NAMED DATA NETWORKING COMMUNITY MEETING

TrustNG: A Framework for Migrating Cloud-Native 5G Cores to Zero-Trust Using Named Data Networking

NDN Community Meeting Presentation – Spring 2026

Amirreza Ghafoori
Tianyuan Yu
Tolga O. Atalay
Alireza Famili
Angelos Stavrou
Lixia Zhang

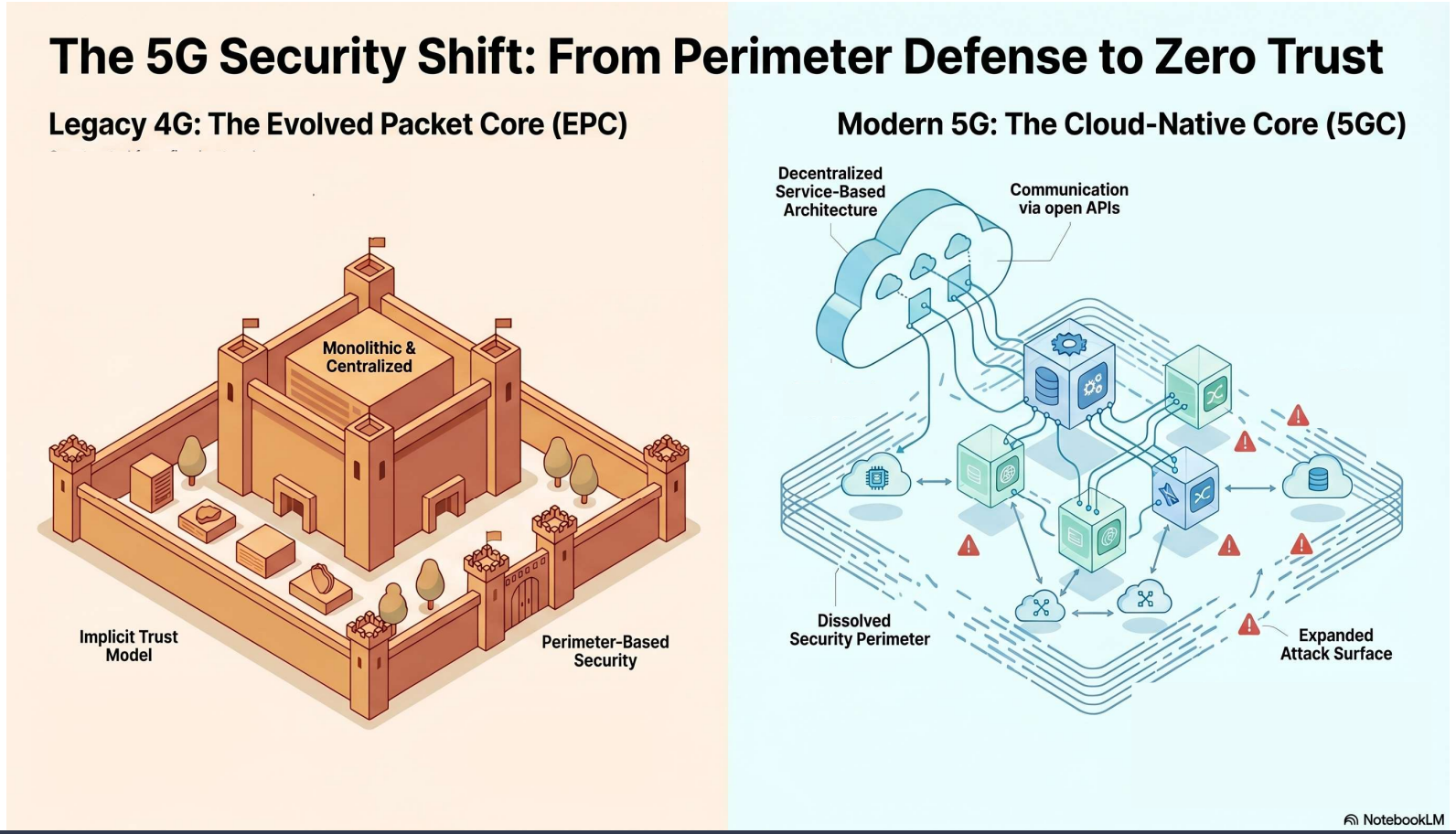
UCLA VIRGINIA TECH

Outline

1. Introduction & Motivation
2. Background
3. TrustNG Design
4. Security Analylsis
5. Performance Evaluation
6. Discussion & Research PATH

