2025 IEEE 24th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) | 979-8-3315-6532-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/Trustcom66490.2025.00331

5GC-PDA:A Novel Proactive Defense Architecture for Enhancing 5G Core Network Security

Xingxing Liao[1], Wei You[1,2], Jie Yang[*2],Jian Tao[1], Runhan Feng[1], Xinsheng Ji[1,2]
[1]*Purple Mountain Laboratories, Nanjing, China*
[2]*Information Engineering University, Zhengzhou, China*
liaoxingxing@pmlabs.com, youwei1102@163.com, yj_csu@126.com

***Abstract*—The arrival of 5G era brings great convenience and unprecedented opportunities to human society under the new technical features of ultra-high speed, ultra-low latency, and mega-connectivity. As the management hub and "brain" of the 5G network architecture, the security of the core network is paramount. However, its evolution towards cloudification has led to frequent cybersecurity incidents; an attack on the 5G core network could trigger severe consequences. To address this, this paper first systematically analyzes potential vulnerabilities and attack paths within the 5G core network from an attacker's perspective. Subsequently, an endogenous proactive defense architecture, grounded in the principles of dynamism, heterogeneity, and redundancy, is proposed. The working mechanism of this architecture is elaborated in detail, alongside a theoretical analysis of its security properties. To validate the efficacy of the proposed architecture, defensive performance was first compared across different schemes via simulation. The results demonstrate that our architecture achieves optimal defensive performance while significantly increasing the attacker's cost. Furthermore, the proposed architecture was implemented on the Unified Data Management (UDM) network function within the open-source free5gc platform, and its enhanced protective capability was assessed through real-world attack testing. Experimental results indicate that the architecture effectively elevates the overall security posture of the 5G core network, introducing only marginal performance overhead.**

***Index Terms*—5G; core network; endogenous security; proactive defense; UDM**

I. Introduction

Cloud-native deployment and service-oriented communication architectures have endowed the 5G core network control plane with unprecedented flexibility and innovation, yet they simultaneously expose it to an expanding spectrum of threats [1]. Malformed packets injected into signaling streams can precipitate reconnaissance [2] or misconfiguration attacks [3]. Exploitation of API vulnerabilities may enable flooding assaults that cripple critical network functions, sever inter-NF connectivity, or disrupt the attachment of user equipment to the 5G network [4].

Furthermore, adversaries who compromise underlying software or hardware can orchestrate advanced persistent threats or zero-day exploits, leading to exfiltration of network data, manipulation of messages originated by virtualized network functions, or outright collapse of VNF services [5].

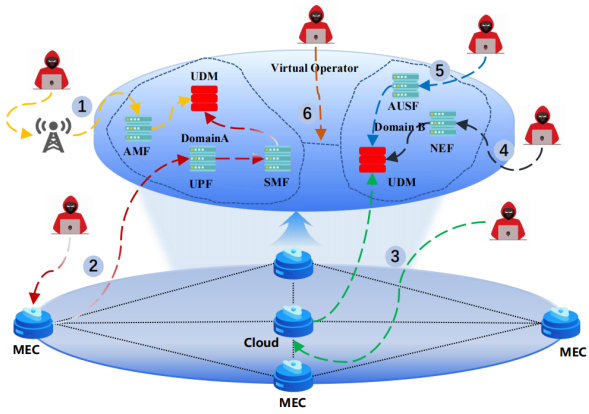


Fig. 1. Security threat landscape in cloudified 5G core network.This figure presents a multidimensional threat analysis for cloud-based 5G core networks, identifying six critical attack vectors:① Base station attacks exploiting radio access vulnerabilities;② Edge/MEC attacks targeting distributed compute resources;③ Cloud infrastructure attacks compromising centralized resources;④ Open interface attacks leveraging;⑤ Internal lateral attacks enabling post-breach propagation;⑥ Cross-domain attackss.

To counter these security threats, various defense measures have been proposed and can be broadly categorized into four classes: first, introducing the "Zero Trust" paradigm to enforce stringent network access control [6]; second, leveraging artificial intelligence (AI) techniques for threat detection and mitigation [7]; third, adopting Moving Target Defense (MTD) strategies to increase the complexity faced by potential attackers [8]; and fourth, integrating conventional defense mechanisms, such as firewalls, IP Security (IPSec) [9], honeypot technologies [10], and disaster recovery and backup procedures, to ensure the reliability of critical network components [11].

Some defensive methods are static, reacting only after threats emerge, thereby exposing their structural limitations. These static defenses—such as firewalls, intrusion detection systems, and code safety scanners—operate deterministically. This means they rely on pre-defined threat signatures, pat-

This work was supported by the National Science and Technology Major Project of China (No. 2025ZD1303100) and the National Key Research and Development Plan of China (No. 2020YFB1806607, No. 2022YFB2902205).
Corresponding author: Wei You.

2324-9013/25/$31.00 ©2025 IEEE
DOI 10.1109/Trustcom66490.2025.00331

terns, and security policies to protect the entire system. While historically effective at a low cost in simpler information systems, they now struggle to adapt to the rapidly evolving threat landscape. Crucially, static defenses lack the capability to counter unknown vulnerabilities, backdoors, or advanced malware.

Conversely, certain proactive defense approaches exist. Taking Moving Target Defense (MTD) as an example, this technique periodically conducts security assessments and proactively changes system configurations. While MTD can sustain defense effectiveness over extended periods, it may still struggle to withstand persistent attacks within a single assessment window. Fundamentally, MTD introduces randomness to obscure the attack surface, thereby increasing the difficulty for attackers to conduct reconnaissance; however, it does not directly defend against individual attack instances. Compared with MTD, honeypot technology—another proactive defense mechanism—is only activated under specific conditions, which significantly limits its effectiveness.

