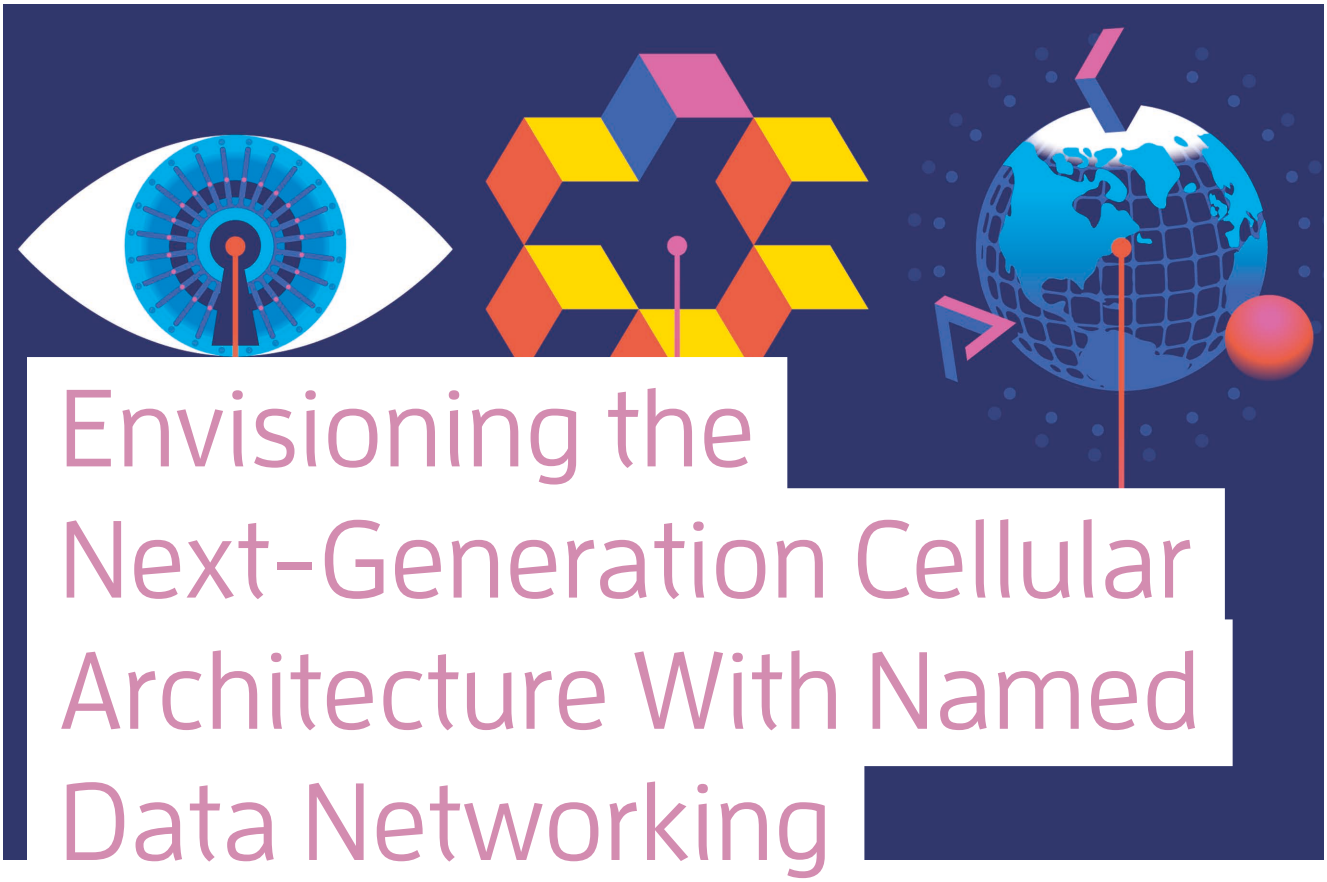

Envisioning the Next-Generation Cellular Architecture With Named Data Networking

Tolga O. Atalay, A2 Labs
Angelos Stavrou, A2 Labs and Virginia Tech
Lixia Zhang, University of California, Los Angeles

This article proposes adopting named data networking (NDN) as a foundation for future cellular networks, including 6G, to shift the focus from connection-based to data-centric communication. Securing data at the network layer, NDN reduces control plane signaling overhead and enables secure distributed deployments.

The next-generation cellular networks are designed to provide ubiquitous connectivity to a wide range of vertical use cases with different quality-of-service (QoS) requirements. To that end, the deployment model of 5G networks adopts a distributed and modular design, comprised of service-chained virtual network functions (VNFs) hosted on commercial off-the-shelf (COTS) hardware. Compared to the legacy long term evolution (LTE) where physical network functions (PNFs) were bound to proprietary hardware, the transition to virtualized deployments enhances the flexibility and scalability of cellular networks. In 5G, services are delivered by dynamically interconnected sets of VNFs that form "network slices." [1] Each network slice serves as a logically distinct segment of the network,

Digital Object Identifier 10.1109/MC.2025.3570331
Date of current version: 28 July 2025

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

0018-9162 © 2025 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies.

tailored to meet the QoS demands of a given use case.