Introduction
&
Motivation

Mobile Network Evolution



Mobile Network Evolution

4G / EPC

- Monolithic network elements
- Tightly managed operator environment
- Security relied on **clear network boundaries**
- Internal components were often **implicitly trusted**

5G Core

- Service-Based Architecture (SBA)
- Network functions become containerized microservices
- Communication through HTTP-based APIs
- Deployment across cloud, edge, and multiple domains

Why Current 5G Security Is Not Enough

- mTLS for mutual authentication
- OAuth2/tokens for authorization
- Network Function IDs for service identity
- Kubernetes/service-mesh policies for workload control

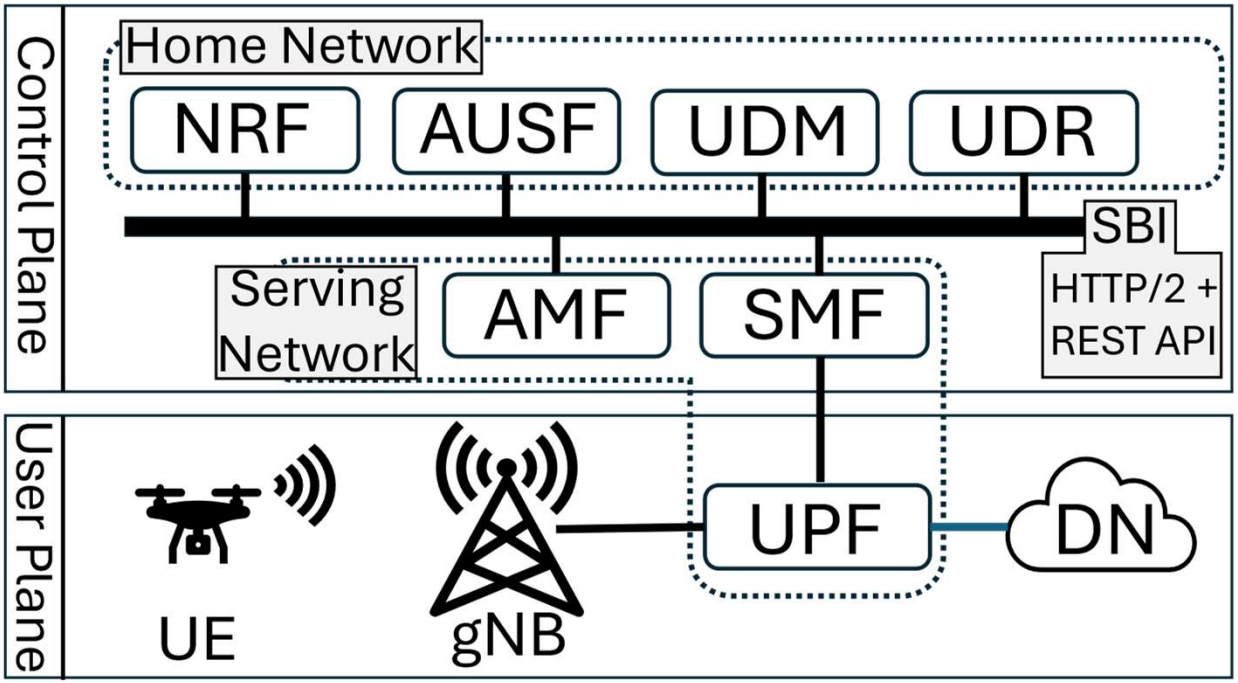
Subject: CN: amf.operator.com
Issuer: operator-root-CA

nfInstanceId: 2f7d8e13-bf1e-48c7
nfType: AMF
services: [namf-comm]

{"iss": "nrf.operator.com",
"sub": "nfInstanceId:2f7d8e13",
"aud": "smf",
"scope": "nsmf-pdusession",
"exp": 1712023123}

