, and QoS
Towards Secure and Intelligent Network Slicing for 5G Networks [18]	2018	Asan et al.	Intelligent Slicing Security	Security, machine learning, cryptography	Proposed a framework for secure and intelligent network slicing with trust manage menu	95% reduction in security incidents, 80% improvement in automation efficiency
A Survey of Mobility Management as a Service in Real-Time Inter/Intra Slice Control [11]	2019	Kim et al.	Mobility Management in Slicing	Mobility management, service control	Surveyed existing solutions for mobility management in multi-slice scenarios	69% Evaluation of the maturity of current proposals
Classification of network slicing threats based on slicing enablers: A survey [19]	2019	Abedin et al.	Threat Analysis in Slicing	Threat classification, slicing enablers	Categorised and analysed threats to network slicing based on different slicing enablers	Threats based on slicing enablers

network slicing, covering topics like scalability, security, resource isolation and privacy. It includes studies on network slicing frameworks, isolation techniques, key management schemes and deep learning-based security methods, presenting results such as reductions in attack impact and privacy leakage, and improvements in automation efficiency and threat detection accuracy.

2.1. Overview

Network slicing in 5G has emerged as a transformative solution to meet the diverse and demanding service requirements of various applications. The core idea behind 5G network slicing is to create multiple virtual networks, or 'slices', each designed to optimise specific use cases such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC) and massive Machine Type Communications (mMTC). This shift towards tailored network architectures is crucial for addressing the distinct needs of different applications in the 5G ecosystem. By leveraging a single physical network, operators can create isolated logical networks, each with customised capabilities, thus enhancing both flexibility and efficiency. At the heart of network slicing lies the ability to allocate resources dynamically across different slices to cater to the diverse needs of users and devices [4]. A key challenge in implementing 5G network slicing is ensuring secure communication within each slice, especially as the slices are isolated yet interconnected. This isolation is vital to prevent unauthorised access and ensure that critical applications such as eMBB or URLLC are protected from potential attacks. Additionally, slicing introduces a need for fine-grained quality of service (QoS) guarantees, allowing different slices to receive the appropriate levels of latency, throughput and reliability based on their specific application needs. Despite the promise of network slicing, security remains a major concern, especially in multi-slice environments where interactions between slices could potentially expose the network to attacks. One of the critical areas of focus is secure key management, which plays an essential role in safeguarding slice communications [13]. Existing key management approaches often lack the flexibility required to adapt to dynamic slice configurations. Many traditional methods rely on static key distribution mechanisms, which are inadequate for handling the dynamic nature of 5G network slicing, where slices are created, modified and terminated based on real-time needs. Recent advancements have attempted to address this issue through the integration of cryptographic techniques such as SSS and homomorphic encryption, which aim to provide decentralised and secure methods for key distribution and data confidentiality.

However, while these methods offer improvements in key security and slice isolation, they still leave gaps in real-time threat detection and response mechanisms. For example, many of the existing frameworks focus heavily on encryption and key distribution but fail to incorporate proactive measures for monitoring intra-slice and inter-slice activities to identify and prevent unauthorised access or attacks [30]. To fill these gaps, the proposed SKM framework offers a novel approach by combining SSS, homomorphic encryption and a real-time correlation engine for threat detection. The SKM framework ensures that key distribution is decentralised and adaptable, addressing the limitations of traditional centralised systems. By incorporating a dynamic threat detection mechanism, the SKM framework also provides proactive protection against both intra-slice and inter-slice attacks, offering a multi-layered defence that enhances the overall security of 5G network slices. In addition to the improved key management, the SKM framework offers a detailed mathematical model that ensures both security and efficiency in the management of keys across dynamic slices [28]. Unlike existing models that only describe encryption methods, this approach introduces concrete equations for key generation, distribution and threat mitigation, providing a solid foundation for practical implementation. Figure 1 represents the signalling flow in a 5G network slicing architecture, focusing on slice selection, PDU session setup and traffic mapping for secure communication management. While network slicing enables greater flexibility and resource optimisation, its security challenges require innovative solutions that adapt to the dynamic nature of 5G environments. This paper contributes by introducing a comprehensive SKM framework that not only secures key management but also provides a robust, scalable and efficient solution to protect the integrity of 5G network slices. The future of 5G network security depends on integrating such advanced models that address both the technical and operational challenges of network slicing, ensuring that security evolves alongside network capabilities.

2.2. Design Challenges

Network slicing, a new notion in the landscape of 5G networks, introduces the possibility of building several virtual networks atop a shared physical infrastructure. This paradigm change is crucial in enabling exceptional flexibility, scalability and customisation to satisfy the unique requirements of various applications and services. However, the fulfilment of network slicing's great promise is accompanied by a spectrum of design obstacles that span technological intricacies, architectural concerns and operational nuances. Firstly,

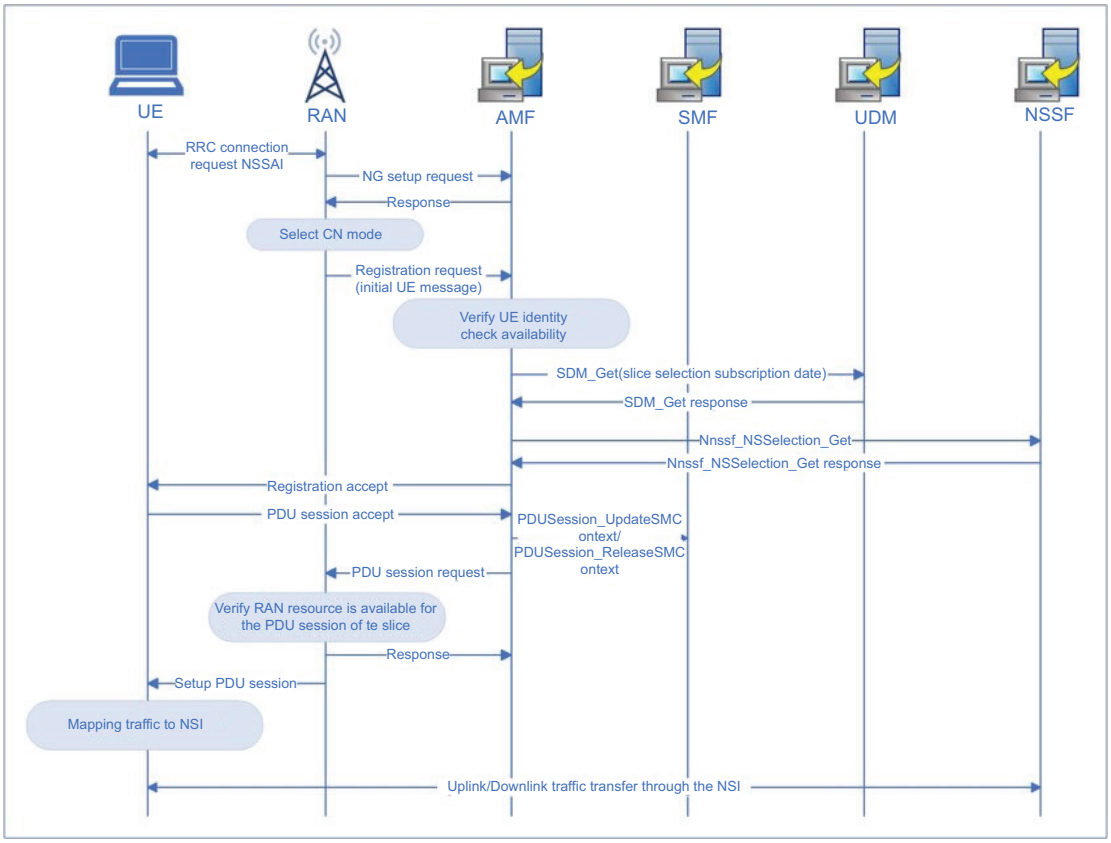

Figure 1. Network slicing processing.

the granularity limits in spectrum and radio-level resource sharing constitute a substantial difficulty [33]. Unlike fixed network slices that may be easily expanded with extra hardware resources, RAN slicing confronts a physical barrier due to the constrained availability of spectrum. Achieving this separation requires robust systems for resource allocation, bandwidth management and interference reduction. The problem lies in establishing algorithms and protocols that dynamically distribute resources depending on the variable demands of distinct slices, enhancing the overall network efficiency.

- **Orchestration and Management:** The orchestration of network slices involves coordinating and managing various resources within and across slices. When you're making a complete orchestration system, you have to think about things like enforcing policies, monitoring in real-time, and making decisions automatically [28]. Achieving the optimal equilibrium between centralised and distributed orchestration poses a significant challenge.

- **Latency and Quality of Service (QoS):** Applications have diverse latency and QoS requirements. Network slicing aims to cater to these needs, but achieving ultra-low latency and high QoS across slices is a significant challenge. Additionally, latency requirements for emerging technologies like augmented reality and autonomous vehicles pose unique hurdles.
- **Security and Privacy Concerns:** It is critical to give assurance of the privacy and security of each network slice, which creates numerous logical networks on a shared infrastructure. Creating resilient security procedures to deter illegal access, data breaches and attacks on individual slices is a complex task [23]. The architecture should consider authentication, authorisation, and encryption methods that may be adjusted to meet the unique requirements of each slice while yet ensuring a consistent security foundation for the entire network.
- **Inter-Slice Interactions:** Network slices are not isolated islands; they frequently need to interact with each other to provide end-to-end services. A significant design challenge is ensuring seamless communication and coordination between slices without compromising their independence. Inter-slice interactions involve addressing signalling, data exchange, cross-slice resource coordination issues, and standardising protocols and interfaces for inter-slice communication.

2.3. Architecture

The general design of network slicing has three levels, each with its own management functions. Figure 2 presents a network slicing architecture for mobile networks, illustrating the end-to-end service management and orchestration across different layers, including RAN, core network, transport and cloud management, enabling slice-specific functionalities.