In recent years, following the cloudification of 5G, security incidents have emerged incessantly, prompting an increasing number of researchers to shift towards more promising proactive defense paradigms. This chapter proposes a proactive defense architecture for the 5G core network control plane based on the concept of endogenous security, namely 5GC-PDA.

The key contributions of this paper are threefold:

1) Proposing the 5GC-PDA architecture: To counter security threats in 5G Core Networks (5GC), we introduce the 5GC-PDA architecture. This work pioneers the systematic integration of the Dynamic Heterogeneous Redundancy (DHR) mechanism into the 5G Service-Based Architecture (SBA). Significantly, 5GC-PDA imbues the control plane with endogenous, proactive security capabilities without disrupting existing 3GPP service procedures.
2) Theoretical security analysis and comparative evaluation: We establish the theoretical security foundation of the 5GC-PDA architecture through rigorous formal analysis. Furthermore, via comprehensive simulation, we quantitatively compare its defensive efficacy against alternative approaches. Results conclusively demonstrate that 5GC-PDA imposes the highest attack cost on adversaries while delivering superior protection under equivalent conditions.
3) Prototype implementation and empirical validation: We validate the practicality of 5GC-PDA by developing a functional prototype within the open-source free5GC platform, using the Unified Data Management (UDM) network element as a representative case. Empirical evaluation through simulated attack injections demonstrates that the architecture significantly enhances core network security protection, achieving this robust defense with only a marginal increase in performance overhead.

II. RELATED WORKS

The principal standardization bodies—such as 3GPP, ETSI, ITU-T and ENISA—have devised dedicated security architectures and solutions to address the multifaceted security risks confronting the 5G network [12]. These efforts have yielded a comprehensive suite of countermeasures encompassing signaling-message encryption, authentication and authorization, access control, vulnerability management, and continuous security monitoring.

3GPP partitions the 5G system into six security domains and analyzes twenty key security issues within the Service-Based Architecture (SBA) of the 5G Core (5GC) [13]. ENISA recently updated the "ENISA Threat Landscape for 5G Networks Report" [14], summarizing seventeen categories of core-network vulnerabilities along with corresponding countermeasures. China's Academy of Information and Communications Technology (CAICT) has released the "5G Security Report" [15] and the "5G Security Knowledge Base" [16], covering eight security modules—including radio access, core network, and edge computing—and 188 security measures. These documents specifically examine core-network security from eight perspectives: resource-availability protection, Network Exposure Function (NEF) security, traffic protection, internal/external boundary isolation, secure identity of Network Functions (NFs), virtual-machine resource protection, user-identifier protection, and roaming security.

The academic community has systematically characterized the novel risks introduced by 5G. Nathalie Wehbe [17] observes that, once the 5G core fully adopts the HTTP/2-based Service-Based Architecture (SBA), the inherent weaknesses of the conventional Web stack—JSON, RESTful APIs, OAuth 2.0, and TLS—are inherited en masse, exposing the signaling plane to native HTTP/2 threats such as replay and injection attacks. Huang et al. [18] proposed a novel attack method targeting privacy information theft in the 5G core network. The attacker exploits side-channel techniques to compromise the underlying infrastructure shared by multiple 5G network slices, deliberately inducing cache hits or misses in the target slice's response, thereby extracting the target's private data. Pattaranantakul et al. [19] pointed out that in 5G networks, Network Function Virtualization (NFV) technology is utilized to deploy Virtualized Network Functions (VNFs) on third-party platforms outside the primary data centers; however, these additional hypervisors may introduce security vulnerabilities that can be exploited by attackers. George et al. [20] conducted a series of attack studies and tests on the Packet Forwarding Control Protocol (PFCP) in the 5G core network. Their results demonstrate that by sending unauthorized session control messages, attackers can disrupt established 5G communication channels without interrupting the user's connection to the NG-RAN, thereby hindering the detection systems' ability to identify the malicious activities.

To counter the aforementioned threats, researchers have proposed holistic defense strategies along two orthogonal dimensions: architecture and protocol. Architecturally, Yan et

al. [21] present 5GC-SDP, which embeds Software-Defined Perimeter (SDP) techniques into the Stand-Alone (SA) 5G core and leverages Single Packet Authorization (SPA) to accurately detect and block DoS floods. Wissem Soussi et al. [22] advocate pushing Moving Target Defense (MTD) into post-5G networks, employing dynamic topologies and address hopping to continuously raise the adversary's cost. At the protocol layer, Ref. [23] employs IPsec tunnels to preserve the integrity and confidentiality of inter-network-element traffic, whereas Ref. [24] propose a novel application-layer anomaly detection framework named 5GShield. This framework innovatively employs neural networks, specifically an Autoencoder, for anomaly detection.Ref. [25] proposes an Intrusion Detection System (IDS) specifically designed for the 5G Core (5GC), named 5GCIDS. This system employs Artificial Intelligence (AI) methods to detect potential cyberattacks targeting the Packet Forwarding Control Protocol (PFCP).