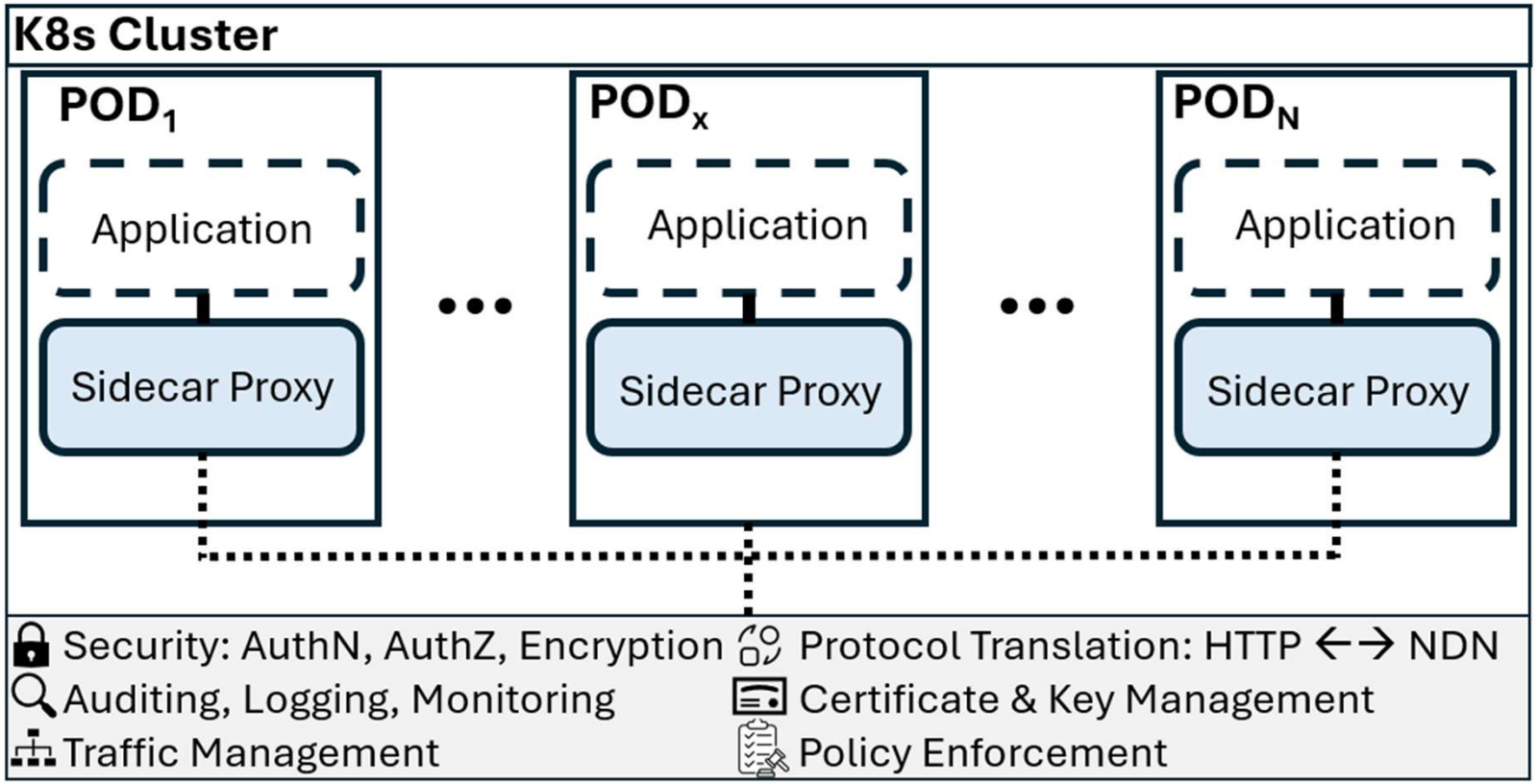
Background

5G Core – Service Based Architecture

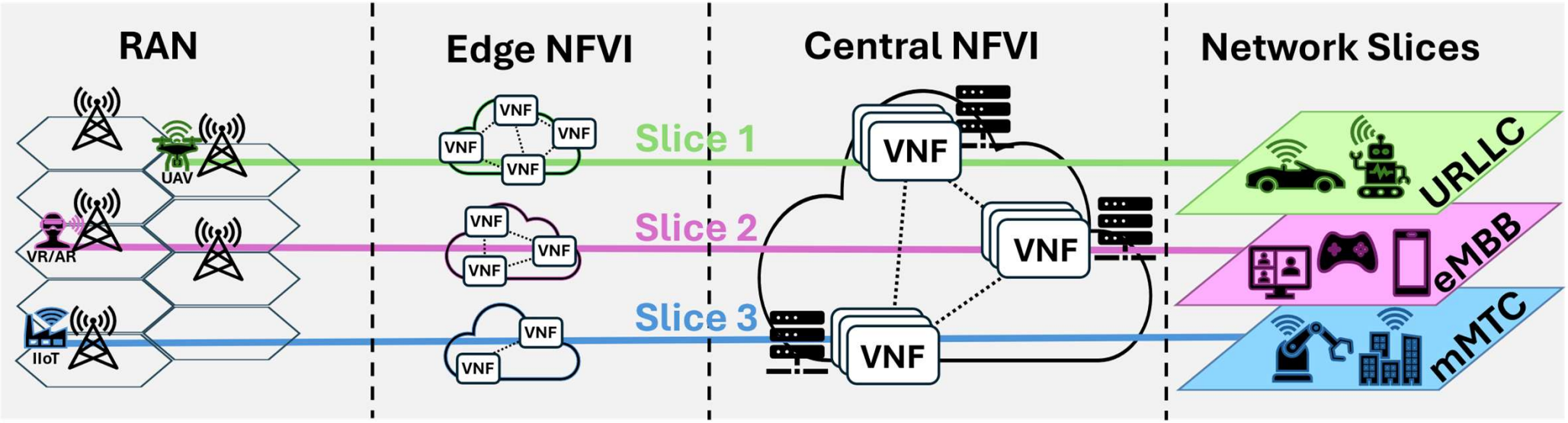


AMF- Access and Mobility Management Function
SMF- Session Management Function
UPF- User Plane Function
AUSF: Authentication Server Function
UDM-Unified Data Management
UDR-Unified Data Repository
NRF- Network Repository Function

Service Mesh



Network Slices



UAV Unmanned Aerial Vehicle
VR/AR Virtual/Augmented Reality
IIoT Industrial Internet of Things
RAN Radio Access Network

NFVI Network Function Virtualization Infrastructure
VNF Virtualized Network Function

URLLC Ultra Reliable Low Latency Communication
eMBB enhanced Mobile Broad Band
mMTC massive Machine Type Communication

Zero-Trust & AAA

Main Zero Trust Principles

- Never trust, always verify
- Assume breach
- Least privilege access

3 Aus (The gold standard of Security)

- Authentication
- Authorization
- Auditing

Named Data Networking - Data-Centric Security

NDN secures the data itself, not the channel that carries it.

From channel security to data security

Consumers request data, not host addresses

Data may arrive from the producer, a cache, or any path

Correctness does not depend on trusting the forwarding path

Every Data packet carries a **signature binding name + content**

Keys, certificates, trust anchors, and trust schemas are all **named Data** too

Why this matters for Zero Trust

The path, cache, or peer can be **untrusted** - the received object is still verifiable

Each Data is an **independent unit of authentication**

No reliance on TLS session termination or **bearer tokens**

Receiver verifies **what arrived**, not **who relayed it**

Trust becomes a property of the object, not of the connection

Takeaway: NDN starts from secured data, not secured channels - the architectural shift that makes Zero Trust natural.

NDN Maps Naturally to the Zero Trust Principles

Zero Trust requires continuous verification of every security-relevant object - exactly what NDN already does.

Zero Trust principle	NDN mechanism	Security effect
Never trust, always verify	Every Data object is **signed**; enabling receivers to verify **every** piece of received data	No implicit trust in path, cache, session, or endpoint address.
Assume breach	Verification of every object defends against any potential malicious parties	A compromised path does **not** compromise Data authenticity.
Least privilege access	Minimize the privilege of every crypto key via trust schema, which defines which key names may sign which data names.	Authority is bound to a **name prefix** - scoped to **/slice/vnf/service/action** granularity.