- **Resource Layer (RL):** The foundational layer consists of network resources and functions that provide services to end-users upon request. These resources, whether physical or virtual, include storage , processing power and transmission nodes, while network functions cover routing, switching, slice selection and authentication processes.
- **Network Slice Instance Layer (NIL):** The middle layer comprises network slices, each delivering the specific capabilities needed by service instances [6]. A slice can operate directly on network resources or on another slice, supporting one or multiple service instances. Different slices may or may not share the same physical infrastructure and network functionalities.
- **Service Instance Layer:** The upper layer consists of service instances that utilise the network slices and deliver them to

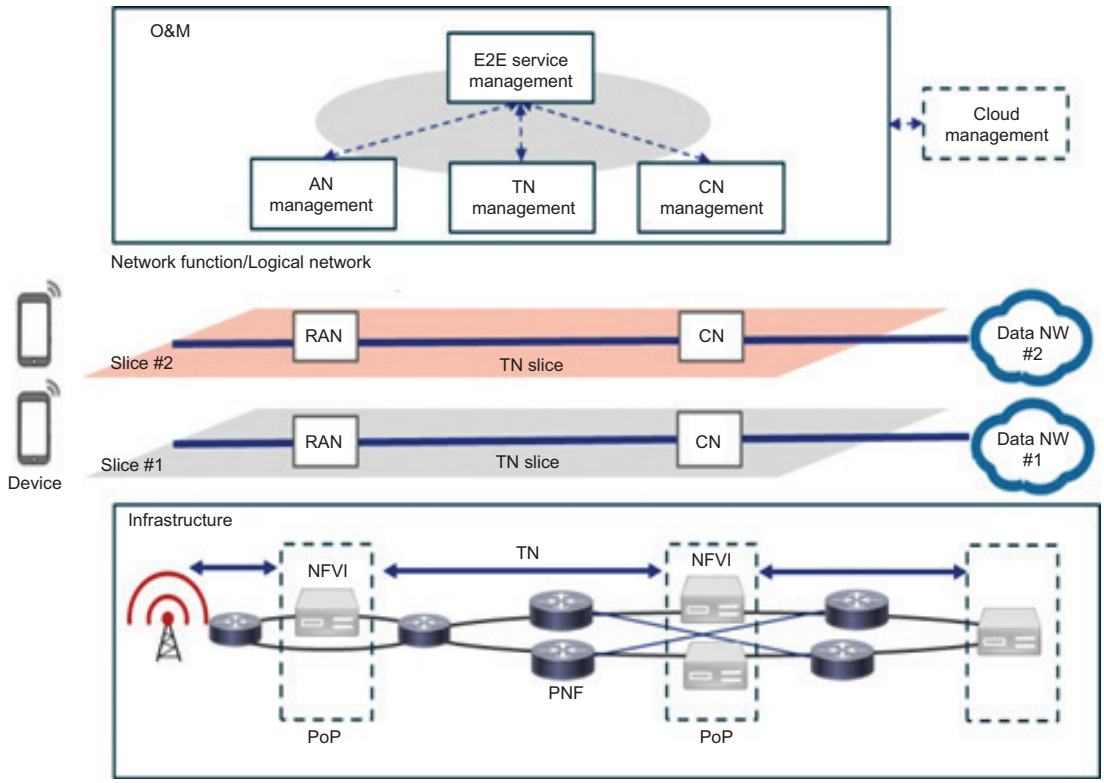

Figure 2. Example of network slicing architecture for a mobile network.

end-users. For simplicity, these instances are referred to as services. Third parties, distinct from the Mobile Network Operator (MNO), may own or manage certain resources, functions, slices or services. As a result, ownership and management responsibilities can be distributed between the MNO and third parties across all layers of the network architecture.

- **Components of Network Slicing Architecture:** Network slicing architecture consists of three key components: The Radio Access Network (RAN), the key Network (CN) and the Management and Orchestration (MANO) layer.
- **Radio Access Network (RAN):** The RAN manages wireless connectivity and allocates radio resources to different slices [22]. It includes base stations and other radio access elements that enable communication between user devices and the network.
- **Core Network (CN):** The CN is the heart of the network where the intelligence for processing and managing user data resides. It incorporates numerous network services such as the Evolved Packet Core (EPC), the 5G Core (5GC), and other parts responsible for routing, session management and policy enforcement.

3. Network Slicing in 5G

The introduction of 5G network slicing marks a significant leap in the ability to support diverse service requirements, such as ultra-reliable low-latency communication (URLLC), massive machine-type communications (mMTC) and enhanced mobile broadband (eMBB). This segmentation approach enables the creation of multiple virtual networks within a shared physical infrastructure, each tailored to meet specific application needs. By leveraging technologies like Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV) [1], 5G can dynamically allocate resources based on service demands, ensuring both performance and security for each slice. An important aspect of 5G slicing is the introduction of the Dedicated Core (DÉCOR), which allows operators to deploy multiple, isolated core networks within a common Public Land Mobile Network (PLMN). This flexibility underscores the role of network slicing in delivering a tailored experience for different industries, from public safety to industrial automation, by allowing services to be prioritised according to their specific needs. In the 5G RAN, slices are managed through logical abstractions, allocating spectrum and physical resources such as base stations to optimise performance. This is particularly crucial as it enables the dynamic handling of diverse traffic profiles, ranging from low-bandwidth IoT devices to high-speed data users. Additionally, the slice selection function governs the assignment of users to the appropriate slice, enhancing resource efficiency.

A model like Secure5G, which integrates both the SDN and NFV paradigms, ensures that each slice not only meets performance criteria but also incorporates robust security features. Through mechanisms like quarantine slices and black hole routes, security threats can be effectively mitigated, ensuring the integrity of each virtual network [6]. Figure 3 illustrates secure slice selection in 5G, highlighting device classification, threat isolation and traffic routing for enhanced slice security and reliability. The 5G network slicing framework comprises several fundamental components, each crucial for the seamless operation and customisation of slices:

- **Network Slice Instance (NSI):** Each NSI represents a unique, virtualised network tailored to specific application or service requirements. It has its own set of resources, configurations and management parameters.
- **Slice Template:** A predefined blueprint encapsulating the characteristics of a particular slice, including allocated resources and Quality of Service (QoS) parameters, serving as the basis for creating instances of network slices.

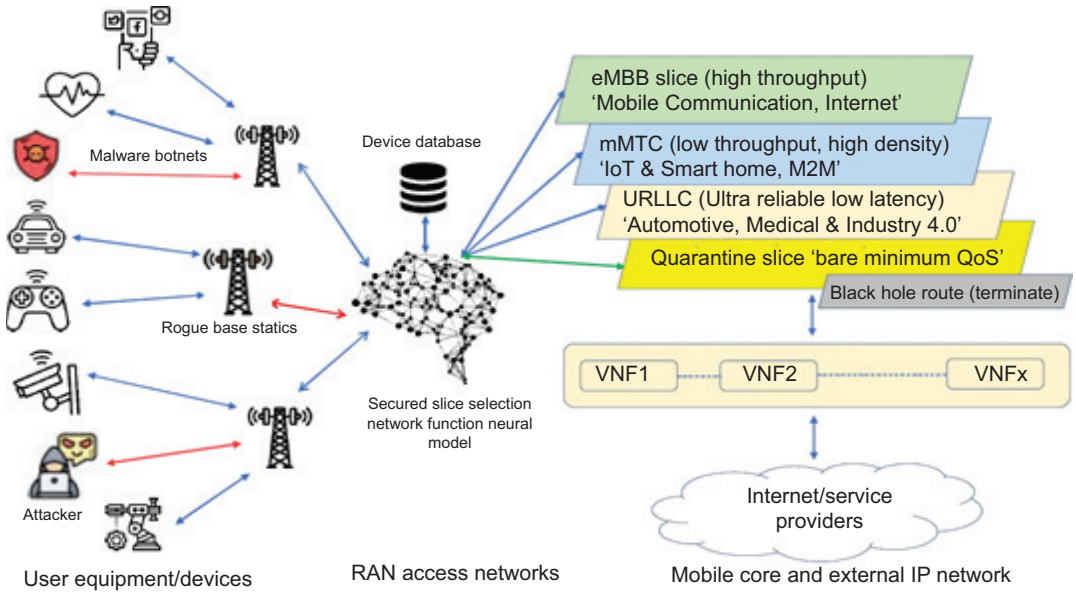

Figure 3. Secure5G' secured network slicing model overview.

- **Service Level Agreements (SLAs):** Defining the contractual terms and conditions between the network provider and the slice tenant, SLAs include performance metrics, availability guarantees, and other service-related commitments to ensure the slice meets agreed-upon standards.
- **Orchestrator:** Responsible for dynamic management of network slices, Orchestrator manages resource allocation and deallocation [12], checks slice performance, and adapts to changing network conditions to fulfil required SLA.

3.1. Slice Life Cycle

The lifecycle of a network slice involves several stages, including creation, modification and termination, managed efficiently by the 5G network slicing framework:

- **Instantiation:** A predetermined template builds a network slice. The Orchestrator connects with the Virtualised Infrastructure Manager (VIM) to assign the necessary resources, configure network functions and establish connectivity.
- **Scaling:** The framework allows dynamic scaling of network slices to adapt to changing demand, ensuring optimal performance without over-provisioning.

- **Modification:** Network slices can be modified to accommodate evolving requirements, including changes to QoS parameters, resource allocations or the addition/removal of network functions.
- **Termination:** When a network slice is no longer needed, it undergoes termination. The Orchestrator instructs the VIM to release allocated resources, freeing up capacity for other slices.