MOTIVATION

Network slices in 5G are transient, with service chains being continuously reconstructed to accommodate diverse user demands, mobility patterns, and service requirements. This existing network slice-based cellular ecosystem is built on top of a traditional IP-based architecture and uses well-established network protocols. As an example, inter-VNF communication in the 5G core service-based architecture (SBA) takes place over HTTP, leveraging transport layer security (TLS) and OpenAuthorization (OAuth) 2.0 for managing authentication and authorization.[2] While these are mature solutions, they are designed for point-to-point, session-based communications and induce nonnegligible overhead to the communication. Given the transient nature of network slices, the signaling overhead associated with repeated creation and tear-down of secure service chains leads to increased process completion times using the classical networking architecture. To optimize and secure the deployment of cellular networks, cloud-native tools are being adopted to enhance the delivery of 5G services. These include but are not limited to, tools like the extended Berkeley Packet Filter (eBPF),[3] service meshes,[4,5] and Kubernetes[6] for container orchestration. Leveraging such technologies offers capabilities for more efficient traffic management, observability, and dynamic scaling of services. However, while these frameworks provide benefits, they are not adequate on their own. Instead, they need to be applied within an architecture fundamentally more suited to the demands of next-generation cellular networks, rather than layered on top of a traditional, session-based model.

CONTRIBUTION

As an alternative to the existing session-based approach, we propose the adoption of named data networking (NDN)[7] as an architectural foundation, which is better suited for a distributed deployment such as the next-generation of cellular networks. Unlike the traditional IP-based architecture that focuses on specific hosts, NDN focuses directly on data. Thus, in an NDN-enabled 5G core, inter-VNF communication would use data names rather than host addresses. As a result of this paradigm shift, the VNFs in the network slice service chains will no longer need to follow the typical client/server model, requiring them to go through the process of registration, discovery, and setting up point-to-point secure sessions.[2,8] As cellular networks embrace distributed deployment with a microservice-based architecture, NDN offers the ability to request data directly, without needing to know where a service is located. This flexibility simplifies the reconfiguration of network services and resources by removing the need to maintain individual secure sessions. This makes NDN a more suitable architectural choice for the decentralized and microservice-based deployments that characterize the future of cellular networks.

Through the adoption of NDN, next-generation cellular networks can move past the constraints of traditional networking to embrace a data-centric model, optimizing performance, simplifying network management, and enhancing security for future-proofing 5G and beyond. This article first presents qualitative arguments regarding the security, computational, and latency impact of an NDN-based cellular core network. Next, a proof of concept is created using the OpenAirInterface (OAI)[9] 5G core along with a custom-built NDN interest/data processing side car proxy (SCP).[10] The design is implemented and tested to provide a quantitative demonstration of the performance benefits of using NDN.

PRELIMINARIES AND OVERVIEW

Existing 5G core communication model

The 5G core network is built as an SBA where VNFs communicate using representational state transfer (REST) application programming interfaces (APIs). Inter-VNF communication is secured using TLS where certificates are provisioned and managed by an operator-controlled public key infrastructure (PKI) system. To remain vendor-agnostic, interactions between 5G core VNFs are standardized under the Common API Framework (CAPIF).[11] A sample API name is: `/nudr-dr/v2/subscription-data/#imsi/` authentication-data, which is used by the unified data repository (UDR) to provide authentication data regarding a user identity. While this naming convention is not strictly semantic, an expert with sufficient domain knowledge can understand the provided functionality by inspecting the given API name.

Figure 1 illustrates a sample cellular deployment with an overview of the existing 5G network slicing architecture and how it is executed in a distributed cloud hierarchy. In this environment, VNFs can be placed in the edge cloud in proximity to the radio access network (RAN) or the central cloud, depending on operational significance and latency requirements.

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

Furthermore, Figure 1 depicts how the physical deployment is logically represented by the 5G core SBA. In the existing core network, each VNF operates in a dual capacity: offering services as a producer while simultaneously consuming services from other VNFs. The existing provider–consumer communication framework depends on the network repository function (NRF),[8] a centralized metadata database. Every VNF registers its services with the NRF, enabling the network to keep track of available service providers. When a VNF requires a specific service, it contacts the NRF to find an appropriate provider. The NRF then identifies a suitable service provider and informs the requesting VNF, enabling the two VNFs to authenticate and establish either direct or indirect communication. This process is illustrated with an example in Figure 1, where the access and mobility management function (AMF) seeks to discover a suitable session management function (SMF) to create a packet data unit session for the user equipment (UE). Within the 5G core, the AMF is responsible for orchestrating the communication between the UE and the remainder of the control plane VNFs. The SMF and the user plane function are the control and user plane anchors for the data session. Finally, the authentication server function (AUSF), Unified Data Management (UDM), and the UDR coordinate with each other to carry out the 5G authentication and key agreement (AKA).

Named data networking

Communications within the current IP-based network architecture rely on point-to-point connections with end-to-end secured sessions. In the transient microservice-based 5G core, that is built on top of such traditional networks, maintaining session continuity requires relocating extensive connection states, a resource-intensive and disruption-prone process. This often results in operational overheads and increases the risk of failure as networks dynamically scale.