Per-packet signatures + trust schema = continuous authentication and authorization at the data layer.

Never Trust, Always Verify - Continuous Authentication

In NDN, every received Data is independently verified through a name-based chain - no sessions, no bearer tokens.

Chain of verifiable named objects

Data packet	`/slice/amf/service/profile`
KeyLocator	`-> signer key: /slice/amf/KEY/k1`
Certificate chain	`/slice/amf/KEY -> /domain/KEY`
Trust anchor	`/domain/KEY/self-signed (root of trust)`

Authentication logic at every exchange

1. **Verify the Data signature**
   Bound to name + content; tamper-evident.
2. **Fetch the signer key by name**
   Keys and certificates are themselves named Data.
3. **Recursively verify the certificate chain**
   Terminates at the domain trust anchor.
4. **Repeat for every received object**
   Continuous verification is a property of the architecture, not an add-on.

Zero Trust angle: each Data object proves its own provenance - no implicit trust in TLS sessions, tokens, or peer endpoint.

Least Privilege & Assume Breach - Trust Schema over Names

Authority is expressed as name-based rules - not flat roles or bearer tokens - and checked on every Interest and Data.

Trust schema = name-based authorization

Authorization is expressed as a rule:

data-name pattern ➡ allowed key-name pattern

/slice/amf/<service> signed only by **/slice/amf/KEY/<id>**

/sliceA/upf/<action> signed only by **/sliceA/upf/KEY/<id>**

Authority is scoped to a name prefix - not to a flat role or bearer token.

What this gives us

Least privilege

Each entity holds authority only inside its assigned namespace - nothing wider.

Assume breach

A compromised entity can forge data only inside its own scope; cross-namespace requests fail the schema check.

Continuous authorization

Every Interest and Data is checked against schema rules - no session-level decision to bypass.

TrustNG builds on this: a unified, name-bound Zero-Trust substrate for the cloud-native 5G core.

