Towards Establishing a Systematic Security Framework for Next Generation Cellular Networks

Tolga O. Atalay
A2 Labs LLC
tatalay@a2labs.com

Tianyuan Yu
UCLA
tianyuan@cs.ucla.edu

Lixia Zhang
UCLA
lixia@cs.ucla.edu

Angelos Stavrou
Virginia Tech
A2 Labs LLC
angelos@vt.edu

***Abstract*—Cellular core networks are deployed as a set of Virtual Network Functions (VNFs) to dynamically provide customized connectivity for specific use cases. These VNFs are software-based applications whose trust management and security rely on well-established network domain solutions and certificate-based trust mechanisms. As VNFs are frequently redeployed, migrated, and scaled across a diverse ecosystem, the reliance on static trust solutions introduces bottlenecks and operational complexities. This approach to trust undermines the ability to ensure seamless, secure, and efficient interactions in a rapidly evolving cellular ecosystem. Addressing these challenges necessitates a fundamental shift toward an architectural foundation that inherently embeds security and trust into the communication fabric. Named Data Networking (NDN) offers such a foundation by focusing on data-centric security, where trust is embedded within the data itself rather than being dependent on external entities or channels. Leveraging named entities, NDN makes it possible to construct fine-grained trust relationships across cellular domains, tenants, and network slices. This paradigm shift enables the cellular core to move beyond static security solutions, providing a cohesive and scalable framework for managing trust in next-generation cellular networks. In this paper, we propose the adoption of the NDN network model to address the limitations of traditional approaches and achieve seamless security that evolves with the dynamic demands of 5G and beyond networks.**

I. Introduction

The next-generation cellular networks are designed to provide ubiquitous connectivity to various use cases with diverse Quality of Service (QoS) requirements. Achieving this requires a flexible infrastructure that can seamlessly adapt to the unique needs of different verticals. To that end, services in Fifth Generation (5G) mobile networks are delivered through logically isolated segments denoted as network slices [1]–[3]. A network slice is formed by service chaining a set of Virtual Network Functions (VNFs) to provide customized connectivity for specific use cases. To facilitate the flexible formation of network slices, 5G leverages Network Functions Virtualization (NFV) as a fundamental building block [4].

As a result of embracing NFV, the cellular core network is deployed as a collection of software applications running on host-centric communication models. The network domain security and trust establishment requirements for these deployments have been standardized by the Third Generation Partnership Project (3GPP). These standards are rooted in traditional approaches, such as Transport Layer Security (TLS) for secure connectivity [5], and certificate-based trust establishment via the Public Key Infrastructure (PKI) [6]. While TLS ensures data security through robust cryptographic methods, a significant challenge lies in the distribution and management of certificates across VNFs. In the highly dynamic and ephemeral environment of the 5G core, where VNFs are frequently redeployed, migrated, or scaled, ensuring seamless and secure certificate provisioning remains a critical hurdle.

Given that the core network VNFs undergo frequent redeployment across diverse network slices and tenants, the resulting architecture exposes significant security and operational complexities. Traditional trust management mechanisms, while effective in static environments, lack the scalability, agility, and resilience needed to address the dynamic and distributed nature of the next-generation cellular core. Additionally, the reliance on host-to-host communication in this microservice-driven deployment model introduces another layer of complexity. Connection-based security mechanisms, such as TLS, tie security to individual sessions, requiring constant connection establishment and teardown as VNFs scale and migrate. This connection-centric security solution leads to significant overhead and operational complexity. These challenges highlight the need for a more flexible and resilient approach to ensure secure interactions within the 5G and beyond core network, all while reducing operational overhead.

To address this, we propose adopting the Named Data Networking (NDN) networking model [7] as an architectural foundation for the next-generation cellular core. Fundamentally, NDN redefines networking by establishing trust relationships among named entities to create a trust plane, and embed security into all data objects directly. This ensures that all received data can be verified based on the established trust relationships, eliminating the need for fixed host-to-host communication. Each piece of data is cryptographically signed to ensure integrity and authenticity regardless of the intermittent transmission elements that are involved. Moreover, the semantic nature of application data names enables finer-grained security policies that surpass the traditional connection-level approaches. This facilitates a scalable and dynamic trust man-

Workshop on Security and Privacy of Next-Generation Networks
(FutureG) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-7-3
https://dx.doi.org/10.14722/futureg.2025.23084
www.ndss-symposium.org

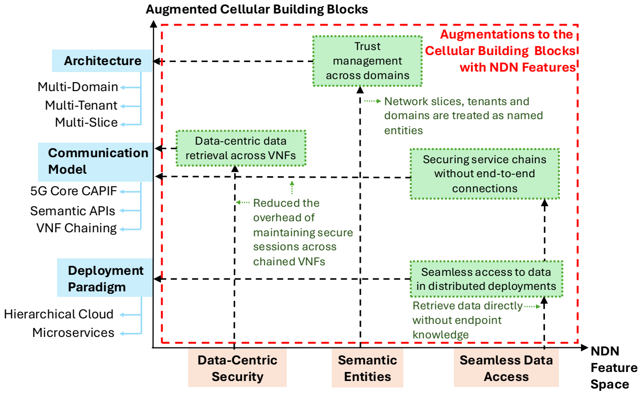
Augmented Cellular Building Blocks
Augmentations to the Cellular Building Blocks with NDN Features
Architecture
Multi-Domain
Multi-Tenant
Multi-Slice
Communication Model
5G Core CAPIF
Semantic APIs
VNF Chaining
Deployment Paradigm
Hierarchical Cloud
Microservices
Trust management across domains
Network slices, tenants and domains are treated as named entities
Data-centric data retrieval across VNFs
Securing service chains without end-to-end connections
Reduced the overhead of maintaining secure sessions across chained VNFs
Seamless access to data in distributed deployments
Retrieve data directly without endpoint knowledge
Data-Centric Security
Semantic Entities
Seamless Data Access
NDN Feature Space

Fig. 1: The emerging security features as a result of the synergistic relationship between NDN feature space and next-generation cellular building blocks

agement model that aligns with the ephemeral and distributed nature of 5G and beyond deployments.