In NDN, each piece of data are uniquely identified by a `Name` rather than by its location. This approach allows NDN to simplify service discovery and routing within the cellular core. When a network function expresses interest in a specific piece of data, it sends out an `Interest` packet. The NDN routing mechanisms then ensure these interest packets find the shortest path to the nearest copy of the data, rather than relying on a centralized broker like the NRF for service discovery.[12] To further support availability and resilience, NDN leverages data redundancy through opportunistic caching at intermediate forwarding nodes. With this approach, the NDN networking model can recover

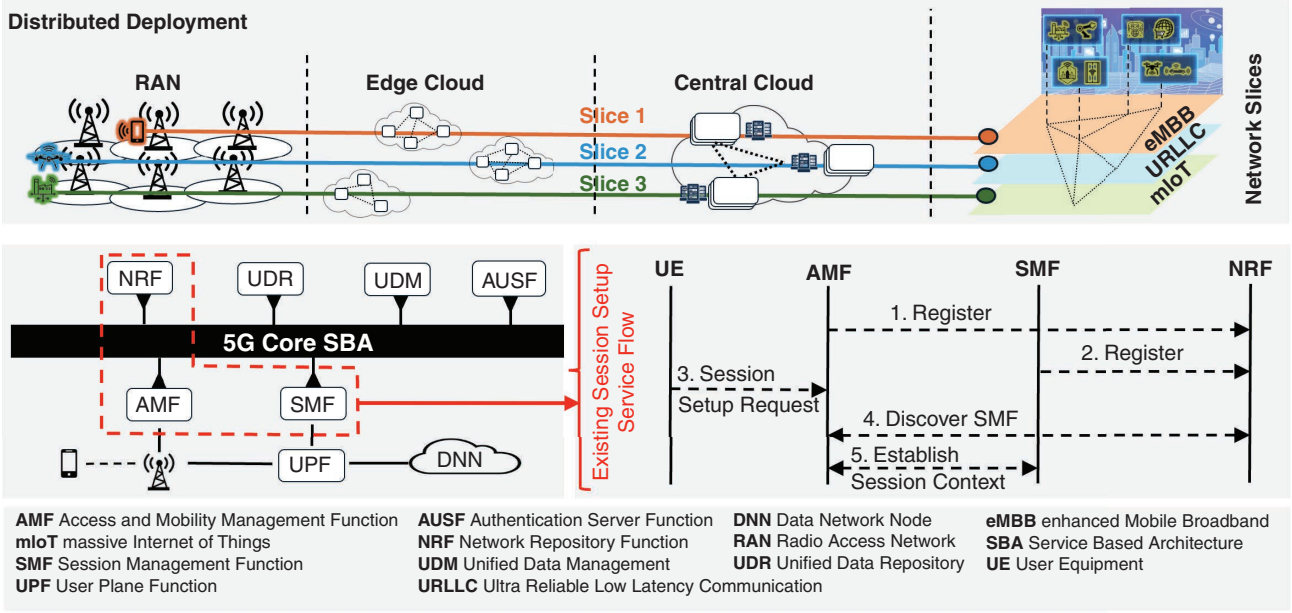

FIGURE 1. 5G network slicing architecture with distributed VNF deployment and core network SBA, highlighting session setup, registration, and discovery processes.

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

from packet losses hop-by-hop, providing much more resilient data delivery between the ends. This redundancy is carefully managed using intelligent cache replacement strategies, preventing excessive resource consumption and unnecessary duplication. This not only eliminates unnecessary signaling overhead associated with managing session states and service lookups but also ensures efficient data retrieval.

Furthermore, each piece of `Data` within the NDN ecosystem is individually signed and authenticatable regardless of the path it takes through the network.[12] By natively integrating these functionalities, NDN provides a streamlined framework for data delivery that inherently reduces the complexity and signaling load typically seen in traditional IP-based network architectures. Thus, transitioning to an NDN model effectively minimizes the need for the frequent signaling overhead associated with the traditional processes of establishing and terminating sessions in a distributed microservice deployment.

Related work

A recent study[13] demonstrates the transition from a host-centric to a data-centric paradigm to enhance the scalability and flexibility of cellular networks through serverless and atomic functional decompositions over distributed infrastructures. This work leverages data-centric mechanisms to seamlessly integrate and interact with services across a fully distributed cellular architecture, optimizing service orchestration and resource utilization. However, the study pays little attention to the security aspect of the system and does not offer any specific design for security and data integrity. Our proposed architecture, on the other hand, integrates NDN to specifically address security and data integrity by embedding security within the data itself. Our work distinctively utilizes the inherent capabilities of NDN to both secure data independently of the transport medium, but also reduce the signaling overhead associated with point-to-point communication. Therefore, the NDN-based cellular architecture not only reduces reliance on traditional security mechanisms but also streamlines data transmission processes.

NAMED-DATA-CENTRIC CELLULAR DEPLOYMENT

Integrating with named data networking

The integration benefits of NDN with cellular networks can be broken down into improvements in both the control and user planes. First, leveraging the semantic nature of the 5G core CAPIF, an NDN-based control plane can be constructed to eliminate the signaling overhead in the existing inter-VNF communication. Second, NDN can be directly used to carry end-user traffic between the RAN and the core user plane. Our integration strategy in this article is exclusively focused on the control plane aspects rather than the user plane.