Research Gap
&
Thesis

Research Gap & Thesis

Research Gap

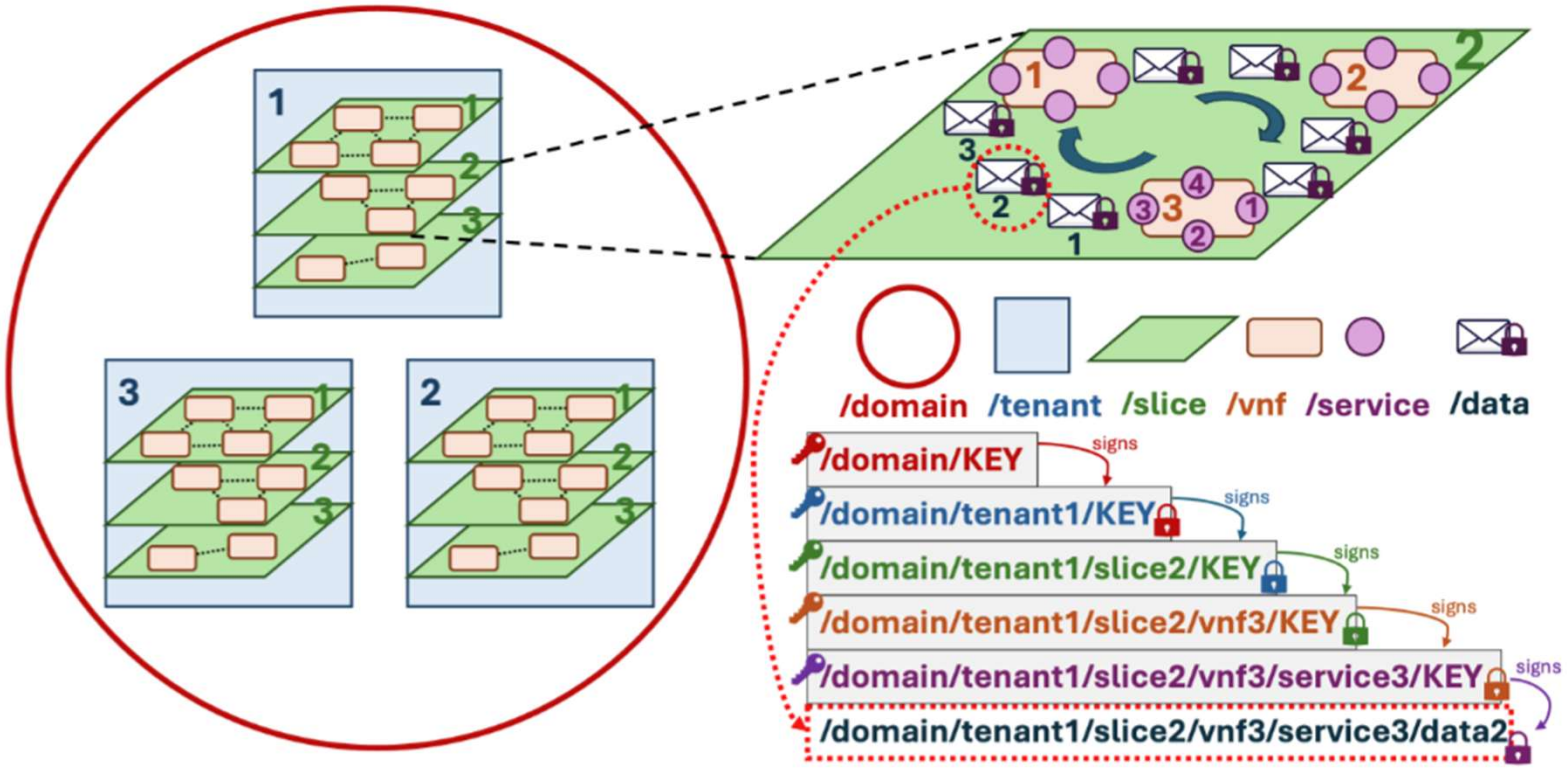
- Trust is still realized through **separate mechanisms and identities**
- Security remains **session/token-centric**
- There is no **unified trust substrate** for cloud-native 5G cores

Thesis

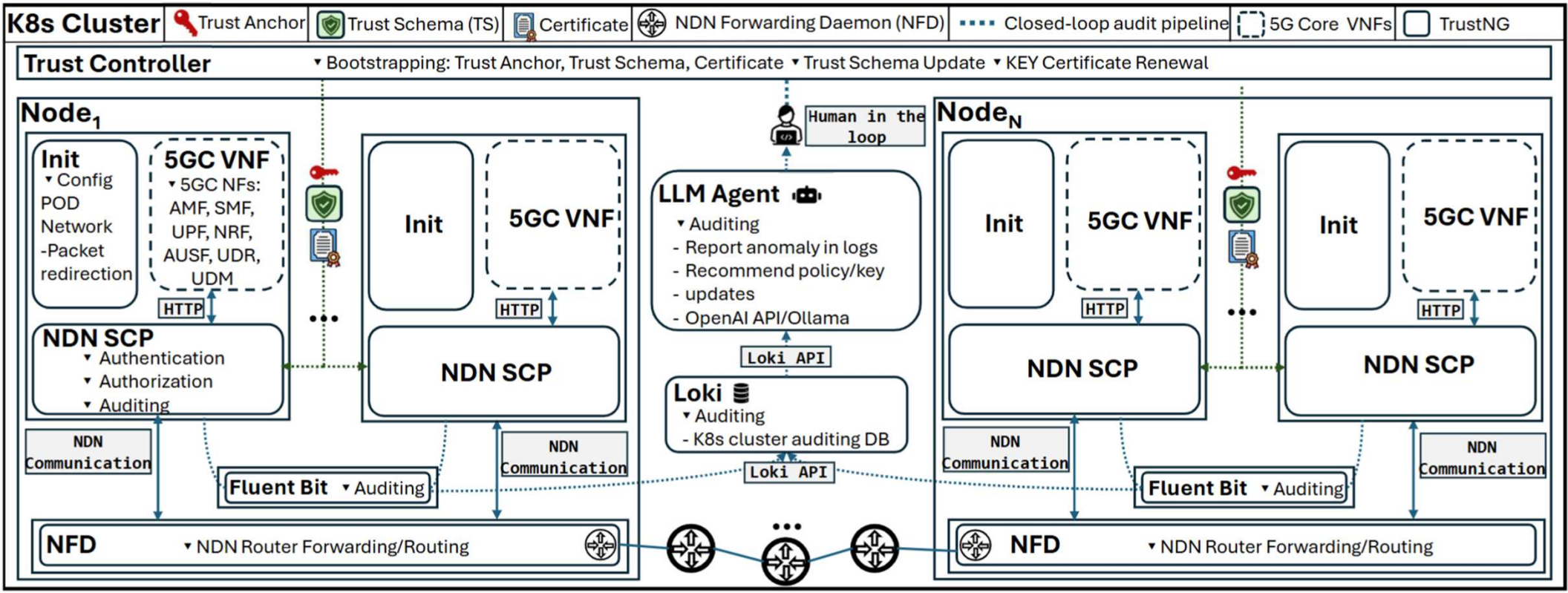
- **NDN can serve as a structural trust substrate for cloud-native 5G cores**
- It can unify **identity, authentication, authorization, and auditing**
- This enables a more native realization of **zero trust** in the 5G core