Looking toward B5G/6G, the Inspire-5Gplus framework proposed in Ref. [26] converges machine learning (ML), artificial intelligence (AI), distributed ledger technology (DLT), and trusted execution environments (TEE) to deliver closed-loop, end-to-end security governance. Ref. [27]emphasizes the role of Security Orchestration (SCO) as a bridge connecting various enabling technologies of 5G/B5G with the goals of automated and intelligent security. Ref. [28] narrows its focus to containerized network functions (CNFs) and identifies cgroup bypasses and container-network attacks as critical threats to 5G's high-reliability objectives, calling for future work on hardening container resource-control mechanisms.

Passive and proactive security protection methods have evolved independently, each possessing distinct advantages and limitations. In the future, 5G system security should be endogenous and proactive. Systems, when facing functional safety and cybersecurity challenges, should be capable of passively defending against known attacks and proactively resisting unknown threats, thereby ensuring controllable security risks and stable operation. However, specific and feasible endogenous proactive defense solutions for the 5G core network are currently lacking. This paper proposes the 5G-PDA architecture and presents corresponding work in model construction, theoretical validation, and experimental verification.

III. THREAT ANALYSIS

With the shift of the 5G core network (5GC) to a cloud - native service - based architecture (SBA), its security threats have become multi-dimensional and infiltrating. Fig 1 illustrates the different modules in the 5G network and the attack paths between them. The interaction and communication of each module may become a potential attack entry point. Attackers can launch attacks through various means such as base stations, open API, cloud vulnerabilities, and MEC.

As critical physical nodes in network access, base stations constitute the primary attack vector. As shown in Path ①, Attackers can exploit malware implantation or zero-day vulnerabilities to infiltrate base station equipment, thereby hijacking control privileges over the Access and Mobility Management Function (AMF).Then, attackers can launch distributed denial - of - service (DDoS) attacks based on signaling storms or conduct lateral privilege escalation via system vulnerabilities to illegally obtain critical user data.

In the NFV architecture, the internet accessibility of VNFs is a key security issue. If some VNF instances are misconfigured with public internet interfaces, ports can be exposed to automated attacker scans. Using vulnerability databases, attackers can then conduct targeted attacks. They can also exploit configuration flaws in orchestration systems to move laterally across VNFs, expanding the attack scope, as shown in Path ⑤. In addition, the inherent unreliability of cloud infrastructure, both in software and hardware, can cause network function failures. This further intensifies security risks, as shown in Path ③.

In the 5G network architecture, to meet the requirements of low-latency services, network functions are deployed at the edge. This shift exposes the edge network to novel security challenges, making it a prime new target for attackers. Attackers can target the N4 interface of the edge User Plane Function (UPF) to launch attacks, thereby causing failures in the Session Management Function (SMF). For instance, attackers may exhaust SMF resources by flooding it with massive association requests, or craft malicious N4 signaling messages to crash the SMF, as shown in path ②. The openness of the Service-Based Interface (SBI) in the 5G core network introduces significant security challenges, encompassing malicious Network Function (NF) registration, signaling path manipulation and service redirection, parameter injection attacks, and protocol implementation vulnerabilities. Furthermore, the business practice of "Network Slicing as a Service" facilitates infrastructure sharing between virtual operators and traditional operators, resulting in increasingly ambiguous security responsibility delineation within heterogeneous network environments. Notably, attackers have begun exploiting semantic vulnerabilities inherent in open interface specifications and leveraging the isolation mechanisms of network slices to launch targeted penetration attacks and lateral cross-domain attacks,as shown in Path ④ and ⑥.

The 5G core network control plane faces systemic security threats. Attackers deploy multi-layered attack chains spanning firmware backdoors in physical base stations, exposed VNF components, and cross-domain slicing attacks. Traditional point-based defenses prove inadequate against such breaches, which risk widespread service disruption. Consequently, an endogenous secure architecture enabling fundamental resilience and proactive threat defense is urgently required to ensure stable 5G core operations.

IV. SYSTEM OVERVIEW

A. System architecture

We propose 5GC-PDA, a security-enhanced architecture for the 5G control plane based on Dynamic Heterogeneous Redundancy (DHR). As shown in Fig 2,5GC-PDA augments the existing core network with the following functional modules:

- Equivalent function heterogeneous executor (EFHE):A set of operational executors with identical functionality but heterogeneous runtime environments, network configurations, and software implementations. Taking the UDM network element in 5G core networks as an example, its software implementations (e.g., Go or C) and runtime environments (e.g., containers or VMs) differ substantially. This multi-dimensional heterogeneity impedes attackers from constructing universal attack vectors. When targeting executors with identical functionality, attack chains frequently fracture due to environmental discrepancies, resulting in a proactive defense effect.
- Equivalent function heterogeneous executor pool (EFHEP):A repository that stores heterogeneous executors providing functionally equivalent services.These Executors are divided into two sets based on their operational status: the working set and the non-working set. The working set includes executors currently in use by the network.
- Message dispatch agent (MDA): Based on scheduling instructions from the negative feedback controller, decides how to connect external inputs to specific executors within the current service set. This enables activating executors, suspending executors for repair, or executing other designated tasks, while also realizing dynamic replication and distribution of input messages by copying and dispatching received messages to EFHE for processing.
- Mimic decision point (MDP): Takes the outputs of EFHE as input and, based on the security level, applies decision strategies—such as majority voting or consistency checks—to adjudicate among multiple response results for the same request message, thereby identifying executors whose signaling messages have been tampered with.
- Negative feedback controller(NFC): Collects various anomaly and status information during system operation from the MDP and EFHE, conducts comprehensive judgment, and proactively adjusts operational parameters such as EFHE combination methods and scheduling strategies. The NFC supports offline cleaning and data recovery of untrusted executors to ensure normal operation of the system.