The difference between the existing host-centric 5G core network communication and the proposed NDN data-centric approach is summarized in Figure 2. In the host-centric approach, two primary shortcomings become evident: 1) the registration of VNFs with the NRF, the signaling required to maintain metadata profiles, the discovery operations;[8] and 2) the constant need to establish secure point-to-point sessions for each interaction. As the number of microservices

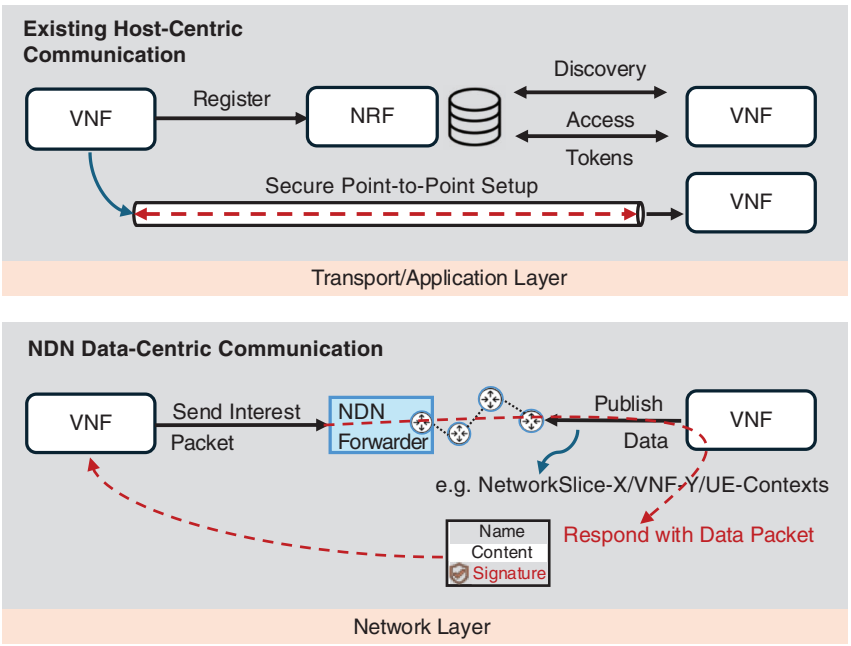

FIGURE 2. Comparing the communication models of the existing 5G core with the proposed NDN-based next-generation cellular network.

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

in the network continues to grow, these limitations lead to significant signaling overhead due to the nature of inter-VNF communication.

Thus, in a cellular network that is becoming increasingly distributed with microservice deployments spread across various locations, the ability to secure data independently of its transmission channel is crucial. With the NDN data-centric model proposed in Figure 2, each VNF can publish its services with a local NDN forwarder at the network layer. At this point, any service consumer VNF can seek to consume services by sending `Interest` packets with a semantic prefix. This `Interest` is propagated to a suitable resource provider through the NDN architecture and a signed `Data` packet is relayed back to the original service consumer with the requested content. Considering the existing API naming convention used in the 5G CAPIF, a fertile foundation already exists to enable the transition to an NDN naming scheme.

Proposed framework

Our proposed design revolves around a Kubernetes-based deployment to create a deployment that is easy to integrate with the existing management and orchestration ecosystem. Given the popularity of Kubernetes, we believe that basing the design around it offers a cloud-native design that is adaptable and showcases the potential of NDN within a modern network architecture. Nevertheless, we acknowledge that the design can evolve to more generalized deployment models as it moves past the initial proof of concept.

The complete system design is given in Figure 3, where each deployment block is depicted within its respective Kubernetes cluster hierarchy, which can be a cluster-, node-, or pod-level deployment. Next, we describe the two fundamental building blocks of our NDN-based cellular core network, which are the 1) Kubernetes-integrated NDN infrastructure and 2) the NDN SCP.

NDN infrastructure. We create an NDN routing domain with our Kubernetes deployment where each node has one NDN forwarder, specifically the NDN forwarding daemon (NFD),[14] that is responsible for managing the routing for pods on a given node. Each node NFD is connected to other NFDs deployed in the cluster. The prefix advertisements are synchronized throughout the cluster using the NDN link state routing (NLSR) protocol.[15] To secure the inter-NFD communication, an automated certificate distribution is built into the deployment, generating and placing the relevant certificates into newly instantiated NFDs.