In Figure 1, we show how elements of the NDN feature space provide key augmentations to the existing operational building blocks of next-generation cellular networks. Through highlighting the pivotal elements within each ecosystem that naturally align and complement one another, we illustrate in Figure 1 the emerging security features that NDN naturally introduces into the cellular ecosystem and summarize the benefits as three key enhancements.

Enhancement 1 - NDN Trust Management for Domains and Network Slices: The semantic naming-based approach of NDN provides a robust foundation for trust management, allowing 5G and beyond networks to establish fine-grained trust relationships across network slices, domains, and tenants. Thus, instead of relying on the external Web PKI, transitive trust relationships can be constructed directly by leveraging NDN naming conventions.

Enhancement 2 - Data-Centric VNF Communication: The 5G core is comprised of VNFs that are designed to be deployed across a distributed cloud hierarchy. The data-centric model of NDN aligns with this distributed microservice-based communication especially given that VNFs communicate using the Common API Framework (CAPIF) [8], [9] that already emphasizes semantics. With NDN, VNFs in network slice service chains can move beyond the traditional client/server model by eliminating the need for 5G core related registration and discovery signaling as well as the need for subsequent point-to-point secure session setup.

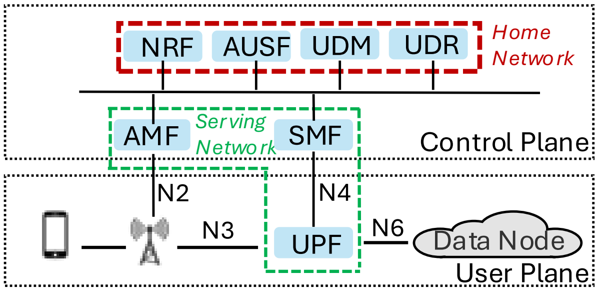

Fig. 2: 5G core Service Based Architecture

Enhancement 3 - Seamless Data Access: The NDN architecture inherently decouples data from its physical location, allowing VNFs in the 5G core to access data without needing to maintain continuous connectivity to specific endpoints. This eliminates the dependency on maintaining complex network states, enabling applications to seamlessly migrate and scale across distributed environments while preserving their operational state. For containerized VNFs, this synergy simplifies mobility and resource allocation by allowing them to fetch data on demand, independent of the underlying network infrastructure. Thus, by focusing on data availability rather than connectivity, NDN ensures uninterrupted communication even in highly dynamic and ephemeral network conditions.

II. Background Information

A. 5G Core Architecture and Network Security

The 5G core, as depicted in Figure 2, is designed as a Service Based Architecture (SBA) where VNFs communicate over Representational State Transfer (REST) APIs using HTTP. The cellular core can be broadly divided into the Home Network (HN) and, Serving Network (SN). Within the SN, the Access and Mobility Management Function (AMF) acts as the anchor point between the Radio Access Network (RAN), and the remainder of the core VNFs. Together with the Authentication Server Function (AUSF), Unified Data Management (UDM), and the Unified Data Repository (UDR) in the HN, the AMF participates in the 5G Authentication and Key Agreement (5G-AKA) for the UE and the core to mutually authenticate each other using secret hardware keys. Within the SN, the Session Management Function (SMF) and the User Plane Function (UPF) are the control and data plane anchors for a data session. Last but not least, the Network Repository Function (NRF) is the metadata database of the core network, maintaining VNF profiles and providing discovery and access token provisioning.

Interactions between 5G core VNFs currently follow a client/server model, where each VNF functions as a service consumer or provider in its communication with others. A sample message flow is given in Figure 3 depicting a simplified version of the session setup chain between the NRF, AMF, and

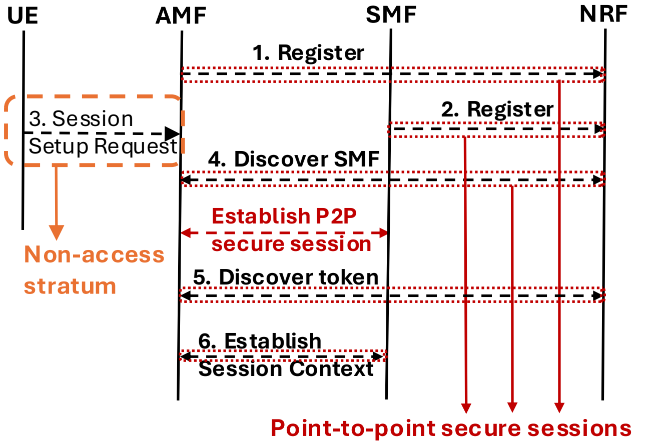

Fig. 3: Simplified message flow showing session setup chain between the NRF, AMF, and SMF over point-to-point secure communication

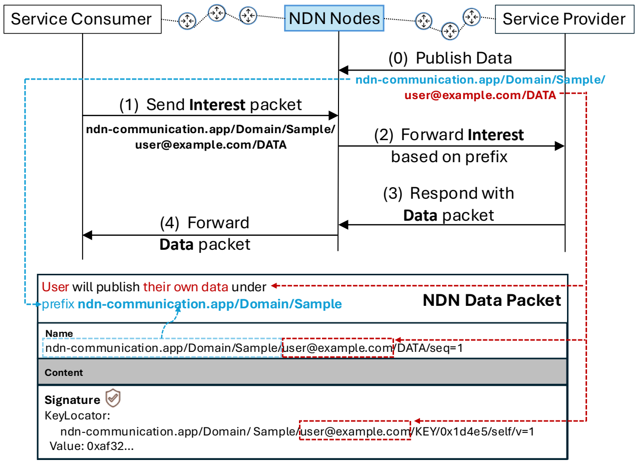
Service Consumer
NDN Nodes
Service Provider
(0) Publish Data
ndn-communication.app/Domain/Sample/
user@example.com/DATA
(1) Send Interest packet
ndn-communication.app/Domain/Sample/
user@example.com/DATA
(2) Forward Interest
based on prefix
(3) Respond with
Data packet
(4) Forward
Data packet
User will publish their own data under
prefix ndn-communication.app/Domain/Sample
NDN Data Packet
Name
ndn-communication.app/Domain/Sample/user@example.com/DATA/seq=1
Content
Signature
KeyLocator:
ndn-communication.app/Domain/ Sample/user@example.com/KEY/0x1d4e5/self/v=1
Value: 0xaf32...