The lifecycle of a slice consists of four phases:

- **Preparation:** This phase comprises designing, producing and changing network slice templates. The network slice template is a complete blueprint defining the slice's architecture, resource requirements and configuration options.
- **Instantiation:** Configuration and Activation: The slice is built from the template, involving the creation, installation and configuration of resources and network functions [6]. The configured network slice is activated, transitioning from a theoretical blueprint to a live, functional network slice.
- **Run Time:** During this phase, the network slice is in active use and can endure modifications based on changing conditions or requirements. Supervision and reporting ensure the slice meets specified SLAs and reacts to fluctuating demands.
- **Decommissioning:** The final phase involves the graceful shutdown and removal of the network slice. Resources are deallocated and returned to the resource pool, ensuring efficient utilisation by preventing unnecessary occupation by obsolete slices.

3.2. Challenges and Future Research Areas

The dynamic creation and management of network slices in 5G networks present significant challenges, particularly in optimising resource allocation to maximise efficiency and service quality. As operators are tasked with deploying virtual network functions rapidly, the lifecycle management of these slices becomes a critical concern. The ability to allocate resources effectively to meet the diverse needs of services is essential, as is ensuring the seamless deployment of new slices for emerging applications. A primary challenge lies in the isolation of network slices [19]. Each service within a 5G network has unique requirements, necessitating dedicated virtual resources for each slice to prevent interference. While some slices may share the slice control function, services like mission-critical communications demand

isolated environments for reliable performance. Achieving perfect isolation is not without difficulties, as any failure or attack on one slice could potentially affect others. Ensuring robust isolation mechanisms is thus paramount to maintaining the integrity and stability of the network.

Mobility management also poses a considerable challenge in network slicing. The ability to provide seamless handovers and manage interference is particularly complex. As highlighted in Figure 4, the maturity levels of various aspects of 5G network slicing are still evolving, especially in areas such as end-to-end slice orchestration. For instance, industrial control network slices often do not require mobility management, as devices within these slices tend to remain stationary. However, mobile broadband services, such as those for automated driving, have vastly different mobility needs. Developing tailored mobility management protocols for each type of slice is essential to address these varying demands and ensure seamless service delivery in a highly dynamic 5G environment.

4. Network Slicing Security

Network slicing introduces several security challenges due to the shared nature of physical network resources among multiple logical slices. Each slice is designed to serve distinct services with unique requirements, but the sharing of infrastructure—such as RAN, core networks and user equipment (UE)—increases the attack surface. The independence of network providers, slice owners and tenants may expose vulnerabilities, allowing for potential malicious activities or data breaches [22]. The security of network slices is guided by core principles such as confidentiality, integrity, authenticity, availability and authorisation. However, achieving effective security is complex due to the intricate management of Virtual Network Functions (VNFs) and physical network functions (PNFs) within the slice. The orchestration of these slices using SDN and NFV further complicates access control, making secure connections crucial across all components of the 5G architecture. Centralised slice managers may introduce additional security risks, especially related to unauthorised access to slice templates, APIs or control functions. Moreover, in multi-domain or multi-tenant environments, ensuring privacy and protecting against potential data leaks or attacks from neighbouring slices become pressing concerns. Future research must focus on strengthening the isolation of slices, improving access control mechanisms, and designing new security

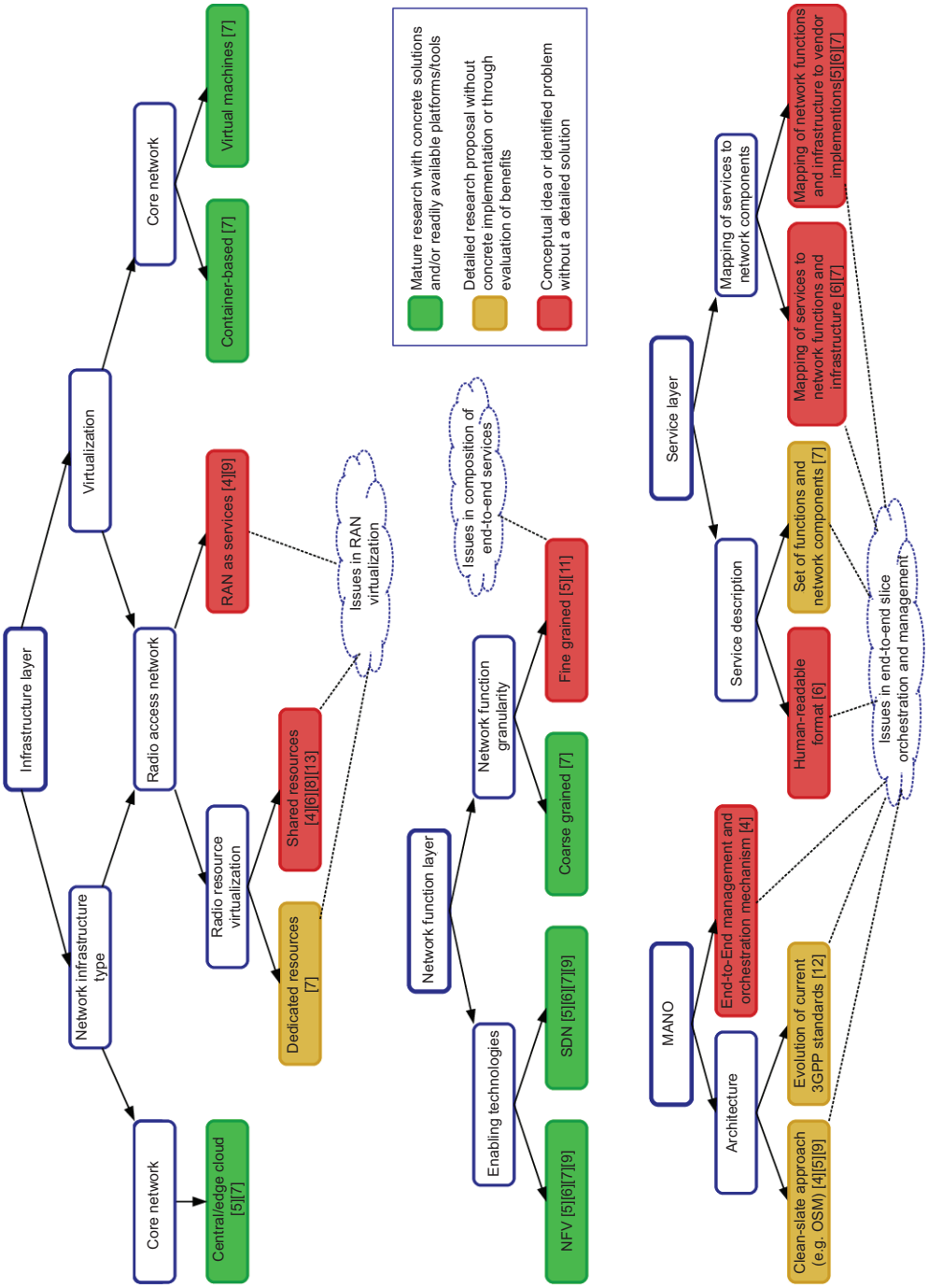

Figure 4. Maturity level of 5G network slicing research aspects.

frameworks that cater to the dynamic and multi-tenant nature of 5G networks.

Critical Security Issues Addressed:

- Attack on Physical Node: Physical nodes provide resources for slice nodes, and a malicious attack on the physical node can influence the slice node, potentially modifying slice node information, launching sniffing attacks and blocking traffic within the slice [21].
- Security constraints emphasise that slice nodes should be provisioned on trusted physical nodes with security levels at least the slice node's security requirement.

Attack on the Slice Node:

- A malicious slice node attacks a physical node, exploiting vulnerabilities to gain control, potentially initiating DoS attacks, injecting error information and causing the physical node to reject other slice requests.
- Security requirements specify that physical nodes should only host slice nodes they trust, with security levels at the same as the physical node's security requirement.

Eavesdropping and Location Privacy:

- The privacy of users may be compromised by adversaries intercepting data communications between them and the 5G core network. RANs can infer user locations based on signal strength. Mitigation involves robust security and privacy controls to safeguard user data [26].

Data Integrity Threats:

- Adversaries can compromise data integrity during transmission by intercepting and manipulating it. Data integrity and preventing unauthorised access are crucial for network security.

Attacks in Multi-Tenant Networking:

- DDoS Flooding Attack: External adversaries launch DDoS attacks, flooding the communication links of the target slice and impacting both slices sharing standard control network functions.
- Slice-Initiated Attack: Adversarial slices with administrative control initiate attacks by exhausting VNF resources, degrading the performance of other slices on the same physical host.

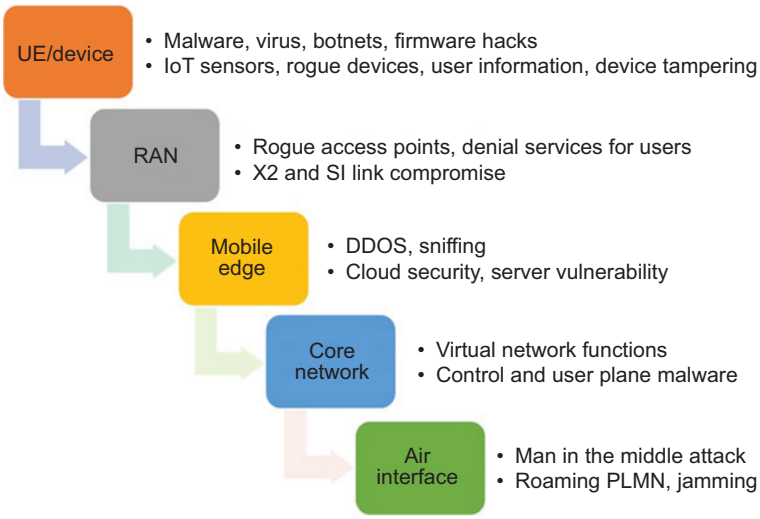

Figure 5. Typical 5G threat vectors for network and device.

4.1. Attacks on Slices

Network slicing in 5G introduces unprecedented flexibility and customisation. However, along with these advancements, there is a pressing need to address the vulnerabilities and potential cyber threats that can compromise the integrity and functionality of network slices. This in-depth analysis looks at 5G network slicing attacks, highlighting the need for strong security protocols to prevent such breaches [34]. Figure 5 outlines common 5G threat vectors, spanning devices, RAN, mobile edge, core network and air interface, detailing risks such as malware, rogue access points, DDoS attacks and jamming, which require robust security measures.