NDN SCP. In our proof-of-concept design for the NDN-based cellular core architecture, each pod is hosting two containers: 1) the primary 5G core VNF made up of multiple microservices and running an HTTP server conforming to the CAPIF; 2) the NDN SCP, that sits adjacent to each 5G core application to provide an abstraction layer toward the NDN routing domain. In this setup, the NDN SCP is the pod-level interaction

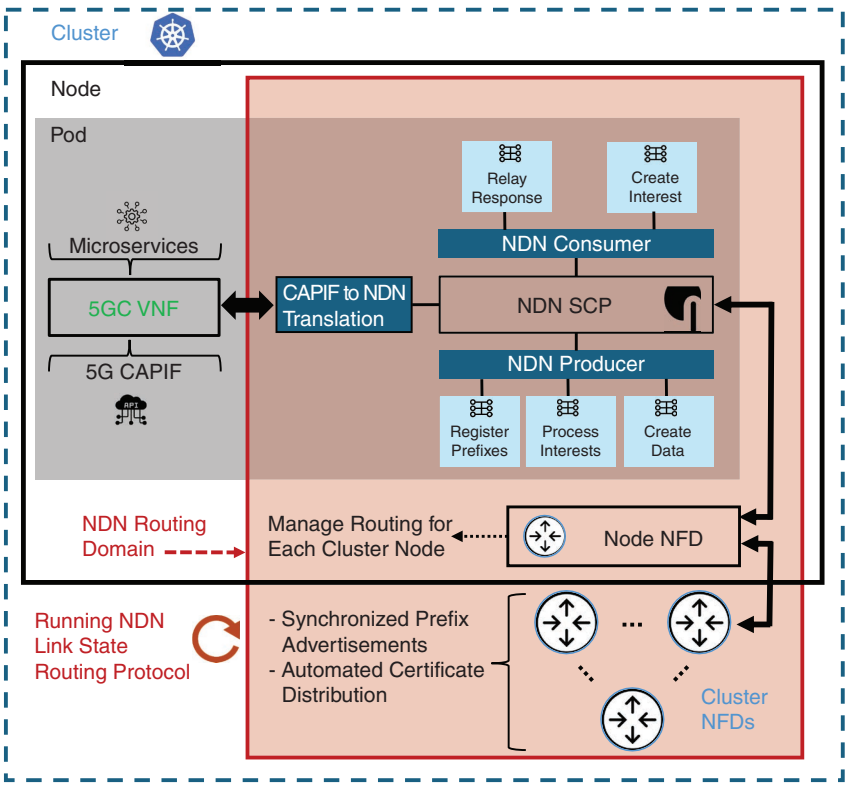

FIGURE 3. NDN-based cellular core integration in a Kubernetes deployment with cluster-, node- and pod-level deployments of NDN and 5G components.

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

point of the 5G core VNF with the NDN routing domain. The SCP has three primary building blocks, each with its submodules. First, the CAPIF to NDN translation unit is the NDN naming convention that is responsible for crafting the interest names for outgoing service consumption requests. In our implementation, this translation leverages the existing semantic nature of the 5G CAPIF[11] to create interest names that are both network slice- and VNF-specific. The NDN naming scheme we use is: `/Domain-Name/Network-Slice-ID/VNF-Type/Service-Name`, which encodes the network architecture into the data names themselves. Each segment of this hierarchy represents a distinct layer of the network, from the public land mobile network to the network slice IDs, all of the way down to specific data identifiers within microservices. This structure supports NDN's ability to directly route requests based on semantic identifiers intrinsic to each data packet. The NDN-CAPIF translation unit uses existing API names such as `/nudr-dr/v2/subscription-data/#imsi/authentication-data`, to construct NDN interests that inherently represent the network architecture, enabling direct and efficient routing without the need for separate service name resolution. This seamless integration highlights the importance of CAPIF's semantic nature, as it provides the necessary descriptors that guide the NDN system in data retrieval and routing decisions, enhancing overall network efficiency and reducing latency. To identify the target resource within a VNF, we directly leverage the CAPIF endpoint API as part of the interest name. These interest names are used by the NDN consumer module to create the actual interest packets. Any response received back from the NDN infrastructure is relayed back to the NDN consumer. Last but not least, the NDN SCP hosts the NDN producer module, which is responsible for registering prefixes with the local node-level NFD. The routing prefixes are used to distinguish service provider VNFs by their VNF type within each network slice.

Our design choice of leveraging the CAPIF in this manner ensures that the NDN augmentation remains vendor-agnostic. As long as vendor implementations conform to CAPIF's standards, the translation from NDN to CAPIF should maintain seamless interoperability, facilitating a unified approach across different vendors' VNFs. This adherence will also promote the practicality of our proposed naming convention-based routing, aligning it with future standards and enhancing its applicability across diverse network ecosystems.

Impact of a named cellular core

Security perspective. Each data packet in NDN carries a cryptographic signature, allowing 5G core network components to independently verify the authenticity and integrity of the data they receive. This removes the need for repeated authentication processes common in traditional session-based models, enhancing communication efficiency and reducing reliance on centralized authorities for verification. In a core network composed of microservices operating in distributed environments, this decentralized security model reduces the attack surface by eliminating dependencies on fixed points that are vulnerable to exploitation, thereby improving overall network resilience.

Beyond data-centric security, NDN introduces a scalable and flexible trust management framework, particularly well-suited for dynamic, multidomain, and multitenant cellular environments.[16] Rather than depending on static, centralized PKI and session-based authentication, NDN employs hierarchical naming and trust schemas that enable transitive trust relationships across domains, tenants, and network slices. This approach allows VNFs to verify data authenticity directly, without the overhead of continuous session setup or complex certificate reconfiguration, supporting seamless and secure interactions in rapidly evolving network environments.