Fig. 4: Overview of NDN forwarding with `Interest` and `Data` packets

SMF. In this interaction, both the AMF and SMF first register themselves with the NRF. Once a session setup request arrives from UE to the AMF, the latter discovers a candidate SMF from the NRF and proceeds to establish a secure point-to-point session (e.g., TLS session). Finally, AMF prompts the NRF for an access token, which is later attached to outgoing HTTP requests.

The VNFs are deployed on top of traditional IP-based infrastructure, where their network domain security relies on well-established concepts such as TLS and OpenAuthorization (OAuth) 2.0 for authentication and authorization [5], [10]. As a result, inter-VNF communication is dependent on the Web PKI framework, be it public or private, to provide trusted certificate management for securing the REST API endpoints. However, this reliance leads to scalability and efficiency challenges within the 5G core. Our NDN-based core formulation in Section III provides an alternative to this existing approach for a more flexible and scalable cellular core communication.

B. NDN Network Model

Data-centric security: In traditional IP-based networking, data is sent from a source to a destination address through the explicit definition of hosts, resulting in point-to-point communication. In contrast to this host-centric approach, NDN embraces a data-centric model where each piece of data is associated with a unique name [11]. Thus, the focus is on what the data is rather than where it is kept. The operational flow for an NDN system is illustrated in Figure 4. Initially, a service provider publishes their data with their local NDN node under a specific prefix. From this point onward, the NDN node with which the data was registered advertises the named data to other nodes in the network. When a service consumer wishes to obtain this data, it creates an `Interest` packet with the corresponding prefix. This `Interest` packet is then forwarded through the NDN nodes to the service provider. Finally, the service provider responds with a *Data* packet, which is cryptographically signed to ensure authenticity and integrity. With this data-centric approach to routing, NDN eliminates the need for point-to-point security mechanisms that focus on securing communication channels. In distributed environments composed of ephemeral microservices, such as cellular network slices, the repetitive signaling required to establish and maintain secure channels introduces significant overhead. The ability to fetch data using `Interest` packets without requiring knowledge of its exact location enables service consumers to request and retrieve data seamlessly, without needing to first discover the service provider.

NDN trust plane: NDN relies on semantic naming conventions to organize and manage trust relationships [11]. Each piece of data is uniquely named (e.g., `/ndn-communication.app/Domain/Sample/user@example.com` in Figure 4) where the name itself reflects the organizational structure and relationships within the network. This hierarchical naming naturally supports the delegation of trust. For instance, a higher-level entity (e.g., a 5G domain or sub-root network slice) can delegate signing authority to its sub-entities, allowing trust to propagate down the naming hierarchy. Using trust schemas, each NDN entity can sign specific types of data, with trust rules encoded to align naturally with the naming structure. Unlike traditional PKI-based systems, NDN does not require a centralized CA to establish trust. In contrast, trust is decentralized and derived through named entities and a signing process where public keys can be embedded as `KeyLocators` in the Data packet as illustrated in Figure 4) or fetched directly from the network. This results in a more scalable and resilient trust establishment, especially for distributed systems such as a cellular core.

III. NDN-Based Cellular Core Design

A. NDN Trust Management for Next-Generation Core

Cellular network deployments are hierarchically organized into different Public Land Mobile Network (PLMN) domains, where multiple tenants and operators can go ahead and deploy their network slices. This creates a multi-domain, multi-tenant,

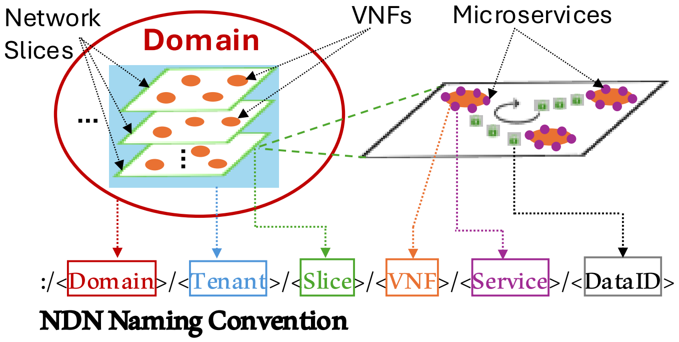

Fig. 5: NDN-based naming convention for trust management in next-generation of cellular networks with multi-domain/tenant/slice deployments

and multi-network slice ecosystem. Given the ubiquitous service nature of 5G, VNFs from different organizations can often be required to establish communication with each other even though they may belong to a different network slice, tenant, or even a different domain. For instance, an **Operator A** can design and deploy a custom Application Function (AF) [12] to collect key performance metrics that may require access to multiple other network slices. In such a scenario, inter-network slice trust needs to be well-defined and managed.

Leveraging the hierarchical trust schematic feature of NDN that was explained in Section II-B, we propose the trust management paradigm in Figure 5 for the next generation of mobile networks. This design introduces a scalable, fine-grained approach to trust management across the PLMN, tenant, slice, and VNF levels, replacing traditional reliance on centralized Certificate Authorities (CAs) that fail to provide transitive trust properties.