B. System workflow

The primary technical challenge in integrating the 5GC-PDA defense mechanism into the service-based architecture of 5G core networks lies in achieving seamless convergence between security capabilities and standardized specifications. Under the 3GPP Release 15 and subsequent evolutionary frameworks, network element design must rigorously comply with Service-Based Interface (SBI) protocols. This establishes two fundamental objectives for 5GC-PDA deployment:

First, existing VNF/CNF network elements must preserve functional integrity and interface consistency, precluding modifications to critical components (e.g., AMF, SMF, UDM). Second, security enhancements must not disrupt 3GPP-defined

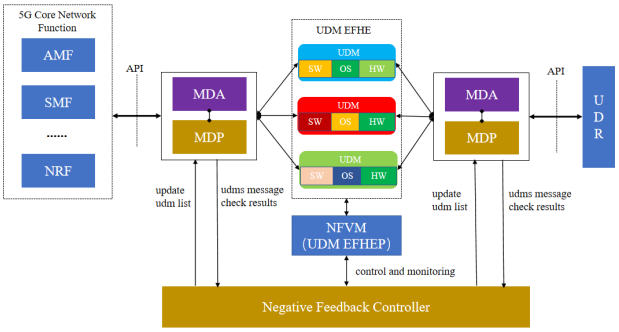


Fig. 2. The overview of our method,Our approach leverages the principles of dynamism, heterogeneity, and redundancy to enhance the security of network elements.Within the proposed architecture, the NFC orchestrates heterogeneous executor pools to facilitate dynamic heterogeneity. Complementary to this, MDA manages signaling message dissemination, while the MDP performs signaling message arbitration.

core service procedures—including registration, session management, and mobility management.

Consequently, a ”network-element-transparent” deployment model is required—one that simultaneously addresses 5G core networks' dual constraints of high reliability and stringent compliance. This model delivers an evolutionary cybersecurity enhancement solution for operators, supporting phased upgrades and incremental evolution while enabling co-advancement of cyber defenses and mobile communication standards.To realize these objectives, we establish the following technical pathway:

NF registration process: As illustrated in Fig 3, while traditional 5G core networks require each Network Function (NF) to register directly with the Network Repository Function (NRF) upon initialization, our enhanced architecture fundamentally transforms this process. Following implementation, the MDP acts as a registration proxy for redundant NF instances: It continuously receives registration requests, selectively forwards only the first-arriving request to the NRF after replacing its source address with the MDP's address, and concurrently maintains state information for registration management. Upon receiving NRF's successful registration response, the MDP distributes this confirmation to all requesting NFs, thereby completing the registration cycle. Furthermore, during subsequent network reconfigurations where active NFs decommission and new NFs activate, service onboarding simplifies to direct registration with the MDP—eliminating redundant interactions with the NRF.

NF service request process: When NF-A needs to invoke services from NF-B, it first queries the NRF for NF-B's address. However, within the mimic-constructed NF-B environment, NF-A actually retrieves the address of the MDP. NF-A then initiates a service request to the MDP. At this point, the MDP distributes NF-A's request to the multiple redundant NF-B instances. The NF-B instances send their corresponding responses back to the MDP. Upon receiving multiple responses,

the MDP compares them and forwards a normal response to NF-A. Should the MDP determine that a specific NF-B instance is anomalous, it reports this anomaly to the NFC (Network Function Controller). The NFC then rotates out the anomalous NF-B instance.

Design of the MDP graceful exit mechanism: When the MDP fails, the heartbeat connections between the MDP, the NRF, and the NF-bs will be interrupted. As a result, both the NRF and the NF-bs will perform deregistration operations, removing any information related to the MDP.At the same time, when the Negative Feedback Controller (NFC) can no longer detect the presence of the MDP, it will shut down all but one of the NF-b executor instances, allowing only a single instance to continue operating.NF-a then re-registers with the NRF using a backup address. After the first service request fails, NF-a will re-initiate service discovery with the NRF to obtain the updated address of the peer NF-b. Once the new address is discovered, normal service operations can resume.Through this process, service continuity can be maintained even in the event of a security component failure or graceful exit.

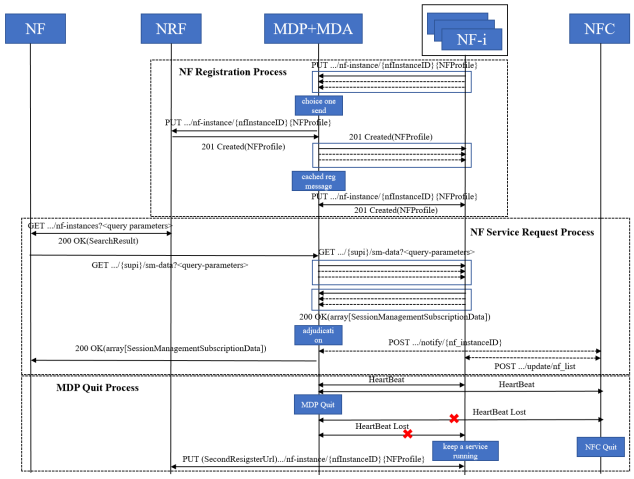


Fig. 3. The interaction between the NF within the PDA architecture and the core network primarily consists of three key procedures: the NF registration process, the NF service request process, and the MDP graceful exit mechanism. These procedures collectively ensure the secure management of NFs without requiring modification to the 3GPP protocols.