Computation perspective. In the existing 5G core SBA, data need to travel large distances between different VNFs across multiple layers. With the adoption of NDN, the data are cached at various locations throughout the network. This enables the processing to occur at more optimal locations by reducing the distance that data need to travel. Thus, in a cellular network architecture that is built around NDN principles, the approach to data and computation can be significantly enhanced by strategically positioning data closer to where it needs to be processed.

Furthermore, such an approach aligns well with the direction of mobile edge computing (MEC), where computational tasks are increasingly handled at the edge of the network rather than being centralized.[17] In the case of a distributed, microservice-based deployment such as a cellular network, NDN will allow data and computation to move fluidly between edge nodes and core VNFs. This not

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

only reduces latency but also optimizes resource utilization across the network. Consequently, this approach can lower the demand for centralized data centers, fostering a more scalable and robust network architecture.

Latency perspective. The NDN data-centric approach to cellular network design simplifies the security model by avoiding repetitive authentication and authorization for every communication session and eliminates the signaling overhead associated with registration and discovery in the cellular core. While specific enhancements like advanced caching mechanisms in the traditional 5G core can reduce discovery-related NRF queries, it is crucial to recognize their limitations compared to a data-centric model like NDN. NDN integrates caching and enhances security through cryptographic signatures on each data packet, allowing for independent verification without session-based checks. This is particularly advantageous in dynamically orchestrated microservices architectures.

The fundamental difference between a traditional network slice and an NDN-based network slice is illustrated in Figure 4. In the traditional setup, VNFs are linked through point-to-point security, typical of IP-based communications. This arrangement features direct connections and session-based security between network functions. In contrast, the NDN-based slice features a mesh-like structure where VNFs are interconnected using NDN protocols, with security managed through named secure data packets. This method facilitates direct data routing based on names, enhancing the network's adaptability and inherent security. The diagram highlights microservices within the NDN slice and illustrates how new VNFs can dynamically enter the network, showcasing NDN's flexibility and ease in integrating new services.

Given the transient nature of network slice service chains, this results in two performance improvements: First, the overall process completion time for service chain interactions is reduced; second, when new VNFs are instantiated and seek to join a service chain, they can do so without the need for discovery and added access token acquisition. The operational difference between these two models is summarized in Figure 4. Thus, an NDN-based data-centric cellular core can provide high reliability for latency-sensitive use cases with shorter service interruptions.

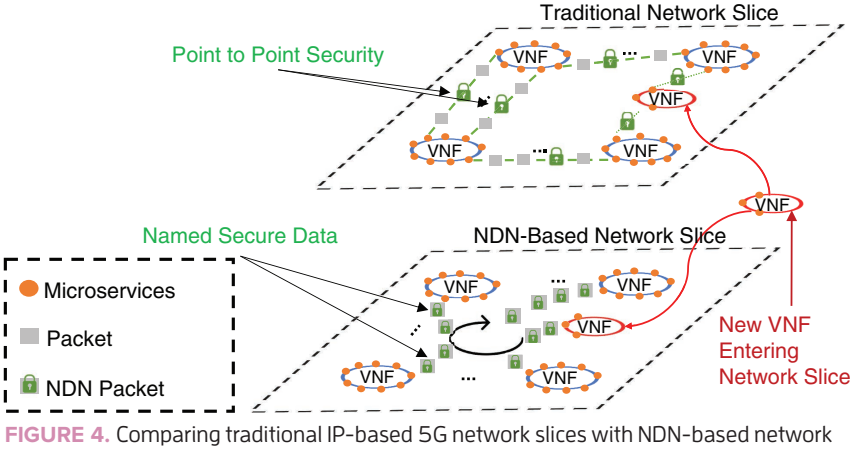

FIGURE 4. Comparing traditional IP-based 5G network slices with NDN-based network slices.

EVALUATION AND ASSESSMENT

To evaluate the latency impact of the proposed NDN-based cellular core network, we use a 5G core testbed that is deployed in the AWS public cloud. As our 5G core solution, we use the OAI 5G core[9] together with the gNBSIM entity[18] to measure the process completion time of inter-VNF service chains such as the 5G-AKA and data session setup. The deployment is deployed within the Northern Virginia AWS Availability Zone (AZ). Our self-managed Kubernetes cluster is deployed across two `t3.xlarge` EC2 instances, each equipped with four vCPUs and 16 GB of RAM.

To understand the latency benefits of adopting an NDN-based cellular core, we compare our framework in Figure 3, with the traditional 5G core. We customize the existing 5G core signaling with additional proxy augmentations to include discovery operations among all of the VNFs to fully illustrate the impact of repeated discovery. Our primary metric is the process completion time for the 5G-AKA and session setup service chains. The key difference between the NDN-based approach and the traditional operation mode is illustrated in Figure 2. In the existing 5G core, before initiating service chain signaling, the VNFs need to register and discover each other. With the NDN-based cellular architecture, this overhead is eliminated.

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

Figure 5 shows there is an overhead of more than 6–7 ms for session setup. For highly ephemeral network slices where VNFs frequently exit/enter service chains, this amount of overhead can cause service disruptions for latency-critical use cases. Furthermore, the centralized design of the service server/client model results in excessive inter-VNF and VNF-NRF signaling to establish and maintain communications. As a result, the centralized NRF is subject to massive control plane traffic. The adoption of the NDN-based cellular core addresses not only the discovery latency overhead but also the VNF-NRF signaling overhead that can lead to congestion.