The NDN naming hierarchy proposed in Figure 5 follows the systematic structure: `/<Domain>/<Tenant>/<Slice>/<VNF>/<Service>` `/<DataID>`, where each component of the naming convention encodes a specific hierarchy. At the top, there is the PLMN designation, followed respectively by the tenant in that PLMN and a network slice being run by that tenant. Tenants may represent Mobile Virtual Network Operators (MVNOs) or other network entities that lease resources. Multiple tenants can coexist under the same PLMN, with trust relationships isolated at this level. The network slice designator after the tenant, specifies a certain network slice allocated to that tenant. Network slices are logically isolated and serve different Slice Service Types (SSTs) [8] (enhanced Mobile Broadband, Ultra Reliable Low Latency Communication, etc.). Trust at this level ensures that slices can securely communicate within their scope.

With this approach to trust management that relies on NDN trust schemas, it becomes possible to delegate signing authority across a hierarchical naming structure, embedding trust directly within the data and eliminating the need for centralized CAs. At the top of the trust hierarchy, a root entity-such as the 5G network operator can establish the initial trust anchor. From this root, signing authority can be further delegated for finer-grained management of inter-domain, inter-tenant, and inter-network slice trust establishment. This hierarchical structure allows trust to propagate naturally across domains, tenants, slices, and VNFs. On the consumer side (i.e., service consumer VNFs), data authenticity and integrity are verified using the hierarchical naming structure and the trust rules defined in the trust schema. In a realistic 5G multi-tenant environment, the operator can act as the root trust authority, but trust delegation to domains, tenants, and network slices ensures they have autonomy over their namespaces. With this proposed model, there is global security enforcement while also making sure that tenants and network slices can act as independent entities for finer-grained trust management.

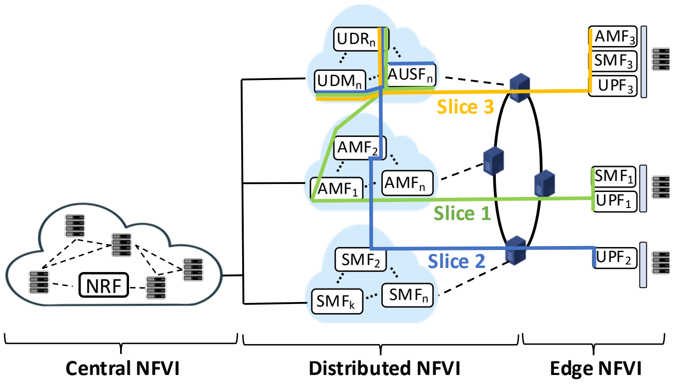

Fig. 6: 5G network slice deployments with VNFs deployed in different cloud hierarchies to accommodate different QoS requirements

B. Data-centric Security in the Cellular Core

The second enhancement as a result of adopting NDN in the cellular core is the transition to data-centric security and the seamless access to data, regardless of VNF location.

The existing signaling model of the cellular core, summarized in Figure 3, has two major shortcomings in supporting a scalable and flexible cellular deployment: **1)** the native registration/discovery approach adopted by the 5G core with token-based authorization; **2)** the need to establish point-to-point secure sessions between the VNFs [5]. These shortcomings become more pronounced as cellular core deployments transition to distributed cloud deployments as illustrated in Figure 6, where VNFs can reside in central, distributed, or edge clouds, depending on the use case they serve. For example, in a low-latency use case such as Ultra Reliable Low Latency Communication, the SMF and UPF are often deployed near the edge cloud. Placing both VNFs at the edge minimizes data plane latency and accelerates frequent session setups and teardowns which is essential for applications like autonomous driving or AR/VR, where latency requirements are stringent. On the other hand, in cases where significant control plane interactions are required, such as mobility-driven use cases or high signaling workloads, the AMF may also be moved to the edge cloud alongside the SMF and UPF.

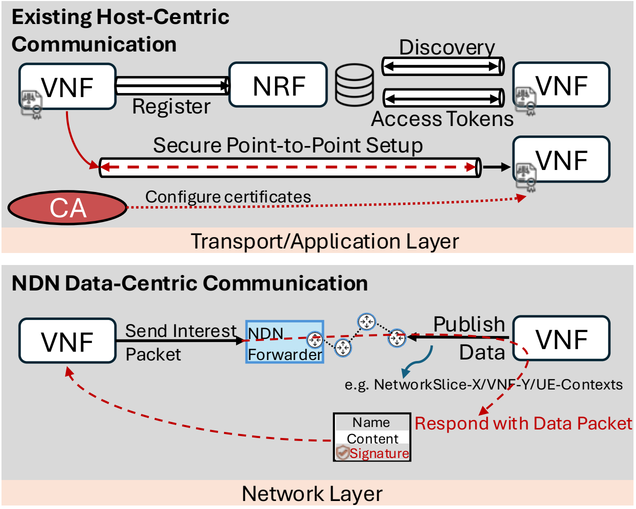

Fig. 7: Transition to data-centric NDN-based 5G core communication compared with the existing registration and token processing communication model

For instance, this setup supports use cases like edge-based mobility management or frequent user handovers, ensuring that control plane and data plane operations remain tightly coupled, reducing signaling delays between AMF and SMF.

In such a distributed deployment, the overhead associated with discovery and secure session establishment procedures in Figure 3 scales with inter-site latency, which varies depending on the location of the VNFs. Furthermore, since network slices are ephemeral, the VNFs can be dynamically moved or re-deployed across different sites. This dynamic nature increases the frequency of discovery operations, thereby increasing the complexity of maintaining secure, reliable connections between VNFs in a scalable way.