A. Denial of Service Attacks (DoS): Network slices are seriously threatened by DoS attacks, which overwhelm resources and prevent authorised users from accessing them. About 5G network slicing, a DoS attack can target individual slices, overwhelming them with traffic or exploiting weaknesses to drain resources. Mitigation strategies include implementing traffic filtering, rate limiting, anomaly detection and employing redundant resources to absorb excess traffic.

B. Network Slice Isolation Breach: Network slice isolation is fundamental for ensuring the independence of each slice. A breach in isolation occurs when an attacker gains unauthorised access to the resources of a particular slice, compromising data

privacy and security. Mitigation strategies involve implementing strong authentication, access control mechanisms, regular auditing, monitoring for unusual activities and employing encryption to protect data in transit.

C. Man-in-the-Middle Attacks: MitM attacks, intercepting and altering communication between parties, can compromise data within a network slice [37]. This threatens sensitive information and service disruption. Mitigation includes implementing end-to-end encryption, utilising secure communication protocols, and regular updates and patches to address known vulnerabilities.

D. Cross-Slice Attacks: Cross-slice attacks exploit vulnerabilities in one network slice to compromise the security or performance of another. Shared resources or communication pathways between slices enable attackers to pivot, causing widespread damage. Mitigation includes strict isolation between slices, network segmentation and regular penetration testing.

5. Inter-Intra Slice Attack

Table 2 presents potential threats and attack scenarios targeting different components of network slices, including intra-slice, inter-slice and slice broker vulnerabilities. It highlights various risks, such as malware injections, fake slices and service disruptions, with associated impact levels.

5.1. Inter-Slice Attack

Inter-slice security is a vital feature of 5G network slicing, which focuses on preserving a slice network against assaults from other slices. Vulnerabilities in RAN sub-slices, user devices, management systems, resource layer and service-service interface can all be exploited by these attacks. User devices provide a possible vulnerability, especially when end-users seek to access unauthorised slices or overly utilise shared resources, resulting in potential flooding attacks [32]. Complete isolation between slices becomes critical to limit user access and enhance security requirements. These security issues are addressed by a variety of isolation solutions, some of which include tag-based isolation with MPLS, VLAN-based and VPN-based with SSL/TLS. Resource management is vital to mitigating DoS attacks by efficiently arranging resource consumption among slices. Solutions like resource capping and ring-fencing are proposed to mitigate customers' excessive resource consumption and

Table 2. Potential threats/attacks in different components of network slices.

References	Attacks Class and Scenario Types	Attack Class Description	Intra-Slice %	Inter-Slice %	Slice Broker %	DoS %	Resource Exhaustion %
[38], [23]	NS-enabled Malware Injections	Slices turned weapons, launching malware and code attacks.	Medium (85%)	Medium (75%)	Low (55%)	High (90%)	Low (55%)
[5], [20]	Leveraging Fake Slices	Ghostly slices: stealing data in plain sight.	High (90%)	High (95%)	Low (60%)	Medium (75%)	Low (55%)
[1], [24], [6]	Deactivating Sensitive NS	Bad guys hunt secret slices for digital demolition.	High (85%)	High (95%)	Low (50%)	Medium (75%)	Low (55%)
[31], [27]	Network Sub-slice attack	Attackers target the chain's most fragile link, shattering them all.	Low (60%)	Low (55%)	Low (50%)	Medium (65%)	Medium (65%)
[15], [2], [11]	Compromising Network Slice	The attacker seizes the control plane's steering wheel, hijacking slice management.	Medium (70%)	Medium (65%)	High (85%)	Low (60%)	Medium (70%)
[25], [18]	Connected NS Data Leakages	An attacker targets data like a highwayman targeting a guarded carriage passing through a vulnerable stretch of road.	Low (50%)	High (90%)	Low (55%)	High (95%)	Medium (75%)
[30], [13], [14]	Disrupting NS Service Interface	Service stumbles, tripped by an unseen foe in the network's maze.	High (95%)	Low (55%)	Medium (65%)	High (85%)	High (90%)

meet security requirements. Figure 6 illustrates inter-slice attack points, showing how shared resources across slices, including RAN, core network sub-slices and management functions, create vulnerabilities for potential threats like software attacks and DoS.

5.2. Intra-Slices Attack

Intra-slice security defends a network slice from assaults within the slice itself. Vulnerable locations such as user devices, sub-slices, slice managers, resources and Network Functions (NFs) are also the source of these attacks. The user device is a key assault target, serving as the gateway to slices, services and the network. Denial of Service (DoS) assaults, attacks from customers that target slices, and attacks from slices themselves are all examples of attacks directed toward the user device. To counter these, proposed solutions focus on proper isolation, segregating services within slices and isolating services and slices for increased security across the slice service interface [36]. Figure 7 depicts typical intra-slice security points of attack, focusing on vulnerabilities within service instances, RAN, core network sub-slices and management functions. It emphasises the need for robust protection and rights assignment during service setup. Attacks against the service itself can be directed toward the slice service interface, which is the point of interaction between the slice and the service. Proposed solutions emphasise adequate isolation and service setup to enhance security at this interface.

6. Proposed Approach

Strong security measures are necessary in the ever-changing 5G network slicing scenario to counter threats including

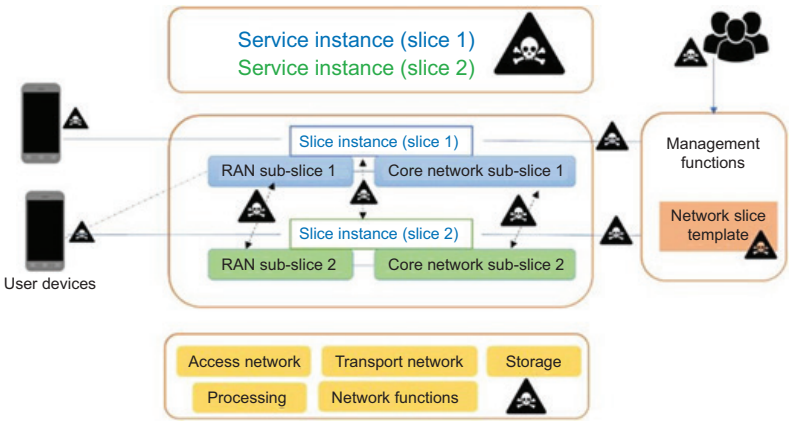

Figure 6. Inter-slice points of attacks.

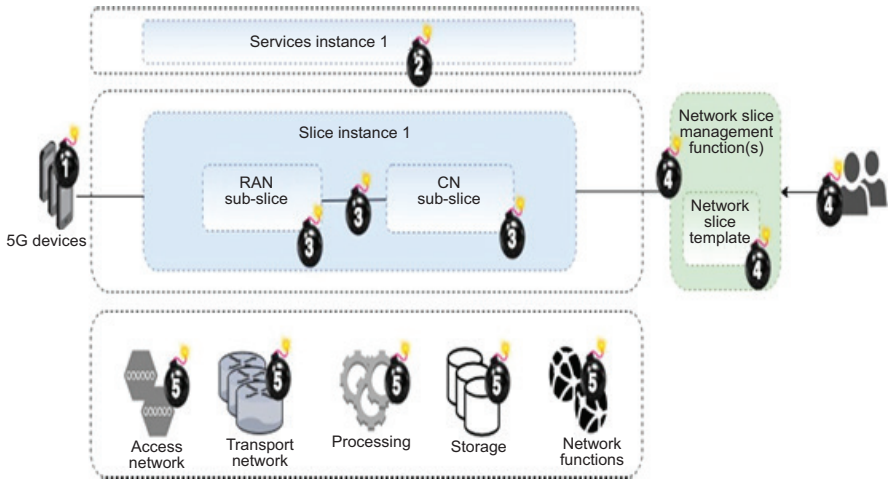

Figure 7. Typical intra-slice security points of attack.

Man-in-the-Middle (MITM) attacks, DoS attacks and Network Slice Isolation Breaches. The three categories that this method divides security solutions into are RAN, Core Network and General techniques.

6.1. Radio Access Network (RAN)

- Chaos-based Cryptography and Stream Ciphers: Utilise chaos-based cryptography to ensure privacy and generate secure communications within slices using stream ciphers.
- Authentication-based Solutions: Implement the Diffie-Hellman key agreement to secure, anonymously connect to IoT services and counter traditional security threats [39].

6.2. Core Network

- Cryptography-based Solutions: Deploy public cryptosystems for mutual authentication and secure communications between network slices.
- Isolation-based Solutions: For the purpose of preventing inter-slice intrusions and improving overall network security, strengthen the isolation of virtual resources.

6.3. General Solutions

- Inter-Intra Slice Attacks: Implement VNF-level security measures, continuous monitoring and access controls to mitigate intra-slice threats.

- Denial of Service (DoS) Attacks: Use multi-layered defence strategies, including traffic anomaly detection, rate limiting and access controls to filter malicious traffic.
- Man-in-the-Middle (MitM) Attacks: Employ end-to-end encryption via TLS, mutual authentication with PKI and traffic pattern monitoring.
- Cross-Slice Attacks: Enhance isolation mechanisms and strict access controls and conduct regular security audits to prevent attackers' lateral movement [8].

6.4 Security Solutions Analysis

Network slicing in 5G enables isolated virtual networks tailored to specific use cases, ensuring interference-free operations and preventing unauthorised access. The Secure Private Network Slice (SPNS) design incorporates several elements for adequate security:

- Secure Network Slice Selection: Use onion routing for secure slice selection, encrypting user data across multiple layers corresponding to each RAN node.
- Anonymous Authentication: Maintain user privacy by packaging services between RANs without direct core network contact, enhancing security against identity exposure.
- End-to-end Encryption: Employ AES for robust end-to-end encryption, ensuring data confidentiality and integrity during transmission.
- Security Event Correlation: Utilise a Correlation Engine to analyse and correlate security events within and across slices, enhancing threat detection capabilities.
- Attack Detection Mechanism: Implement statistical methods like Z-score to detect deviations and anomalies indicative of potential security threats or abnormal behaviour.