CHALLENGES AND FUTURE DIRECTIONS

Interoperability with legacy systems

To facilitate a smooth transition toward NDN-based cellular deployments, establishing initial interoperability with existing 5G infrastructure is essential. While maintaining compatibility with current systems, the development of a robust, standardized NDN framework tailored to 6G will be key to driving widespread adoption. However, it is practically not possible to discard the existing infrastructure that is already supporting cellular communication. In our existing deployment, the NDN routing domain is built as an overlay on top of the existing IP network infrastructure. Instead of immediately replacing IP networks, NDN can initially coexist as an overlay, similar to how IP itself was adopted. As more applications begin to run over NDN and its benefits become clearer, the reliance on IP-based underlays could naturally diminish over time. Thus, the shift to NDN needs to be incremental, reducing the need for immediate, large-scale infrastructure changes. To ensure a seamless migration, we propose gradual integration strategies, such as dual-stack operations where NDN and IP protocols operate concurrently, allowing for phased traffic migration and interoperability testing between old and new systems. This approach will help mitigate operational risks and technical barriers during the transition phase. Nevertheless, deploying NDN-capable routers, redesigning core and edge network functions, and incorporating new management tools will be beneficial for long-term success. Addressing these challenges will require collaboration between academia, industry, and standardization bodies to develop scalable, cost-effective solutions that support the unique demands of NDN in a cellular context.

NDN for 6G and beyond

As 6G evolves, several emerging paradigms, including AI-driven networking, ubiquitous computing, and trust-based communications, necessitate a shift beyond traditional IP-based models. NDN's data-centric architecture aligns naturally with these trends by providing built-in security, in-network caching for localized decision-making, and name-based routing that supports dynamic, distributed service models. These capabilities make NDN a strong candidate for enabling future 6G architectures, particularly in scenarios requiring edge-intelligent processing, multidomain trust, and scalable content distribution.

In this article, we presented a novel design for the next-generation cellular architecture by leveraging NDN as a foundation. Compared with traditional IP-based infrastructure that uses session-based communication with point-to-point connections, our proposed NDN-based design embraces a data-centric model to provide built-in support for a more flexible, secure, and efficient cellular architecture.

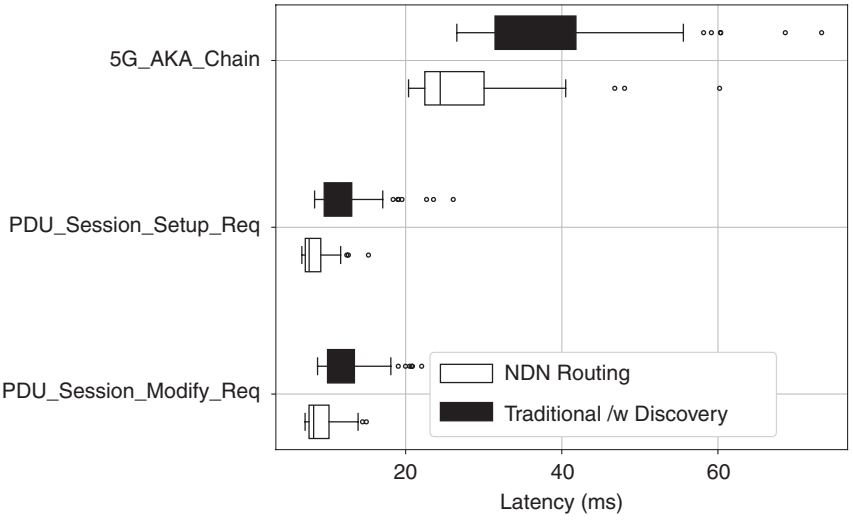

FIGURE 5. Comparing the process completion time of 5G-AKA and session setup service chains across the NDN-based cellular core and traditional discovery-based 5G core.

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

ABOUT THE AUTHORS

TOLGA O. ATALAY is a senior research and development engineer at A2 Labs, Arlington, VA 22203 USA. His research interests include cellular networks, cloud computing, and system security. Atalay received his Ph.D. in computer engineering from Virginia Tech. Contact him at tatalay@a2labs.com.

ANGELOS STAVROU is a professor with the Department of Electrical and Computer Engineering at Virginia Tech, Blacksburg, VA 24061 USA, and the founder of A2 Labs, Arlington, VA 22203 USA. His research interests include large systems security and survivability, intrusion detection systems, privacy and anonymity, and security for MANETs and mobile devices. Stavrou received his Ph.D. in computer science from Columbia University. He is a Senior Member of IEEE. Contact him at angelos@vt.edu.

LIXIA ZHANG is a professor of computer science at the University of California, Los Angeles, Los Angeles, CA 90095 USA. Her research interests include network architecture and protocol designs, as well as the development of large-scale, secure, and resilient systems. Zhang received her Ph.D. in computer science from the Massachusetts Institute of Technology. She is a Life Fellow of IEEE and ACM. Contact her at lixia@cs.ucla.edu.