C. Defense mechanisms and security analysis

The 5GC-PDA architecture achieves heterogeneity of Network Functions (NFs) through diversified compilation techniques and multi-supply-chain components, enabling multiple NF instances with identical functionality to operate concurrently and provide services. Taking the UDM (Unified Data Management) as an example, when the UDM is under attack or its signaling messages are maliciously tampered with due to software vulnerabilities, the Mimic Decision Point (MDP) plays a critical role. By comparing the output results of multiple heterogeneous executors, the MDP can effectively detect anomalous behavior in the UDM. Upon identifying an issue, the MDP notifies the Negative Feedback Controller (NFC) to perform cleanup or rotation operations on the affected UDM executor. The compromised UDM component is then replaced by a healthy backup UDM, maintaining business continuity throughout the process.

The 5GC-PDA features a unique ”indeterminacy operation mechanism”. This mechanism can suppress or manage the impact of widespread indeterminate disturbances within the NF set, effectively mitigating threats whether they stem from reliability risks caused by natural factors or security attacks initiated by deliberate human actions.

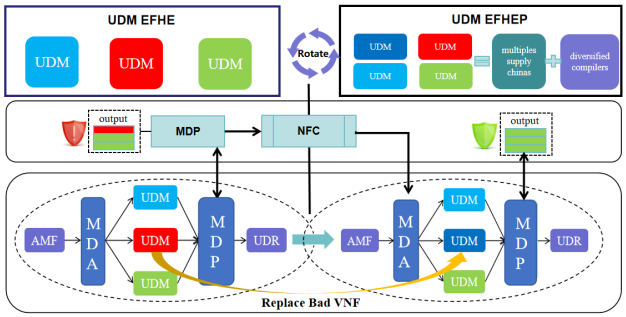


Fig. 4. The defense principle of the 5GC-MDA architecture is demonstrated through specific examples of the generation of heterogeneous UDMs, MDP arbitration, and NFC (Network Function Coordination) scheduling.

In the security analysis, we make the following assumptions:

- Independence of NF executors: Each NF executor is independent and implemented in a different manner (heterogeneity).
- Attack Model: The attacker can only launch destructive attacks against specific NF executors, and each attack can compromise at most one NF executor at a time.
- Recovery mechanism: The NFC replaces NF executors at a fixed interval T, and each replacement is selected from a pool containing n secure executors.
- Adjudication mechanism: The MDP is capable of detecting abnormal responses and selecting the correct ones.

Let m denote the number of NF executors currently in operation, and n denote the total number of NF executors in the pool, with $n > m$. Let λ represent the attack rate on a single NF executor (number of attacks per unit time), and μ denote the NF replacement rate by the NFC(number of replacements per unit time).

Let $P_k(t)$ denote the probability that k NF executors are compromised at time t. The dynamic behavior of the system can be described by the following differential equations:

$$\frac{dP_k(t)}{dt} = \lambda P_{k-1}(t) - (\lambda + \mu)P_k(t) + \mu P_{k+1}(t) \quad (1)$$

Among them, $k = 0, 1, 2, \ldots, m$, In the steady-state condition, $\frac{dP_k(t)}{dt} = 0$, we have P_k^*

$$\lambda P_{k-1}^* = (\lambda + \mu) P_k^* + \mu P_{k+1}^* \tag{2}$$

derivation:

$$P_k^* = \frac{\binom{m}{k} \lambda^k \mu^{m-k}}{\sum_{k=0}^{m} \binom{m}{k} \lambda^k \mu^{m-k}} \tag{3}$$

Probability of system failure is:

$$\pi_f = \frac{\lambda^m}{\sum_{k=0}^{m} \binom{m}{k} \lambda^k \mu^{m-k}} \tag{4}$$

Assuming $r = \frac{\lambda}{\mu}$, We can derive:

$$\pi_f = \frac{(r\mu)^m}{\sum_{k=0}^{m} \binom{m}{k} (r\mu)^k \mu^{m-k}} \tag{5}$$

Finally:

$$\pi_f = \left(\frac{r}{1+r} \right)^m \tag{6}$$

When m is sufficiently large, for any given ε, we have:

$$\lim_{m \to \infty} \pi_s = 1 - \varepsilon \tag{7}$$

In conclusion, the security analysis under coordinated attack scenarios demonstrates that 5GC-PDA possesses endogenous security with probabilistically controllable characteristics.

V. EXPERIMENTS

A. Simulation experiments

In an NFV environment, NF instances are deployed as Virtualized Network Functions (VNFs) within a cloud infrastructure. To evaluate the security posture of various countermeasures against the threats identified during threat modeling, we define the following parameters:

TABLE I
PARAMETER DEFINITIONS AND CONFIGURATION

Parameter	Value	Parameter Explanation
τ_{attack}	100	Maximun time to breach a system
τ_{defence}	20	Time required for system defense
τ_{switch}	5	Time for system dynamic switch
τ_{min}	2	Minimum breach time
m	3	Number of running VNFs
n	5	Total number of VNF pools
k	0.01	Attacker's attack time decay factor
τ_{location}	10	Time required for attacker to locate
r	0.05	VNF reconfiguration rate

Experimental parameters are configured as specified in Table 1. Suppose an attacker can breach a system within time τ_{attack}, with the time required for each attack decreasing according to a specific pattern, as illustrated in Fig 5(a). We evaluate the attack resistance of four systems (A, B, C, and D) by defining the security capability metric as: I = remaining attack time / total system attack time. The evaluated systems are characterized as follows:

- System A: No defensive mechanisms.
- System B: Implements defenses against selected known vulnerabilities.
- System C: Employs moving target defense (MTD) techniques.
- System D: Utilizes the 5GC-PDA defense strategy.