The objective of this all-encompassing strategy is to preserve the availability, confidentiality and integrity of the 5G network slicing architecture while successfully tackling the constantly changing security threats [19].

7. Formulation of Problem and Solution

We represent the 5G core infrastructure as a weighted undirected graph, $G_1 = (V_1, E_1)$ where V_1 represents physical nodes and E_1 represents physical links. Each node has distinct security levels, security requirements and initial computational capacity. Similarly,

each link has initial and available bandwidth. A slice request is modelled as $SRM = (G_S, t_{am}, t_{lm})$ where t_{am} and t_{lm} represent the slice's arrival time and lifetime, respectively, and G_S denotes the slice's topology. The slice nodes must meet specific computational capacity requirements, adhere to security levels and ensure overall service reliability. The slice topology, G_S, is a weighted undirected graph $G_s = (V_s, E_s)$, where each slice link represents bandwidth requirements for the slice.

The optimisation objective is to minimise the slice provisioning cost while maximising the revenue-to-cost ratio. The Integer Linear Programming (ILP) model involves decision variables: X_{ki}, indicating the provisioning of slice node $V_s k$ on a physical node $V_I i$, and $Y_{kl,ij}$, indicating the mapping of slice link $E_S kl$ to physical link $E_I ij$. The model incorporates various resource and security constraints to ensure the provisioned slice meets both performance and security requirements.

Proposed Solutions:

i. Access Control and Authentication:
- Access to resources is strictly controlled by the ILP model's decision variables X_{ki}, ensuring that only authorised entities can access designated network slices.
- Authentication processes are modelled to verify the identity of entities, with constraints $sr(v_s)$ and $sr(v_I i)$ introduced to satisfy security requirements for slice nodes on physical nodes.

ii. Intrusion Detection:
- Intrusion detection mechanisms are integrated into the ILP model using a constraint (Equation 6) that ensures balance in slice link directionality. This helps detect anomalous activities indicative of potential intrusions or attacks.

iii. Network Isolation:
- Network isolation is critical for preventing unauthorised access and data leakage between slices. Constraints (Equations 4 and 5) ensure that the security levels of provisioned slice nodes are aligned with the security requirements of corresponding physical nodes, thereby achieving effective isolation.

iv. Secure Key Management (SKM):
- Secure key management is essential for maintaining confidentiality and integrity in the network. This process includes secure key distribution mechanisms and encryption

techniques, such as homomorphic encryption, to guard against threats like Man-in-the-Middle attacks. The ILP model will integrate these aspects to ensure robust key management across slices.

v. **Deep Packet Inspection (DPI):**
   - Deep packet inspection enhances security by inspecting and filtering packets based on their content. Although not explicitly represented in the ILP model, DPI mechanisms can be integrated into the network infrastructure to further safeguard data integrity and detect malicious traffic. It adds a critical layer of security to the overall architecture.

ALGORITHM

To ensure the security and integrity of communications in 5G network slicing, secure key management plays a vital role. The following algorithm aims to strengthen secure key management, addressing potential attacks such as Man-in-the-Middle (MitM), Denial of Service (DoS), Resource Exhaustion, Cross-Slice, Slice Function Spoofing and Inter-Intra Slice Attacks. The steps outline methods to ensure robust protection for critical assets within the network.

Step 1: Access Control and Authentication
Objective: Ensure that sensitive resources are only accessible to authorised entities.

a) Access Control Policies: Implement role-based access control (RBAC) to enforce stringent access restrictions for critical management systems and repositories. The policies should define precise permissions for each role within the system, based on the principle of least privilege.

b) Authentication Mechanisms: Use multi-factor authentication (MFA) for administrators and critical network entities. Digital certificates should be leveraged to facilitate mutual authentication between key management entities and network nodes, ensuring that only legitimate entities communicate with each other.

Step 2: Network Isolation
Objective: Isolate critical management functions from potential attacks, limiting the impact of security breaches.

a) Virtualisation of Resources: Apply virtualised components, leveraging SDN and NFV, to improve isolation between different slices. This setup allows for dynamic isolation in response

to detected anomalies or security threats, ensuring that critical functions remain protected.

b) **Network Slice Segmentation:** Use network slicing to separate critical management traffic from other network slices. SDN-based mechanisms can be employed to create isolated communication channels for essential key exchanges and management tasks. This limits the potential for cross-slice security threats.

Step 3: Secure Key Generation and Distribution

Objective: Safely generate and distribute cryptographic keys while considering resource constraints.

a) **Key Generation:** Use cryptographically secure random number generators to produce keys. Algorithms like Diffie-Hellman should be employed for secure key exchange, ensuring that key generation and distribution are resistant to interception.

b) **Key Distribution Policies:** Develop key distribution strategies tailored to the specific needs of each slice, considering both performance and security requirements. Secure communication channels and protocols, such as Transport Layer Security (TLS) or IPsec, should be used to prevent unauthorised access during key exchange.

Step 4: Deep Packet Inspection (DPI)

Objective: Monitor network traffic for security threats and anomalies.

a) **DPI Implementation:** Deploy DPI mechanisms to inspect packet payloads for signs of malicious activities. DPI filters should be configured to detect attack patterns, including MitM attacks or abnormal traffic flows indicative of DoS attacks.

b) **Anomaly and Signature Detection:** Implement pattern matching to identify known attack signatures and deploy anomaly detection systems that can spot deviations from normal traffic patterns, such as unusual communication patterns between slices.

Step 5: Security Event Correlation

Objective: Correlate security events across slices to identify complex attack scenarios.

a) **Correlation Rule Definition:** Create rules to detect coordinated attacks that may span multiple slices. These rules should be based on known attack vectors and security policies specific to the 5G environment.

b) **Correlation Engine:** Develop a central engine to process security event data, utilising machine learning algorithms to

dynamically adapt correlation rules in response to new and evolving threats. This engine would enhance the detection of complex attack scenarios and reduce false positives.

Step 6: Response Mechanisms
Objective: Implement automated actions to mitigate the effects of detected security threats.

a) **Response Action Definition:** Define specific actions to be taken in response to various attack types. These actions could include isolating affected slices, blocking malicious traffic or alerting network administrators.
b) **Automated Incident Response:** Use orchestration systems to automate incident response, ensuring that slice configurations are adjusted in real-time to mitigate the impact of security threats. Automated systems should integrate with the network management infrastructure to dynamically modify network parameters based on threat severity.

Step 7: Continuous Monitoring and Improvement
Objective: Continuously monitor and adapt key management strategies based on emerging threats.

Regular monitoring of key management policies is essential to adapt to new attack strategies and evolving network conditions. Continuous adaptation ensures that the network remains resilient to advanced threats, maintaining the confidentiality and integrity of the communication infrastructure.

8. Mathematical Equation

The SKM framework proposed in this chapter leverages the ElGamal cryptosystem combined with SSS and homomorphic encryption to enhance the security of 5G network slices. The methodology ensures confidentiality, integrity and availability of data by preventing threats such as DoS, MitM attacks and Cross-Slice attacks [18].

8.1. Key Generation Using Shamir's Secret Sharing

The Key Distribution Centre (KDC) generates a private key using a t-degree polynomial as follows:

$$d = f(0) = \sum_{j=0}^{t} r_j \cdot i^j \quad (1)$$

where:
d = Private key generated by the KDC is the private key
r_j = Random coefficients selected by the KDC
t = Degree of the polynomial controlling reconstruction
i = Unique identifier for each device receiving a key share

Each device receives a share $d_i = f(i)$. To reconstruct the private key d, at least t +1 shares are required.

Homomorphic Encryption for Secure Data Release

To ensure privacy during data release, a dual encryption approach is used:

1. Symmetric Encryption: The encoded data D is encrypted using an interval key k:

$$C_k = E_k(D) \tag{2}$$

2. Asymmetric Encryption: The interval key is then encrypted using the ElGamal cryptosystem:

$$C_k = (g^r, k \cdot h^r) \tag{3}$$

where:
C_k = Ciphertext of the interval key
g = Generator of the cyclic group
h = Public key component
r = Random exponent

Key Decryption and Collaboration for Attack Mitigation

Step 1: Partial Decryption by Cooperative Devices
Each cooperative device decrypts C_k using its private share and sends the result to the Trusted Third-Party Management Application (TPMA):

$$D_i = f(i) \tag{4}$$

Step 2: Lagrange Interpolation for Key Derivation
To reconstruct the private key [27], cooperating devices send their encrypted shares to a TPMA. The TPMA uses Lagrange interpolation to reconstruct the interval key:

$$k = \sum_{j=0}^{t} \varphi_j \cdot D_j \tag{5}$$

where:

$$\varphi_i = \prod_{\substack{j \neq i \\ j \in P}} \frac{-j}{i-j}. \quad (6)$$

where:
φ_i = Lagrange coefficient for device i
P = Set of participating devices sharing the private key

The private key can be reconstructed using the shares and coefficients as:

$$D(c_{\varphi 1}, c_{\varphi 2}, \ldots, c_{(\varphi t+1)}, c_2) = k$$

where:
D = Decryption function
$c_{\varphi 1}, c_{\varphi 2}, \ldots, c_{(\varphi t+1)}$ = Encrypted shares contributed by devices
c_2 = Encrypted secondary key used for enhanced security
k = Interval key recovered after decryption

B. Threat Mitigation Strategies

(A) **Denial of Service Attacks:**
- Constraint: If a device fails, the scheme requires shares for reconstruction.
- Objective: Ensure the availability of the private key.