The transition to NDN is illustrated in Figure 7, where the communication model transitions to a data-centric approach, eliminating the need for centralized discovery mechanisms like the NRF. Instead of relying on registration and discovery, VNFs can directly request data by leveraging semantic prefixes, combining those defined in CAPIF APIs with network slice-specific designators (e.g., **NetworkSlice-X/VNF-Y/UE-Contexts** in Figure 7) to retrieve the target information. This shift removes the dependency on a dedicated entity for service discovery and simplifies the interactions between VNFs. Additionally, the data-centric security model of NDN eliminates the need to establish point-to-point secure sessions between VNFs. Securing the data itself rather than the communication channel, NDN reduces the overhead associated with session setup and management, enabling a more efficient and scalable framework for 5G core deployments, particularly in cloud environments where inter-site latency can otherwise degrade performance. Given the transitive nature of network slices, where VNFs are frequently re-deployed, migrated, or scaled based on dynamic workload demands, the repeated signaling and secure session establishment add significant latency and resource overhead. Removing these requirements, NDN ensures faster and more reliable inter-VNF communication.

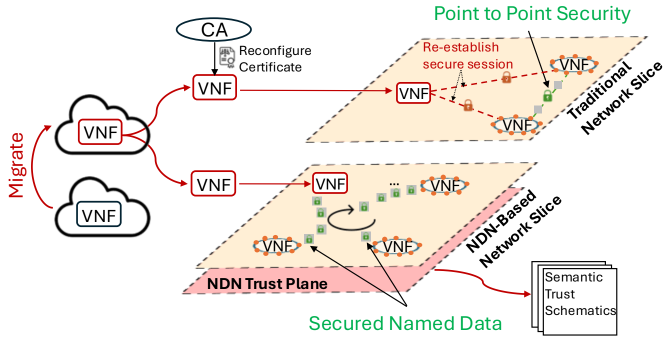

Fig. 8: 5G VNF migration in traditional cellular core vs NDN-based cellular core

C. *Seamless Data Access*

Building on the adoption of the NDN trust plane for trust establishment in next-generation cellular networks, along with data-centric security, the next enhancement focuses on the ability to preserve application state independently of the network state. This characteristic offers a significant benefit for dynamic and distributed environments like the 5G core, where VNFs are frequently re-deployed, migrated, or scaled to meet varying operational demands.

A sample 5G core VNF migration scenario is illustrated in Figure 8. For traditional host-centric communication models, VNFs rely on maintaining established connections to ensure seamless communication. Thus, when migrating a containerized application (e.g., a 5G core VNF) to a different host or network slice, it is not sufficient to simply preserve the application state; the associated network state, including active connections, session-specific data, and cryptographic certificates, must also be transferred to maintain continuity. Certificates, in particular, require careful reconfiguration to align with the new network context and ensure secure communication, adding to the operational complexity. This dependency complicates the migration process and introduces potential points of failure,

TABLE I: Comparison of certificate reconfiguration in traditional systems vs. NDN-based systems

Aspect	Traditional Systems	NDN-Based Systems
Certificate Scope	Endpoint-specific (host/IP/domain)	Data-specific (naming hierarchy)
Reconfiguration	Required for VNF migration or scaling	Not required; trust is decoupled from hosts
Operational Overhead	High, involves multiple entities (CA, DNS, etc.)	Low, integrated into the NDN naming schema
Trust Management	Centralized, dependent on CAs	Decentralized, follows transitive trust rules
Migration Impact	Requires re-establishment of secure sessions	No sessions required

particularly in dynamic environments where frequent reconfiguration is required.

In contrast, the data-centric approach of NDN eliminates the need for maintaining host-to-host connectivity and simplifies certificate management. With NDN, communication is based on the hierarchical naming of data rather than fixed network addresses, and certificates are tied to these semantic names rather than specific endpoints. This decoupling of application state from the network state enables a containerized VNF to be migrated or scaled without disrupting its ability to communicate or requiring certificate reconfiguration. As long as the application state, including its cryptographic keys and hierarchical naming schema, is preserved, the VNF can seamlessly rejoin the network and resume its operations. There is no need to re-establish network sessions, transfer session-specific data, or reconfigure certificates, as data requests and responses are inherently self-contained within the NDN naming and security framework.

The key differences in certificate reconfiguration between traditional systems and NDN-based systems are summarized in Table I, emphasizing how NDN eliminates the need for reconfiguration during migration or scaling, thereby reducing operational overhead and enhancing flexibility.

The synergy between the data-centric paradigm of NDN and containerized deployments in the 5G core is particularly impactful. Containers are inherently designed for portability, enabling applications to be moved across hosts or regions with minimal downtime. NDN complements this by ensuring that communication remains unaffected by the underlying network changes and that certificates tied to data names remain valid and effective across different network contexts. For example, a migrated AF [12] container can continue to fetch and verify performance metrics from other VNFs without the need for re-establishing connections, reconfiguring network policies, or updating certificates. This is possible because the data being fetched is secured and routed based on its name rather than the location of the hosting entity.

Moreover, this seamless access to data supports the distributed and ephemeral nature of 5G VNFs, reducing the operational overhead associated with maintaining network state and reconfiguring certificates during migrations. It also enhances reliability by removing dependencies on host-centric configurations and complex certificate reissuance processes, making the 5G core more resilient to failures and adaptable to dynamic workloads. This characteristic of NDN further strengthens its suitability as a foundational architecture for next-generation cellular networks.

IV. Integrating NDN into the 5G Core: Proof-of-Concept

This section presents our initial proof-of-concept design to demonstrate how cellular networks can benefit from the NDN security features and adopt the trust plane formulation that was introduced in Section III. Our primary objective with the current system design is to make sure that the integration takes place seamlessly, without disrupting the existing operational model of the endpoint VNFs. To achieve this, we build an NDN overlay to encapsulate the 5G core deployment using cloud-native development tools such as the Side Car Proxy (SCP) [13], [14] and service meshes [15]–[17]. The full system design is illustrated in Figure 9, which shows the deployment within a Kubernetes hierarchy, ranging from cluster-, node-, to pod-level components.