As illustrated in Fig 5(b), System A, devoid of defensive capabilities, is compromised during the initial attack. System B possesses basic defensive mechanisms capable of detecting and defending against certain known threats; however, both threat detection and defensive deployment require time. As attackers gain familiarity with the system, they can breach it before defensive measures become fully operational. System C disrupts attackers by dynamically altering IP addresses and ports, significantly increasing the time cost for attackers to locate the system. Nevertheless, the system remains vulnerable to compromise under sustained attacks. System D demonstrates superior defensive efficacy: when under attack, it dynamically replaces targeted components through its redundant architecture and dynamic scheduling mechanism. Based on its triple-redundancy design, the system is compromised only when either all VNFs are simultaneously breached or the integrity of any two VNFs is compromised concurrently. Fig 5(c) compares the time costs required to breach the four systems, demonstrating that the time cost for attackers to compromise System D substantially exceeds that of the other systems.

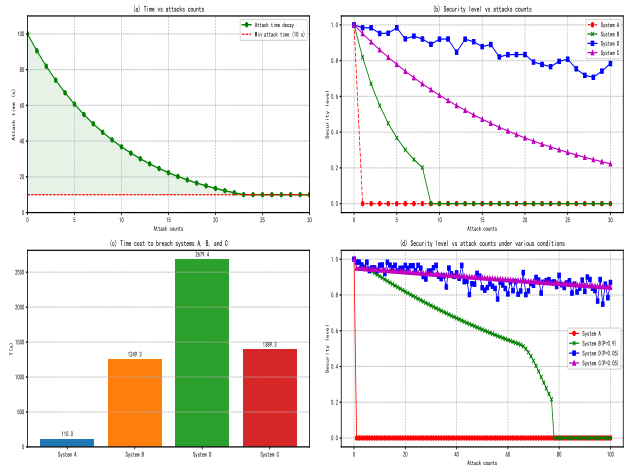


Fig. 5. Simulation results for different defense systems: (a) presents a model of the attacker's attack time varying with the number of attacks. (b) simulates the security performance of four different systems under attack. (c) illustrates the attack costs imposed on the attacker by the four defense systems. (d) compares the security capabilities of the four systems, assuming that the systems have a certain reconfiguration ability after being attacked.

As depicted in Fig 5(d), upon attack detection, systems may reconfigure their settings or perform environmental resets to increase attack difficulty. If such modifications can partially reset the attacker's accumulated experience, thereby prolonging the required attack duration, the defensive effectiveness of

Systems B, C, and D will be enhanced. However, owing to its static defense mechanisms, System B will ultimately be compromised. While both Systems C and D employ proactive defense strategies, System D demonstrates significantly superior overall defensive effectiveness compared to System C.

B. Prototype system testing

Using the critical Unified Data Management (UDM) function – designated Mimic UDM post-PDA transformation – as a representative case, we conducted security validation through simulated cyberattacks. Fig 6 delineates the attack trajectory: An adversary leveraged the CVE-2021-44228 vulnerability (Apache Log4j2 RCE) in an internal jump server to deploy a reflective shell, achieving unauthorized access and subsequent infiltration of the UDM host. The Mimic UDM system, comprising three functionally equivalent but architecturally heterogeneous instances (UDM1-3), included UDM3 with an intentionally configured SSH weak-password vulnerability. Following brute-force acquisition of root credentials, the attacker established remote SSH access to UDM3 and executed arbitrary commands.

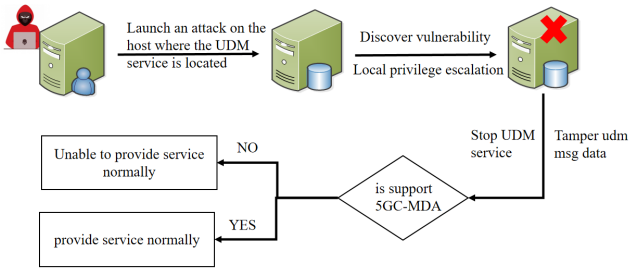
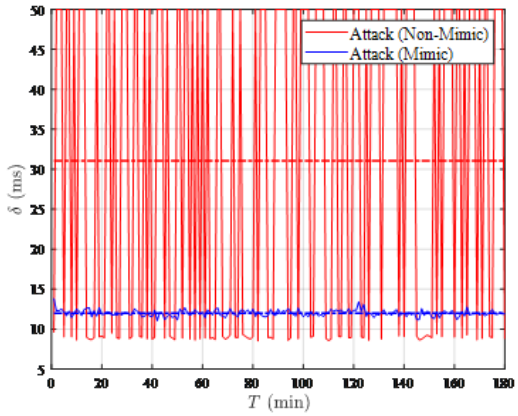


Fig. 6. UDM attack path map: The attacker first compromises an intermediary machine and then uses it to scan internal network service ports to identify the core network UDM service, which is subsequently targeted for attack. This section compares the security capabilities under two different UDM architectural frameworks.

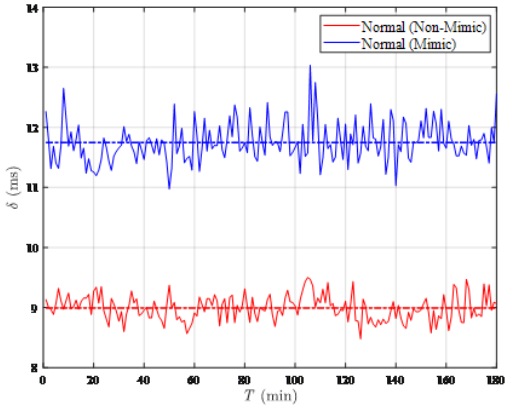
The test subjects included the standard UDM service (UDM3) and the mimic UDM service (comprising UDM1, UDM2, and UDM3). The test results are shown in the curve graph in Fig 7.