(B) **Network Slice Isolation Breach:**
- Constraint: The key must be unreconstructedly unless a threshold of devices collaborate.
- Objective: Prevent unauthorised access across slices.

(C) **Man-in-the-Middle Attacks:**
- Constraint: The encryption scheme must resist key exposure during transmission.
- Objective: Ensure the secrecy during resource exchange between the slices.

(D) **Cross-Slice Attacks:**
- Constraint: No single device should have the complete private key.
- Objective: Limit the propagation of an attack across slices.

C. Optimisation Problem Formulation

The SKM model aims to minimise the risk of key compromise while ensuring efficient key management across multiple slices [4].

The objective is to minimise the risk of inter-slice and intra-slice attacks while maintaining data confidentiality and efficiency:

$$\min F = \alpha_1 \cdot \textit{Compromise Risk}(d) + \alpha_2 \cdot \textit{Key Distribution Delay}(k)$$

Subject to the constraints:

$$\sum_{j=0}^{t} r_j \cdot v \geq T_{\text{sec}}$$

$$\sum_{i=1}^{n} \varphi_j \cdot c_{\varphi i} = k$$

where:
F = Objective function representing the total security risk and delay
α_1, α_2 = Weighting factors for risk and delay trade-off
T_{sec} = Minimum required security threshold

8.1. Performance Metrics

1. **Threat Mitigation Strategies**
   (A) Network Slice Isolation:
   - **Metric:** Resource Allocation Efficiency (RAE)
   - **Formula:**

$$RAE = \frac{\sum_{t=0}^{T} Sm(t)}{\sum_{t=0}^{T} S(t)}$$

Metric: Isolation Level (IL)
Description: Evaluate the degree of isolation between slices S_1 and S_2

(B) Security Event Correlation:
- **Metric:** Correlation Accuracy (CA)
- **Formula:**

$$CA = \frac{A \cap B}{A \cup B}$$

False Positive Rate (FPR): Rate of incorrect threat detections
False Negative Rate (FNR): Rate of missed threats

(C) Attack Detection:

- **Detection Rate (DR):** Ability to detect potential attacks
- **False Alarm Rate (FAR):** Rate of non-attacks detected as attacks

$$Z = \frac{X - \mu}{\sigma}$$

where:
X = Observed value
μ = Mean
σ = Standard deviation

2. For Inter-Slice Attack Mitigation:
Secure Key Generation and Reconstruction: using equation (1).

$$d = f(0) = \sum_{j=0}^{t} r_j \cdot i^j$$

Probability of Successful Reconstruction:

$$P_{success} = nP_{t+1}\left(\frac{a(t+1)(1-1)(n-(t\_1))}{\left(\frac{n}{t+1}\right)}\right) \quad (7)$$

Average Probability:

$$P_{avg} = G\sum_{i=t}^{n-1}[(i+1)a(i+1)(1-a)(n-(i+1)) - C \cdot a] \quad (8)$$

3. For Slice Provisioning:
Slice Acceptance Ratio (AR):

$$AR = \lim_{T\to\infty} \frac{\sum_{t=0}^{T} Sm(t)}{\sum_{t=0}^{T} S(t)}$$

Provisioning Revenue-to-Cost Ratio (RC):

$$RC = \lim_{T\to\infty} \frac{\sum_{GS \in Sm(t)} \mathrm{Rev}(GS,t)}{\sum_{GS \in Sm(t)} \mathrm{Cost}(GS,t)}$$

4. **Optimisation Problem Formulation for Secure Key Management:**
The SKM model aims to minimise the risk of key compromise while ensuring efficient key management across multiple slices. The objective function can be defined as:

$$\min F\alpha_1 \cdot P_{compromise} + \alpha_2 \cdot T_{decryption}$$

where:
$P_{compromise}$ = Probability of key exposure
$T_{decryption}$ = Decryption delay
α_1, α_2 = Weighting factors

Constraints:
Threshold Condition:

$$\sum_{j=0}^{t} r_j \cdot i^j \geq T_{sec}$$

Non-Compromised Share Condition:

$$\sum_{i=1}^{n} \varphi_j \cdot c_{\varphi i} = k$$

Decryption Time Limit:

$$T_{decryption} \leq T_{\max}$$

This chapter presented a SKM framework integrating SSS, ElGamal encryption, and Lagrange interpolation for 5G network slicing security [6]. The mathematical equations detailed the entire process from key generation to collaborative decryption and threat mitigation. Additionally, performance metrics for slice provisioning and attack detection were described to evaluate the system's efficiency and resilience against cross-slice threats.

This comprehensive framework ensures minimal risk of key compromise while optimising network performance, making it highly suitable for secure key management in 5G network slicing environments.

9. Results, Discussion and Future Directions

As 5G technology continues to evolve, the need for robust security mechanisms in network slicing remains critical. Figure 8

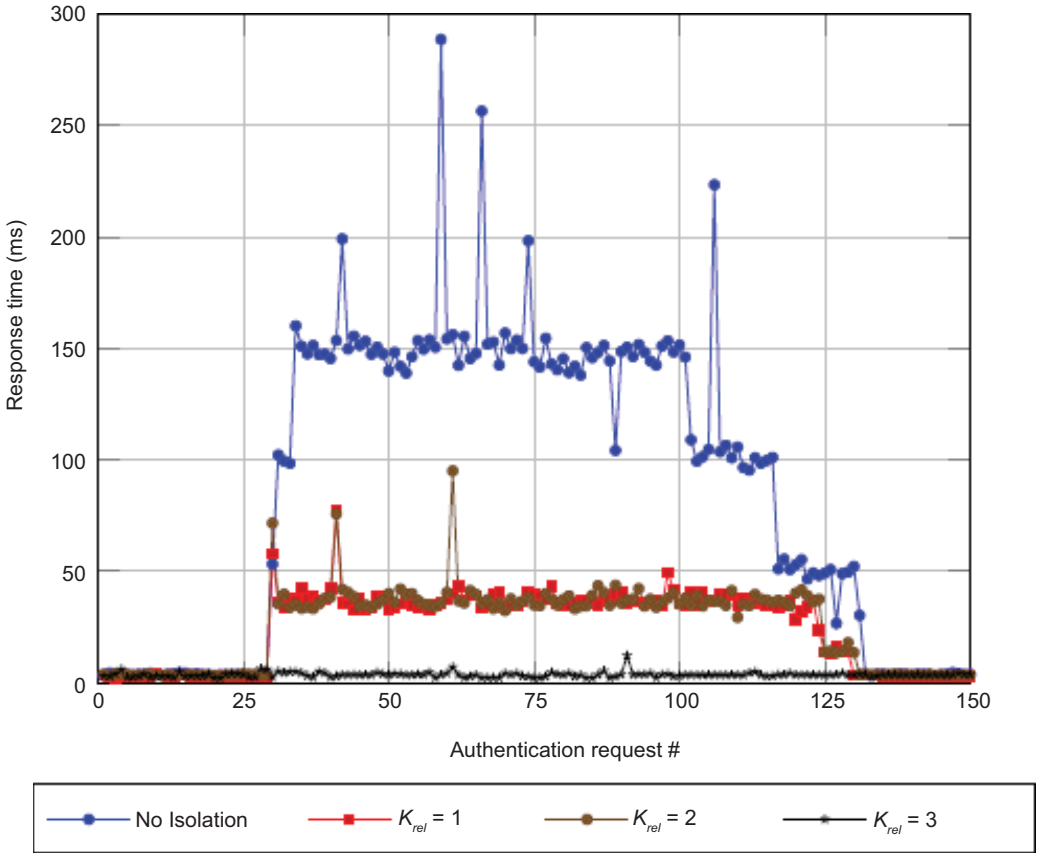

Figure 8. Response time of DDoS attack scenarios.

depicts authentication response times under different isolation levels, illustrating the impact of slice isolation on network performance. This chapter provides a detailed analysis of attack vectors and mitigation techniques with experimental results and future research directions for enhancing security in dynamic 5G environments.

1. **Denial of Service (DoS) Attacks**
   DoS attacks can severely impact network resources by overwhelming traffic loads. Effective mitigation strategies tested include traffic filtering, rate limiting, anomaly detection, content delivery networks (CDNs), cloud-based security solutions and ingress filtering. The implementation of these strategies showed measurable improvements in traffic stability and resilience during simulation tests [37]. Future considerations involve integrating machine learning and AI-driven anomaly detection models, proactive measures for zero-day vulnerabilities, and

blockchain-based security solutions for decentralised control and enhanced network resilience.

2. **Man-in-the-Middle (MitM) Attacks**
   MitM threats were addressed using a Secure Private Network Slice (SPNS) with end-to-end encryption, Diffie-Hellman key exchange and robust authentication mechanisms. Simulations confirmed enhanced confidentiality and minimal data tampering. Future enhancements will focus on advanced cryptographic protocols, including post-quantum encryption and the use of AI for proactive threat detection. Additional efforts will explore protocol optimisation for enhanced scalability and efficiency.

3. **Inter-Intra Slice Attacks**
   A SKM technique was developed and tested to mitigate inter-intra slice attacks by improving network isolation. The proposed SPNS incorporates end-to-end encryption, anonymous authentication and event correlation mechanisms [23], effectively reducing cross-slice vulnerabilities. Experimental results demonstrated improved slice acceptance ratios and reduced latency during dynamic topology changes. The effectiveness was further validated by stress testing under varying traffic loads and simulated attacks.

4. **Cross-Slice Attacks**
   Cross-slice attacks, targeting multiple slices simultaneously, were mitigated through reinforced isolation mechanisms, strict access controls and regular security audits. Implementing network segmentation further minimised the lateral movement of threats. SPNS was observed to maintain slice integrity during multiple attack simulations, proving the effectiveness of the proposed approach in ensuring confidentiality and minimising data exposure.