As an initial proof-of-concept, we create an integrated deployment of the existing 5G core by designing an abstraction layer that provides seamless interactions with the NDN routing domain. We conduct evaluations in the AWS public cloud to demonstrate that our proposed approach eliminates the signaling overhead associated with VNF-NRF discovery operations and reduces the process completion time of 5G core service chains by up to 15 ms. In the future, we plan to extend our proof of concept to more complex real-world scenarios with heterogeneous network conditions. This includes expanding beyond control plane experimentation to explore NDN integration in the user plane, assessing its impact on end-to-end performance and user experience—both critical for a fully integrated NDN-based cellular architecture.

REFERENCES

1. S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, 2019, doi: 10.1109/MWC.2019.1800234.
2. "Network domain security (NDS); IP network layer security," TSG Service and Syst. Aspects (SA), 3rd Generation Partnership Project (3GPP), TS 33.210 V18.1.0, Jun. 2024.
3. D. Soldani et al., "eBPF: A new approach to cloud-native observability, networking and security for current (5G) and future mobile networks (6G and beyond)," *IEEE Access*, vol. 11, pp. 57,174–57,202, 2023, doi: 10.1109/ACCESS.2023.3281480.
4. 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 *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Piscataway, NJ, USA: IEEE Press, 2024, pp. 2308–2317, doi: 10.1109/INFOCOM52122.2024.10621131.
5. T. O. Atalay, S. Maitra, D. Stojadinovic, A. Stavrou, and H. Wang, "Securing 5G OpenRAN with a scalable authorization framework for xApps," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Piscataway, NJ, USA: IEEE Press, 2023, pp. 1–10, doi: 10.1109/INFOCOM53939.2023.10228961.
6. J. Larrea, A. E. Ferguson, and M. K. Marina, "CoreKube: An efficient, autoscaling and resilient mobile core system," in *Proc. 29th Annu. Int. Conf. Mobile Comput. Netw.*, 2023, pp. 1–15.
7. L. Zhang et al., "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, 2014, doi: 10.1145/2656877.2656887.
8. "Network function repository services; Stage 3," T. S. G. C. Network and Terminals, 3rd Generation Partnership Project (3GPP), TS 29.510 V19.0.0, Sep. 2024.
9. "5G software alliance for democratising wireless innovation." OpenAirInterface, Sep. 2024. Accessed: May 22, 2025. [Online]. Available: https://openairinterface.org/
10. 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 *Proc. 21st ACM*

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.

Workshop Hot Topics Netw., 2022, pp. 221–227.
11. "System architecture for the 5G system (5GS); Stage 2," TSG Service and Syst. Aspects (SA), 3rd Generation Partnership Project (3GPP), TS 23.501 V19.0.0, Jun. 2024.
12. Z. Zhang et al., "An overview of security support in named data networking," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 62–68, Nov. 2018, doi: 10.1109/MCOM.2018.1701147.
13. G. Baldoni, J. Quevedo, C. Guimarães, A. de la Oliva, and A. Corsaro, "Data-centric service-based architecture for edge-native 6G network," *IEEE Commun. Mag.*, vol. 62, no. 4, pp. 32–38, Apr. 2024.
14. "Named-data/NFD: Named data networking forwarding Daemon." GitHub, Sep. 2024. Accessed: May 22, 2025. [Online]. Available: https://github.com/named-data/NFD
15. A. K. M. Mahmudul Hoque, S. O. Amin, A. Alyyan, B. Zhang, L. Zhang, and L. Wang, "NLSR: Named-data link state routing protocol," in *Proc. 3rd ACM SIGCOMM Workshop Inf.-Centric Netw.*, 2013, pp. 15–20.
16. T. O. Atalay, T. Yu, L. Zhang, and A. Stavrou, "Towards establishing a systematic security framework for next generation cellular networks," in *Proc. Workshop Secur. Privacy Next-Gener. Netw. (FutureG)*, Feb. 2025.
17. A. Mtibaa, R. Tourani, S. Misra, J. Burke, and L. Zhang, "Towards edge computing over named data networking," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Piscataway, NJ, USA: IEEE Press, 2018, pp. 117–120, doi: 10.1109/EDGE.2018.00023.
18. "omec-project/gnbsim: gNB simulator." GitHub, Oct. 2024. Accessed: May 22, 2025. [Online]. Available: https://github.com/omec-project/gnbsim

Unlock Your Potential

WORLD-CLASS CONFERENCES — Over 195 globally recognized conferences.

DIGITAL LIBRARY — Over 900k articles covering world-class peer-reviewed content.

CALLS FOR PAPERS — Write and present your ground-breaking accomplishments.

EDUCATION — Strengthen your resume with the IEEE Computer Society Course Catalog.

ADVANCE YOUR CAREER — Search new positions in the IEEE Computer Society Jobs Board.

NETWORK — Make connections in local Region, Section, and Chapter activities.

Explore membership today at the IEEE Computer Society
www.computer.org

IEEE COMPUTER SOCIETY

IEEE

Digital Object Identifier 10.1109/MC.2025.3583803

Authorized licensed use limited to: BEIJING INSTITUTE OF TECHNOLOGY. Downloaded on November 06,2025 at 07:43:16 UTC from IEEE Xplore. Restrictions apply.