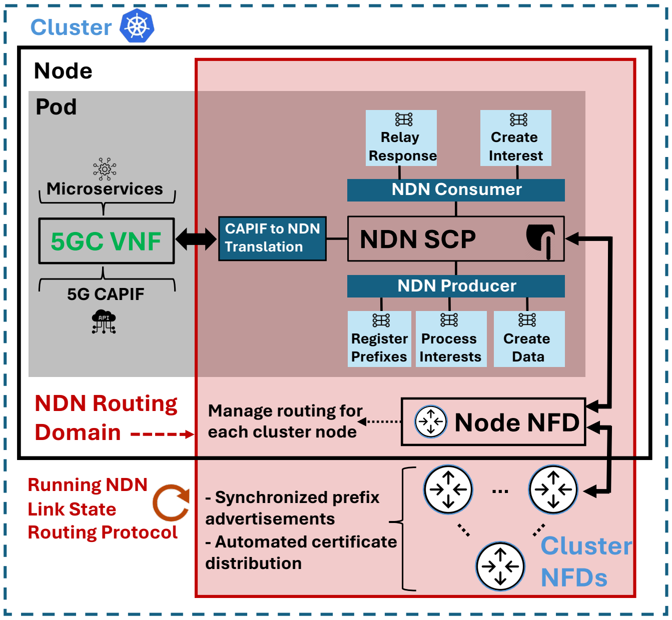

Fig. 9: The NDN service mesh overlay encapsulating the 5G core deployment in a Kubernetes-based deployment

In our Kubernetes deployment, we establish an NDN routing domain where each node includes an NDN Forwarder, specifically the NDN Forwarding Daemon (NFD) [18], to handle routing operations. The NFD instances on individual nodes are interconnected across the cluster. The NDN Link State Routing (NLSR) protocol [19] is employed to synchronize prefix advertisements throughout the cluster. To ensure secure communication between NFD instances, the deployment includes an automated process for generating and distributing certificates, which are placed into newly deployed NFDs as part of the setup.

Our key design piece that enables this integration is the construction of a custom NDN SCP that sits adjacent to each cellular core VNF. As seen in Figure 9, each pod is comprised of two containers. The first container is the 5G core VNF (e.g., AMF, SMF) that adheres to the CAPIF, while the second container is the NDN SCP that sits adjacent to this VNF to provide it with an abstraction layer towards the NDN routing domain. To that end, the NDN SCP serves as the pod-level anchor for the VNF by providing three primary services that are summarized below.

1) CAPIF to NDN translation: We avoid modifying the 5G core VNFs directly to make sure that our design can be seamlessly adopted. However, as a result, the 5G core VNFs remain adherent to the CAPIF and continue to

TABLE II: Comparison of NDN security and operational features with existing cellular core network mechanisms

Aspect	NDN Mechanisms	Existing Mechanisms
Security Features		
Trust Model	Semantic naming-based trust management	Host-centric PKI-based trust (e.g., TLS, IPsec)
Key Management	Decentralized, tied to naming convention and transitive relationships	Centralized, requiring frequent updates and maintenance
Data Integrity	Ensured at the network layer for each data packet	Ensured per session, requiring continuous verification
Inter-Slice Communication	Seamless trust establishment using semantic NDN names	Requires explicit configuration policies
Inter-VNF Authentication	Embedded in data via cryptographic signatures	End-to-end authentication at session-level
Multi-Tenant Support	Transitive trust allows easy integration of multiple entities	Complicated by centralized trust agreements and scaling
Operational Features		
Scalability	High scalability due to transitive trust relationships across domains and slices	Limited scalability with centralized CA
Latency Overhead	Low, discovery and session overhead is eliminated	Higher due to repetitive signaling requirements
Complexity	Reduced complexity as no need for session-level security management	High due to dynamic VNF scaling, requiring frequent re-authentication
Adaptability	Agile and efficient for dynamic, distributed cloud environments	Rigid for distributed architectures

communicate over HTTP using REST APIs. Thus, the NDN SCP intercepts outgoing and incoming HTTP messages to translate the CAPIF API path to our NDN naming convention. This is especially convenient since the core network CAPIF already possesses semantic features. As an example, the path **`/nsmf-pdusession/v1/smcontexts`** is used to locate the context creation endpoint of the SMF. As an initial proof-of-concept, the NDN SCP will add slice-level information to this endpoint to indicate which network slice the interest originates from in adherence to our naming convention introduced in Figure 5.

2) NDN consumer: As part of the NDN communication model, this module creates the outgoing interest packets that are propagated into the NDN routing domain. The interest prefix is the output of the CAPIF to NDN translation. For any data packet that is received back from the NDN routing domain, the consumer will relay it back to the 5G core VNF.

3) NDN producer: The producer registers the prefixes with an NFD to make sure that interest packets reach the correct VNF. Using the `/Domain-Name/Network-Slice-ID/VNF-Type/Service-Name` naming convention, it becomes possible to distinguish between VNFs that reside in different domains and network slices.

This initial proof-of-concept demonstrates how NDN principles can be integrated into a working cellular core network.

V. Security and Operational Analysis

The key differences between the NDN-based cellular core and the standard security practices are highlighted in Table II.

Security. NDN represents a major shift in how trust is managed, moving away from traditional host-based authentication and centralized PKI systems. Instead, NDN uses a naming-based trust model, which enables flexible and detailed trust management across different domains, tenants, and slices without relying on centralized CAs. Unlike traditional methods that depend heavily on session-level configurations and centralized control—often creating bottlenecks in large-scale, dynamic environments—NDN secures data by embedding cryptographic signatures directly into packets. This ensures both authentication and data integrity, independent of the underlying transport layer. As a result, there is no need for ongoing session-level verification, offering a more streamlined and reliable security approach. NDN's decentralized approach to key management ties cryptographic keys to hierarchical naming conventions and transitive trust relationships. This reduces the operational complexity of frequent key updates. Traditional systems often struggle to handle the complexity of reconfiguring certificates and managing keys in such dynamic environments. NDN addresses these challenges by using semantic naming for authenticating communications between slices and VNFs. This approach helps maintain trust relationships even in rapidly changing scenarios.