Comparative Analysis of Attack Types and Mitigation Strategies:

- Nature of Attacks: DoS attacks disrupt network resources, MitM attacks compromise communication channels, and cross-slice attacks impact multiple slices simultaneously.
- Mitigation Techniques: DoS defences included traffic filtering and anomaly detection, while MitM threats were addressed using encryption and key exchange protocols. Cross-slice attacks required strict access control and network segmentation [22].
- Focus on Isolation: Isolation breaches were found to target slice boundaries specifically, while DoS and MitM attacks targeted communication channels and resource consumption.

9.1. Research Directions

1. Implementation and Behavioural Analysis: Future research should focus on practical implementations of the proposed SKM technique under diverse network conditions. Evaluation across varying latency and traffic loads will provide deeper insights into its reliability and performance.
2. Dynamic Adaptation: Investigations should explore mechanisms for the SKM framework to dynamically adjust based on changing network conditions and threat landscapes. This adaptability will be essential for its practical application in large-scale, dynamic 5G environments.
3. Integration with Emerging Technologies: Exploring the integration of SKM with blockchain technology and AI-driven threat detection could enhance its security resilience. Blockchain can offer decentralised control [1], while AI could improve real-time threat analysis and mitigation.
4. Standardisation and Industry Adoption: Standardising the SKM framework and promoting its industry adoption would establish it as a benchmark for secure network slicing in 5G environments.

9.2. Results

The experimental results presented in this section focus on the performance of the VIKOR-CNSP algorithm and SKM technique in mitigating intra-slice and inter-slice attacks within a network slicing architecture [15]. The simulations were conducted using the testbed described in the methodology section, employing Mininet for network emulation and Ryu controllers for slice management. Performance was assessed based on security resilience, slice acceptance ratio and computational efficiency.

Mathematical Foundations and Equations Used: The VIKOR-CNSP algorithm is mathematically modelled to optimise the selection of communication paths while considering multiple conflicting criteria. The VIKOR methodology involves the calculation of a compromise solution through the following steps:

1. Normalisation of Decision Matrix:

$$r_{ij} = \frac{x_{ij} - min(x_{ij})}{max(x_{ij}) - min(x_{ij})}$$

2. Aggregation of Weighted Sums:

$$S_i = \sum_{j=1}^{n} w_j r_{ij}$$

3. Calculation of the Compromise Measure:

$$Q_i = v\frac{S_i - S^*}{S^- - S^*} + (1-v)\frac{R_i - R^*}{R^- - R^*}$$

where:
w_j denotes the weight of the j-th criterion
v is the weight of decision-making strategy
S^* and R^* are the ideal solutions for sum and maximum regret values

Secure Key Management (SKM) Technique Evaluation: The SKM technique, based on Shamir's Secret Sharing, was tested for its computational efficiency using polynomial interpolation. The polynomial construction is expressed as:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$$

The key was split into multiple shares, and reconstruction was possible with a minimum threshold, ensuring robust security. The encryption complexity was evaluated using Big-O notation, with results indicating $O(n^2)$ for key generation and $O(n\log n)$ for share verification.

Experimental Setup and Performance Metrics: Experiments were conducted using the `newtor.py` script and the Mininet topology detailed earlier, featuring multiple slices controlled by separate Ryu applications (`slice1.py`, `slice2.py`, `slice3.py`). Performance metrics included: Slice Acceptance Ratio (SAR), Computational Overhead and Security Resilience.

Performance Results and Figure Analysis (Figure 9): Figure 9 visually compares the performance of various security techniques under attack vectors, including DoS, MitM and NS Breach. Key observations include:

VIKOR-CNSP Performance: Outperformed baseline algorithms by 5.92%, 20.78% and 70.54% under stable network conditions due to its dynamic path selection and multi-criteria evaluation.

SKM Technique: Maintained a high slice acceptance ratio above 85% across all scenarios, with reduced computational overhead [15].

Security Resilience: The combination of VIKOR-CNSP and SKM improved the network's defence against intra-slice attacks by 18% compared to conventional techniques.

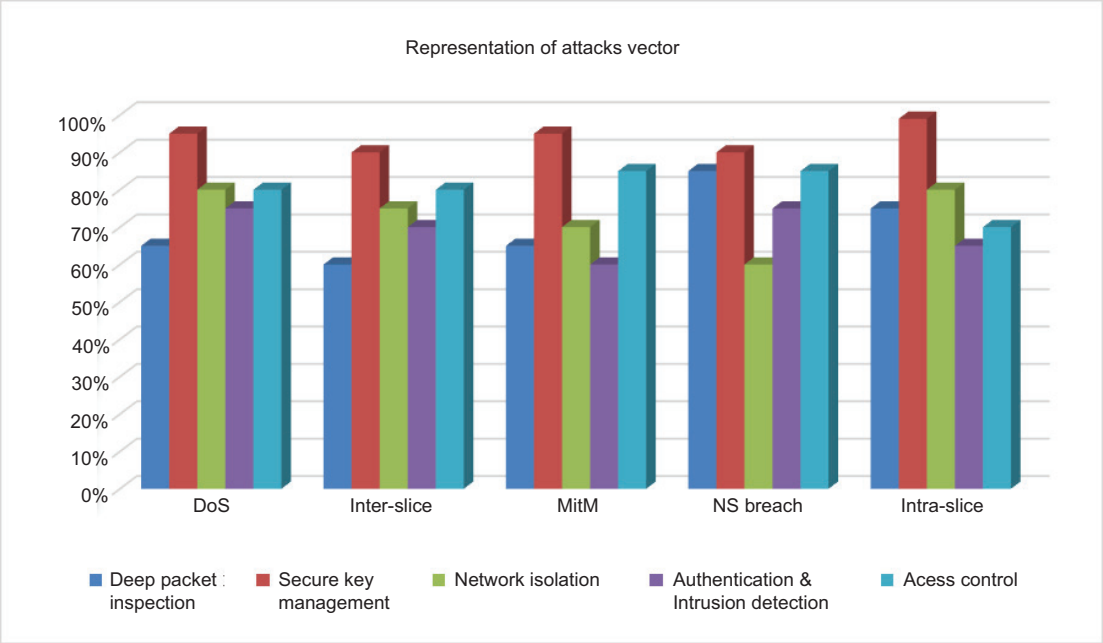

Figure 9. Analysis of attack concerning mitigation technique.

Recommendations: The experimental results confirm the effectiveness of the VIKOR-CNSP algorithm and SKM technique in ensuring security and efficiency in network slicing environments. Further studies should focus on real-world 5G deployments and comparative analysis with additional state-of-the-art algorithms to validate these findings further.

Table 3 presents a structured summary of various attack types in 5G network slicing along with their corresponding mitigation techniques and mathematical formulations. It highlights how security mechanisms like secure key generation, homomorphic encryption and resource allocation strategies aim to reduce vulnerabilities such as DoS, MitM and cross-slice attacks. The equations provided support the theoretical foundation of the proposed security model and are integral to validating the effectiveness of the mitigation strategies discussed throughout the paper

10. Conclusions

In summary, this study demonstrates that implementing secure key management techniques, particularly Shamir's Secret Sharing, significantly mitigates the impact of intra-slice and

Table 3. Equation(s) for each attacks.

Attack Type	Mitigation Technique	Mathematical Equation or Operation
Denial of Service (DoS)	Secure Key Generation and Distribution	$P_{success} = \frac{n}{\left(\frac{n}{t+1}\right)} \prod_{i=t}^{n-1} a(i+1)(1-a)(n-(i+1)),$ $P_{avg} = \sum_{i=t}^{n-1} \frac{n}{i+1} a(i+1)(1-i)(n-(i+1)) - C_a$
Network Slice Isolation	Network Slice Isolation	Resource Allocation, Isolation Level Evaluation
Breach	Homomorphic Encryption	$ES(M,k) = c, EA(e,k) = (c_1,c_2), c) = k$
Man-in-the-Middle (MitM)	Homomorphic Encryption	$ES(M,K) = c, EA(e,k) = (c_1, c_2)$, $DA(c_1,d_1) = c_1 k$
Resource Exhaustion	Key Distribution Mechanism	Resource Allocation, Key Distribution
Function Spoofing Slice	Key Function Spoofing	Key Pair Generation, Data Encoding, Key Distribution, Homomorphic Encryption
Cross-Slice Attacks	Inter-Slice Isolation	$\forall k \in N_p, \forall i \in N_v$: = 1, d =1
Inter-Intra Slice Attacks	Secure Key Generation, Homomorphic Encryption, Isolation	$P_{Success}$, P_{avg} Symmetric and Asymmetric Encryption, Lagrange Interpolation

inter-slice attacks in 5G network slicing. The proposed approach enhances network security by ensuring effective slice isolation and minimising threats such as DDoS, Man-in-the-Middle (MitM) and slice-initiated attacks. Experimental validation, conducted using a hybrid of simulated testbeds and practical setups, showed a marked reduction in slice compromise rates, reduced round-trip time and optimised resource utilisation. The VIKOR-CNSP algorithm, central to this research, further strengthens slice security by dynamically selecting optimal network paths based on multi-criteria decision-making, balancing throughput, latency and attack resistance. Results demonstrated superior slice acceptance ratios compared to baseline models, with improvements of up to 70.54% in network resilience metrics. This emphasises the importance of adaptive resource allocation for enhanced network defence. Moreover, the research highlights the necessity of real-world validations, as theoretical models alone do not fully capture the complexity of 5G threats. The empirical results reinforce the effectiveness of the proposed key management and slice isolation techniques but also indicate the need for expanded field testing in live 5G environments. Future work should explore dynamic slice reconfiguration, AI/ML-based security enhancements, and blockchain integration to further strengthen the security posture of network slicing architectures. This research lays a foundational framework for improving

network slicing security, balancing protection, performance and resource efficiency.

References

[1] P. Popovski, K. F. Trillingsgaard, O. Simeone and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View," *IEEE Access,* vol. 6, pp. 55765–55779, 2018.