- Under normal (non-attack) conditions, we issued benign service requests to the interfaces of both the standard UDM service and the Mimic UDM service. Performance metrics were continuously monitored and recorded over a continuous three-hour testing period, with response times captured for each individual request.
- Under attack scenarios, benign service requests were issued to both standard UDM and Mimic UDM service interfaces, while attackers periodically targeted UDM3 with intrusion attempts. Throughout the three-hour test duration, response times for all requests were continuously monitored and recorded in real-time.

The blue curve quantifies the defensive efficacy of the Mimic UDM system, while the red curve corresponds to the no-mimic UDM implementation. Under simulated attacks administered at fixed intervals, Fig7(a) presents the measured service response times for both systems. Post-attack analysis reveals service disruption in the no-mimic UDM system, whereas the Mimic UDM maintained operational stability with only minor timing variations. Comparative assessment of experimental overhead between Mimic UDM and no-mimic UDM systems, as empirically demonstrated in Fig7(b), indicates that the Mimic UDM architecture necessitates a measurable performance trade-off to ensure security robustness.



(a) Attack result for Mimic vs Non-Mimic



(b) Latency comparison for Mimic vs Non-Mimic

Fig. 7. UDM real-world attack experiments result. The open-source UDM was modified according to the proposed architecture to implement a mimicry-based transformation. (a) compares attack/defense capabilities; (b) shows latency changes.

VI. CONCLUSION

This paper proposes an endogenous proactive defense mechanism to enhance the security of 5G core networks. The mechanism safeguards core network security through dynamic, heterogeneous, and redundant design principles. To ensure protocol consistency preservation, specialized registration, service

request, and deregistration procedures were designed, with formal verification of architectural security. Modeling analysis comparing four defense systems demonstrates the significant superiority of mimicry defense. For scientific validation, a mimic UDM system was developed on the free5GC platform, simulating vulnerability-injection cyberattacks. Comparative analysis of service continuity and defensive efficacy between mimic and non-mimic systems pre/post-attack was conducted alongside performance benchmarking. Results confirm that mimic UDM achieves substantial security improvements at quantifiable performance overhead. Future research will focus on: 1) integration mechanisms for Dynamic Heterogeneous Redundancy (DHR) and Network Function Virtualization (NFV), 2) security frameworks for distributed deployment scenarios, and 3) multidimensional security capability assessment in extended threat landscapes.

REFERENCES

[1] Rajib Taid, "5G Core Network Architecture," in Mobile Communications Systems Development: A Practical Introduction to System Understanding, Implementation and Deployment , Wiley, 2021, pp.447-472, doi: 10.1002/9781119778714.ch20.

[2] C. Coldwell, D. Conger, E. Goodell, B. Jacobson, B. Petersen, D. Spencer, M. Anderson, and M. Sgambati, "Machine learning 5g attack detection in programmable logic," in IEEE Globecom Workshops, 2022, pp. 1365–1370.

[3] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, W. Mallouli, A. Cavalli, D. Klonidis, E. Markakis, and P. Sarigiannidis, "Threatening the 5g core via pfcp dos attacks: the case of blocking uav communications," EURASIP J. Wirel. Commun. Netw., vol. 2022, no. 1, pp. 1–27, 2022.

[4] O.-M. Dumitru-Guzu and C. Vladeanu, "Analysis of potential threats in ˘ nextgen 5g core," in IEEE ISETC, 2022, pp. 1–4.

[5] Alnaim, A.K. Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security. Int. J. Inf. Secur. 23, 3569–3589 (2024). https://doi.org/10.1007/s10207-024-00900-5

[6] Y. Bello, A. R. Hussein, M. Ulema and J. Koilpillai, "On Sustained Zero Trust Conceptualization Security for Mobile Core Networks in 5G and Beyond," in IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 1876-1889, June 2022, doi: 10.1109/TNSM.2022.3157248.

[7] H. Whitworth, S. Al-Rubaye, A. Tsourdos and J. Jiggins, "5G Aviation Networks Using Novel AI Approach for DDoS Detection," in IEEE Access, vol. 11, pp. 77518-77542, 2023, doi: 10.1109/ACCESS.2023.3296311.

[8] Z. Abdelhay, Y. Bello, and A. Refaey, "Toward zero-trust 6gc: A software defined perimeter approach with dynamic moving target defense mechanism," IEEE Wirel. Commun., vol. 31, no. 2, pp. 74–80, 2024. [Online]. Available: https://doi.org/10.1109/MWC.001.2300358.

[9] G. D'Onghia, F. Ciravegna, G. Bruno, M. A. Elorza Forcada, A. Pastor and A. Lioy, "Securing 5G: Trusted Execution Environments for Centrally Controlled IPsec Integrity," 2024 IFIP Networking Conference (IFIP Networking), Thessaloniki, Greece, 2024, pp. 595-597, doi: 10.23919/IFIPNetworking62109.2024.10619852.

[10] N. Provos, "A virtual honeypot framework," in Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA, M. Blaze, Ed. USENIX, 2004, pp. 1–14. [Online]. Available: http://www.usenix.org/publications/library/ proceedings/sec04/tech/provos.htm.