Operational. The transitive trust relationships inherent in NDN naming conventions allow it to scale seamlessly across domains and slices, whereas traditional approaches rely on centralized CAs, which impose scalability limitations. Furthermore, NDN eliminates the need for repetitive signaling overhead that is used in the 5G core for registration, discovery, and access token acquisition, thus leading to lower operational latency. This is especially critical in 5G and beyond environments, where latency-sensitive applications demand consistent performance. NDN simplifies the integration of distributed cloud environments, allowing VNFs to migrate, scale, or reconfigure without the need for session-level security management. In contrast, traditional models require extensive re-authentication and network reconfiguration, adding operational overhead and complexity. This adaptability aligns well with the dynamic and ephemeral nature of cellular core VNFs, enabling faster deployments and reduced management burden.

Attack Mitigation. As a result of NDN adoption, the cellular core is hardened against several existing attacks summarized in Table III. For instance, NDN provides a higher degree of resilience to Distributed Denial of Service (DDoS) by

TABLE III: Comparison of NDN attack mitigation mechanisms with existing cellular core network mechanisms

Attack	NDN Mechanisms	Existing Mechanisms
DDoS Attacks	Name-based routing and caching reduce reliance on specific servers, mitigating resource exhaustion	Resource exhaustion at centralized VNFs (i.e., NRF) or endpoints is a significant vulnerability
Man-in-the-Middle	Data-centric cryptographic signatures ensure authenticity and integrity of data packets	Endpoint authentication mechanisms are vulnerable if VNFs compromised
Intrusion Attacks	Fine-grained trust and hierarchical naming schemes prevent unauthorized data access	Endpoint-based security leaves systems vulnerable to unauthorized host access
Replay Attacks	Nonce and freshness checks in data signatures prevent replayed data from being accepted	Rely on session-level validation, which can be bypassed
Routing Attacks	Interest packet forwarding based on names prevents malicious redirection of traffic	Vulnerable to routing table poisoning and traffic redirection

shifting from a “pushing to destinations” to “delivering upon requests” approach [20]. For intrusion attacks, the NDN semantic naming convention provides finer-grained trust control. This prevents unauthorized access at the data level rather than the host level, while endpoint-centric security is vulnerable to host-level intrusions. Additionally, NDN addresses replay attacks through nonce and freshness checks embedded within data signatures, ensuring that stale data cannot be reused maliciously [21]. Traditional models, by comparison, rely on session-level validations that are easier to bypass. Lastly, by relying on interest packet forwarding based on semantic names, NDN offers inherent protection against routing attacks that would seek the malicious redirection of traffic. In traditional systems, routing table poisoning and traffic redirection remain significant vulnerabilities due to the reliance on fixed network addresses and host-level configuration.

VI. Related Work

As a future Internet architecture paradigm NDN has matured over the past years. Research has been conducted that modified existing applications for NDN deployment, such as decentralized photo sharing [22], Metaverse applications [23], and satellite communications [24]. However, existing research has yet to explore the incorporation of NDN into the cellular ecosystem, let alone demonstrate a proof-of-concept implementation to showcase a seamless integration.

As cellular networks have evolved, numerous studies have leveraged cloud-native tools for enhancing and devising various security and performance enhancements for the core network. A very recent and pertinent research [25] highlights a shift from traditional host-centric approaches to a data-centric paradigm, aiming to improve the scalability and flexibility of cellular networks. The study employs data-centric methods to enable seamless interaction and integration of services in a fully distributed cellular framework, thereby enhancing service orchestration and optimizing resource management. Despite these advancements, the study does not delve deeply into the security challenges posed by such architectures and lacks a concrete design for ensuring data integrity. In contrast, our proposed framework leverages NDN to inherently introduce data-centric security and trust management features into the cellular core.

In another study [26], the authors have proposed a decentralized authorization scheme for the 5G core. Instead of relying on the centralized NRF for token-based authorization, VNFs can leverage WAVE [27] for decentralized and transitive authorization delegation for inter-VNF and inter-slice communication. While this approach eliminates the need for reliance on the NRF, it introduces other proprietary entities that are centralized. Thus, the adoption of this scheme does not eliminate centralization entirely but rather shifts it from the 5G core to the WAVE abstraction domain. Even though this may address some scalability issues within the 5G core, it ultimately replaces one form of centralization with another.

VII. Conclusion and Future Work

Conclusion. This paper proposes adopting NDN as the architectural foundation for next-generation cellular core networks, introducing key enhancements to address the limitations in the existing security solutions. Embracing a data-centric security model and leveraging the semantic naming convention of NDN, the proposed approach to cellular core security redefines trust management across network slices, tenants, and domains, enabling fine-grained, scalable, and transitive trust relationships. Additionally, the seamless data access facilitated by NDN decouples application state from network state, allowing for efficient VNF migration and scaling without the need for reconfiguring certificates or maintaining session-level security. Together, these enhancements position NDN as a transformative architecture to strengthen the security, adaptability, and operational efficiency of 5G and beyond cellular networks. Last but not least, we provide an initial proof-of-concept that demonstrates how NDN can be integrated into the cellular core without disrupting existing operational flows.

Future Work. As future work, we plan to conduct computational and latency overhead evaluations for the NDN-5G core integration to demonstrate the real-life practical challenges of adopting such an overlay. Furthermore, various network attacks will be carried out against both the traditional cellular core and the NDN-based core to compare the respective behaviours of the two architectures. Last, but not least, we plan to eventually embrace a more cloud-native integration model by developing an NDN-based Container Networking Interface (CNI) [28] for Kubernetes. This will enable 5G core deployments to directly communicate using the NDN networking model when they are instantiated as part of a Kubernetes deployment.