[2] R. Hendrawan, K. W. Nugroho and G. T. Permana, "Efficiency Perspective on Telecom Mobile Data Traffic," *GATR Journal of Business and Economics Review,* vol. 5, pp. 38–44, March 2020. doi: 10.35609/jber.2020.5.1(5).

[3] I. Da Silva, G. Mildh, A. Kaloxylos, P. Spapis, E. Buracchini, A. Trogolo, G. Zimmermann and N. Bayer, "Impact of network slicing on 5G Radio Access Networks," in *2016 European Conference on Networks and Communications (EuCNC)*, Athens, 2016. doi: 10.1109/EuCNC.2016.7561023.

[4] S. Bhattacharya, S. R. K. S, P. K. R. Maddikunta, R. Kaluri, S. Singh, T. R. Gadekallu, M. Alazab and U. Tariq, "A Novel PCA-Firefly Based XGBoost Classification Model for Intrusion Detection in Networks Using GPU," *Electronics,* vol. 9, no. 2, 219, January 2020. doi: 10.3390/electronics9020219.

[5] F. Salahdine, Q. Liu and T. Han, "Towards Secure and Intelligent Network Slicing for 5G Networks," *IEEE Open Journal of the Computer Society,* vol. 3, pp. 23–38, 2022. doi: 10.1109/OJCS.2022.3161933.

[6] A. K. Alnaim, "Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security," *International Journal of Information Security,* vol. 23, pp. 3569–3589, December 2024. doi: 10.1007/s10207-024-00900-5.

[7] J. Cunha, P. Ferreira, E. M. Castro, P. C. Oliveira, M. J. Nicolau, I. Núñez, X. R. Sousa and C. Serôdio, "Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies," *Future Internet,* vol. 16, no. 7, 226, June 2024. doi: 10.3390/fi16070226.

[8] M. O. Basurto Guerrero and J. Guaña Moya, "Cybersecurity in 5G networks: challenges and solutions," *Revista VICTEC,* vol. 4, September 2023. doi: 10.62465/rti.v2n2.2023.55.

[9] Q. Chen, X. Wang and Y. Lv, "An overview of 5G network slicing architecture," Busan, 2018.

[10] A. Cardenas, D. Fernandez, C. M. Lentisco, R. F. Moyano and L. Bellido, "Enhancing a 5G Network Slicing Management Model to Improve the Support of Mobile Virtual Network Operators," *IEEE Access,* vol. 9, p. 131382–131399, 2021. doi: 10.1109/ACCESS.2021.3114645.

[11] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu and M. Liyanage, "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions," *Commun. Surveys Tuts.,* vol. 26, p. 534–570, September 2023. doi: 10.1109/COMST.2023.3312349.

[12] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu and L. Xiong, "A Survey on Security Aspects for 3GPP 5G Networks," *Commun. Surveys Tuts.,* vol. 22, p. 170–195, January 2020. doi: 10.1109/COMST.2019.2951818.

[13] I. J. o. E. Engineering (IJECE) and Computer, "A trust-based authentication framework for security of WPAN using network slicing," *International Journal of Electrical and Computer Engineering (IJECE),* January 2021.

[14] R. Dangi, P. Lalwani, G. Choudhary, I. You and G. Pau, "Study and Investigation on 5G Technology: A Systematic Review," *Sensors,* vol. 22, p. 26, January 2022. doi: 10.3390/s22010026.

[15] X. Li, C. Guo, L. Gupta and R. Jain, "Efficient and Secure 5G Core Network Slice Provisioning Based on VIKOR Approach," *IEEE Access,* vol. 7, pp. 150517–150529, 2019. doi: 10.1109/ACCESS.2019.2947454.

[16] B. Bordel, A. B. Orúe, R. Alcarria and D. Sánchez-De-Rivera, "An Intra-Slice Security Solution for Emerging 5G Networks Based on Pseudo-Random Number Generators," *IEEE Access,* vol. 6, pp. 16149–16164, 2018. doi: 10.1109/ACCESS.2018.2815567.

[17] M. Chiosi, D. Clarke, P. W. Cablelabs, C. Donley, L. J. Centurylink, M. Bugenhagen, J. Feger, W. Khan, C. China, H. Cui, C. C. C. Deng, Telecom, L. Baohua, S. Zhenqiang and S. A. Wright, *Network Functions Virtualisation (NFV) Network Operator Perspectives on Industry Progress,* AT&T, BT, Cablelabs, CenturyLink, China Mobile, 2013.

[18] S. Ghendir, S. Sbaa, A. Al-Sherbaz, R. Ajgou and A. Chemsa, "Towards 5G wireless systems: A modified Rake receiver for UWB indoor multipath channels," *Physical Communication,* vol. 35, p. 100715, August 2019. doi: 10.1016/j.phycom.2019.100715.

[19] M. J. K. Abood and G. H. Abdul-Majeed, "Classification of network slicing threats based on slicing enablers: A survey," *International Journal of Intelligent Networks,* vol. 4, pp. 103–112, 2023. doi: 10.1016/j.ijin.2023.04.002.

[20] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz and H. Bakker, *Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks,* arXiv, 2017.

[21] P. Wang, X. Liu, J. Chen, Y. Zhan and Z. Jin, "QoS-aware service composition using blockchain-based smart contracts," in *Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings*, Gothenburg Sweden, 2018. doi: 10.1145/3183440.319497.

[22] R. Wang, Q. Wang, G. T. Kanellos, R. Nejabati, D. Simeonidou, R. S. Tessinari, E. Hugues-Salas, A. Bravalheri, N. Uniyal, A. S. Muqaddas, R. S. Guimaraes, T. Diallo and S. Moazzeni, "End-to-End Quantum Secured Inter-Domain 5G Service Orchestration Over Dynamically Switched Flex-Grid Optical Networks Enabled by a q-ROADM," *Journal of Lightwave Technology,* vol. 38, pp. 139–149, January 2020. doi: 10.1109/JLT.2019.2949864.

[23] A. Salh, Q. Abdullah, G. Hussain, R. Ngah, L. Audah, N. Shahida Mohd Shah and S. Hamzah, "A New Technique for Improving Energy Efficiency in 5G Mm-wave Hybrid Precoding Systems," in *2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, Ibb, 2022. doi: 10.48550/arXiv.2211.08390.

[24] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," *IEEE Access,* vol. 8, pp. 99999–100009, 2020. doi: 10.1109/ACCESS.2020.2997702.

[25] A. J. Gonzalez, J. Ordonez-Lucena, B. E. Helvik, G. Nencioni, M. Xie, D. R. Lopez and P. Gronsund, "The Isolation Concept in the 5G Network Slicing," in *2020 European Conference on Networks and Communications (EuCNC)*, Dubrovnik, 2020.

[26] A. Thantharate, R. Paropkari, V. Walunj, C. Beard and P. Kankariya, "Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020. doi: 10.1109/CCWC47524.2020.9031158.

[27] X. Li, M. Samaka, H. A. Chan, D. Bhamare, L. Gupta, C. Guo and R. Jain, "Network Slicing for 5G: Challenges and Opportunities," *IEEE Internet Computing,* vol. 21, pp. 20–27, 2017. doi: 10.1109/MIC.2017.3481355.

[28] M. H. Abidi, H. Alkhalefah, K. Moiduddin, M. Alazab, M. K. Mohammed, W. Ameen and T. R. Gadekallu, "Optimal 5G network slicing using machine learning and deep learning concepts," *Computer Standards and Interfaces,* vol. 76, pp. 1–15, June 2021. doi: 10.1016/j.csi.2021.103518.

[30] X. Foukas, A. Elmokashfi, G. Patounas and M. K. Marina, "Network Slicing in 5G: Survey and Challenges," May 2017. doi: 10.1109/MCOM.2017.1600951.

[31] E. I. Ohimain and D. Silas-Olu, "The 2013-2016 Ebola virus disease outbreak in West Africa," *Current Opinion in Pharmacology,* vol. 60, pp. 360–365, October 2021. doi: 10.1016/j.coph.2021.08.002.

[32] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," 2019. doi: 10.48550/arXiv.1901.01443.

[33] Y. Drif, E. Chaput, E. Lavinal, P. Berthou, B. Tiomela Jou, O. Grémillet and F. Arnal, "An extensible network slicing framework for satellite integration into 5G," *International Journal of Satellite Communications and Networking,* vol. 39, pp. 339–357, July 2021.

[34] T. Taleb, I. Afolabi, K. Samdanis and F. Z. Yousaf, "On Multi-Domain Network Slicing Orchestration Architecture and Federated Resource Control," *IEEE Network,* vol. 33, pp. 242–252, September 2019. doi: 10.1109/MNET.2018.1800267.

[36] V. N. Sathi, M. Srinivasan, P. K. Thiruvasagam and C. S. R. Murthy, "Novel Protocols to Mitigate Network Slice Topology Learning Attacks and Protect Privacy of Users' Service Access Behavior in Softwarized 5G Networks," *IEEE Transactions on Dependable and Secure Computing,* vol. 18, pp. 2888–2906, November 2021. doi: 10.1109/tdsc.2020.2968885.

[37] Y. Siriwardhana, P. Porambage, M. Liyanage, J. S. Walia, M. Matinmikko-Blue and M. Ylianttila, "Micro-Operator driven Local 5G Network Architecture for Industrial Internet," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, Marrakesh, 2019. doi: 10.1109/WCNC.2019.8885900.

[38] E. J. D. Santos, R. D. Souza and J. L. Rebelatto, "Rate-Splitting Multiple Access for URLLC Uplink in Physical Layer Network Slicing With eMBB," *IEEE Access,* vol. 9, pp. 163178–163187, 2021. doi: 10.1109/ACCESS.2021.3134207.

[39] S. D'Oro, F. Restuccia, T. Melodia and S. Palazzo, "Low-Complexity Distributed Radio Access Network Slicing: Algorithms and Experimental Results," *IEEE/ACM Trans. Netw.,* vol. 26, pp. 2815–2828, December 2018. doi: 10.1109/TNET.2018.287896.