[11] H. Zhu, J. Li, J. Hu and W. Li, "Failure-Aware and Automated Disaster Backup in the 5G Core Network," 2022 International Communication Engineering and Cloud Computing Conference (CECCC), Nanjing, China, 2022, pp. 48-53, doi: 10.1109/CECCC56460.2022.10069046.

[12] J. Cao et al., "A Survey on Security Aspects for 3GPP 5G Networks," in IEEE Communications Surveys Tutorials, vol. 22, no. 1, pp. 170-195, Firstquarter 2020, doi: 10.1109/COMST.2019.2951818.

[13] 3GPP TS 33.501 V17.7.0, "Security architecture and procedures for 5G system," 3rd Generation Partnership Project, Jun. 2024. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/33series/33.501/33501-h70.zip.

[14] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape for 5G Networks, Nov. 2019. [Online].Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

[15] China Academy of Information and Communications Technology (CAICT) and IMT-2020(5G) Promotion Group, "5G Security Report," CAICT, Beijing, China, Tech. Rep., Feb. 2020.

[16] IMT-2020(5G) Promotion Group and China Academy of Information and Communications Technology (CAICT), "5G Security Knowledge Base," CAICT, Beijing, China, Tech. Rep., Dec. 2021.

[17] N. Wehbe, H. A. Alameddine, M. Pourzandi, E. Bou-Harb and C. Assi, "A Security Assessment of HTTP/2 Usage in 5G Service-Based Architecture," in IEEE Communications Magazine, vol. 61, no. 1, pp. 48-54, January 2023, doi: 10.1109/MCOM.001.2200183.

[18] Kaizhi HUANG, Qirun PAN, Quan YUAN, Wei YOU. A Virtual Node Migration Method for Sensing Side-channel Risk[J]. Journal of Electronics Information Technology, 2019, 41(9): 2164-2171. doi: 10.11999/JEIT180905

[19] M. Pattaranantakul, R. He, Q. Song, Z. Zhang and A. Meddahi, "NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures," in IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 3330-3368, Fourthquarter 2018, doi: 10.1109/COMST.2018.2859449.

[20] Amponis, G., Radoglou-Grammatikis, P., Lagkas, T. et al. Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications. J Wireless Com Network 2022, 124 (2022). https://doi.org/10.1186/s13638-022-02204-5

[21] Z. Yan, G. Yu, M. Zhan, Y. Zhang and J. Hu, "5GC-SDP: Security Enhancement of 5G Core Networks With Zero Trust," 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Tianjin, China, 2024, pp. 1597-1602, doi: 10.1109/CSCWD61410.2024.10580371.

[22] W. Soussi, M. Christopoulou, G. Xilouris and G. Gür, "Moving Target Defense as a Proactive Defense Element for Beyond 5G," in IEEE Communications Standards Magazine, vol. 5, no. 3, pp. 72-79, September 2021, doi: 10.1109/MCOMSTD.211.2000087.

[23] G. D'Onghia, F. Ciravegna, G. Bruno, M. A. Elorza Forcada, A. Pastor and A. Lioy, "Securing 5G: Trusted Execution Environments for Centrally Controlled IPsec Integrity," 2024 IFIP Networking Conference (IFIP Networking), Thessaloniki, Greece, 2024, pp. 595-597, doi: 10.23919/IFIPNetworking62109.2024.10619852.

[24] N. Wehbe, H. A. Alameddine, M. Pourzandi and C. Assi, "5GShield: HTTP/2 Anomaly Detection in 5G Service-Based Architecture," 2023 IFIP Networking Conference (IFIP Networking), Barcelona, Spain, 2023, pp. 1-9, doi: 10.23919/IFIPNetworking57963.2023.10186410.

[25] P. Radoglou-Grammatikis et al., "5GCIDS: An Intrusion Detection System for 5G Core with AI and Explainability Mechanisms," 2023 IEEE Globecom Workshops (GC Wkshps), Kuala Lumpur, Malaysia, 2023, pp. 353-358, doi: 10.1109/GCWkshps58843.2023.10464667.

[26] J. Ortiz, R. Sanchez-Iborra, J. B. Bernab´e, A. F. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Mu˜noz, R. Vilalta, C. Gaber, J. Wary, D. Ayed,P. Bisson, M. Christopoulou, G. Xilouris, E. M. de Oca, G. G¨ur,G. Santinelli, V. Lefebvre, A. Pastor, and D. R. L´opez, "Inspire-5gplus:intelligent security and pervasive trust for 5g and beyond networks," in ARES 2020: The 15th International Conference on Availability,Reliability and Security, Virtual Event, Ireland, August 25-28, 2020,M. Volkamer and C. Wressnegger, Eds. ACM, 2020, pp. 105:1–105:10.[Online]. Available: https://doi.org/10.1145/3407023.3409219

[27] JS. Batewela, M. Liyanage, E. Zeydan, M. Ylianttila and P. Ranaweera, "Security Orchestration in 5G and Beyond Smart Network Technologies," in IEEE Open Journal of the Computer Society, vol. 6, pp. 554-573, 2025, doi: 10.1109/OJCS.2025.3563619.

[28] J. Song, K. Park, C. Park, J. Kim and I. Kim, "Analyzing the container security threat on the 5G Core Network," 2024 Silicon Valley Cybersecurity Conference (SVCC), Seoul, Korea, Republic of, 2024, pp. 1-3, doi: 10.1109/SVCC61185.2024.10637370.