References

[1] S. Zhang, "An Overview of Network Slicing for 5G," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019.

[2] T. O. Atalay, D. Stojadinovic, A. Stavrou, and H. Wang, "Scaling Network Slices with a 5G Testbed: A Resource Consumption Study," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2022, pp. 2649–2654.

[3] M. Chahbar, G. Diaz, A. Dandoush, C. Cérin, and K. Ghoumid, "A Comprehensive Survey on the E2E 5G Network Slicing Model," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 49–62, 2020.

[4] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN—Key Technology Enablers for 5G Networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2468–2478, 2017.

[5] T. S. G. Services and S. Aspects, "Network Domain Security (NDS); IP network layer security," 3rd Generation Partnership Project (3GPP), TS 33.210 V18.1.0 , Jun. 2024.

[6] ——, "Network Domain Security (NDS); Authentication Framework (AF)," 3rd Generation Partnership Project (3GPP), TS 33.310 V19.2.0 , Sep. 2024.

[7] A. Afanasyev, T. Refaei, L. Wang, and L. Zhang, "A Brief Introduction to Named Data Networking," in *Proc. of IEEE MILCOM*, Oct. 2018.

[8] T. S. G. Services and S. Aspects, "System Architecture for the 5G System (5GS); Stage 2," 3rd Generation Partnership Project (3GPP), TS 23.501 V19.0.0 , Jun. 2024.

[9] ——, "Security Aspects of Common API Framework (CAPIF) for 3GPP Northbound APIs," 3rd Generation Partnership Project (3GPP), TS 23.501 V19.0.0 , Jun. 2024.

[10] ——, "Security Architecture and Procedures for 5G System," 3rd Generation Partnership Project (3GPP), TS 33.501 V19.0.0 , Sep. 2024.

[11] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "An Overview of Security Support in Named Data Networking," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 62–68, 2018.

[12] T. S. G. C. Network and Terminals, "5G System; Application Function Event Exposure Service; Stage 3," 3rd Generation Partnership Project (3GPP), TS 29.517 V19.0.0 , Dec. 2024.

[13] G. Yuan, D. K. Zhang, M. Sotoudeh, M. Welzl, and K. Winstein, "Sidecar: In-Network Performance Enhancements in the Age of Paranoid Transport Protocols," in *Proceedings of the 21st ACM Workshop on Hot Topics in Networks*, 2022, pp. 221–227.

[14] S. Ashok, P. B. Godfrey, and R. Mittal, "Leveraging Service Meshes as a new Network Layer," in *Proceedings of the Twentieth ACM Workshop on Hot Topics in Networks (HotNets)*, 2021, pp. 229–236.

[15] W. Li, Y. Lemieux, J. Gao, Z. Zhao, and Y. Han, "Service Mesh: Challenges, State of the Art, and Future Research Opportunities," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. IEEE, 2019, pp. 122–1225.

[16] T. Atalay, S. Maitra, D. Stojadinovic, A. Stavrou, and H. Wang, "Securing 5G OpenRAN with a Scalable Authorization Framework for xApps," in *IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2023, pp. 1–10.

[17] H. Saokar, S. Demetriou, N. Magerko, M. Kontorovich, J. Kirstein, M. Leibold, D. Skarlatos, H. Khandelwal, and C. Tang, "{ServiceRouter}: Hyperscale and Minimal Cost Service Mesh at Meta," in *17th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 2023, pp. 969–985.

[18] NFD, "NFD: Named Data Networking Forwarding Daemon." [Online]. Available: https://docs.named-data.net/NFD/current/

[19] A. M. Hoque, S. O. Amin, A. Alyyan, B. Zhang, L. Zhang, and L. Wang, "NLSR: Named-data Link State Routing Protocol," in *Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking*, 2013, pp. 15–20.

[20] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in Named Data Networking," in *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2013, pp. 1–7.

[21] M. S. M. Shah, Y.-B. Leau, M. Anbar, and A. A. Bin-Salem, "Security and Integrity Attacks in Named Data Networking: A Survey," *IEEE Access*, vol. 11, pp. 7984–8004, 2023.

[22] V. Patil, T. Yu, X. Ma, and L. Zhang, "Decentralized Photo Sharing via Named Data Networking," in *Proceedings of the 10th ACM Conference on Information-Centric Networking*, 2023, pp. 118–120.

[23] T. Yu, X. Ma, V. Patil, Y. Kocaogullar, Y. Zhang, J. Burke, D. Kutscher, and L. Zhang, "Secure Web Objects: Building Blocks for Metaverse Interoperability and Decentralization," in *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)*. IEEE, 2024, pp. 25–33.

[24] S. Theeranantachai, B. Zhang, and L. Zhang, "NDN's Stateful Forwarding Plane Meeting Frequent Connectivity Changes of LEO Satellite Constellations," in *Proceedings of the 10th ACM Conference on Information-Centric Networking*, 2023, pp. 127–129.

[25] G. Baldoni, J. Quevedo, C. Guimaraes, A. de la Oliva, and A. Corsaro, "Data-centric Service-based Architecture for Edge-native 6G Network," *IEEE Communications Magazine*, 2023.

[26] P. Sharma, T. Atalay, H. A. Gibbs, D. Stojadinovic, A. Stavrou, and H. Wang, "5G-WAVE: A Core Network Framework with Decentralized Authorization for Network Slices," in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications*. IEEE, 2024, pp. 2308–2317.

[27] M. P. Andersen, S. Kumar, M. AbdelBaky, G. Fierro, J. Kolb, H.-S. Kim, D. E. Culler, and R. A. Popa, "{WAVE}: A Decentralized Authorization Framework with Transitive Delegation," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 1375–1392.

[28] S. Qi, S. G. Kulkarni, and K. Ramakrishnan, "Assessing Container Network Interface Plugins: Functionality, Performance, and Scalability," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 656–671, 2020.