TrustNG Design

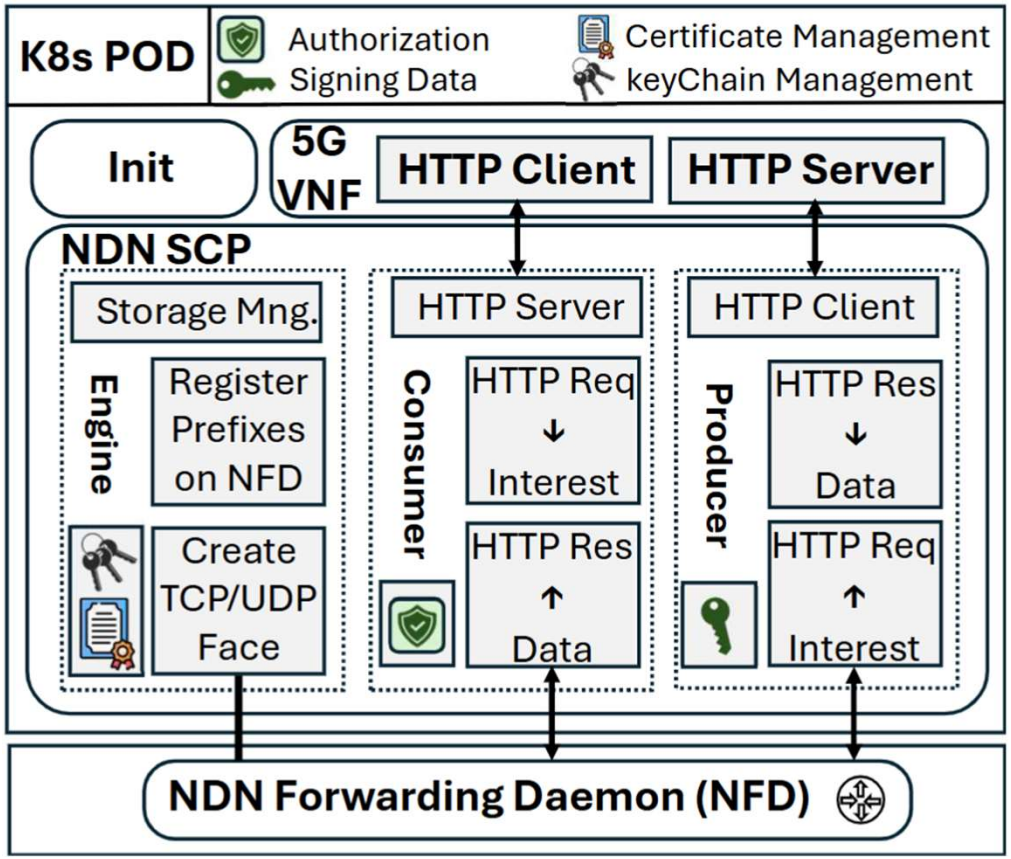
Hierarch Naming & Trust Relations



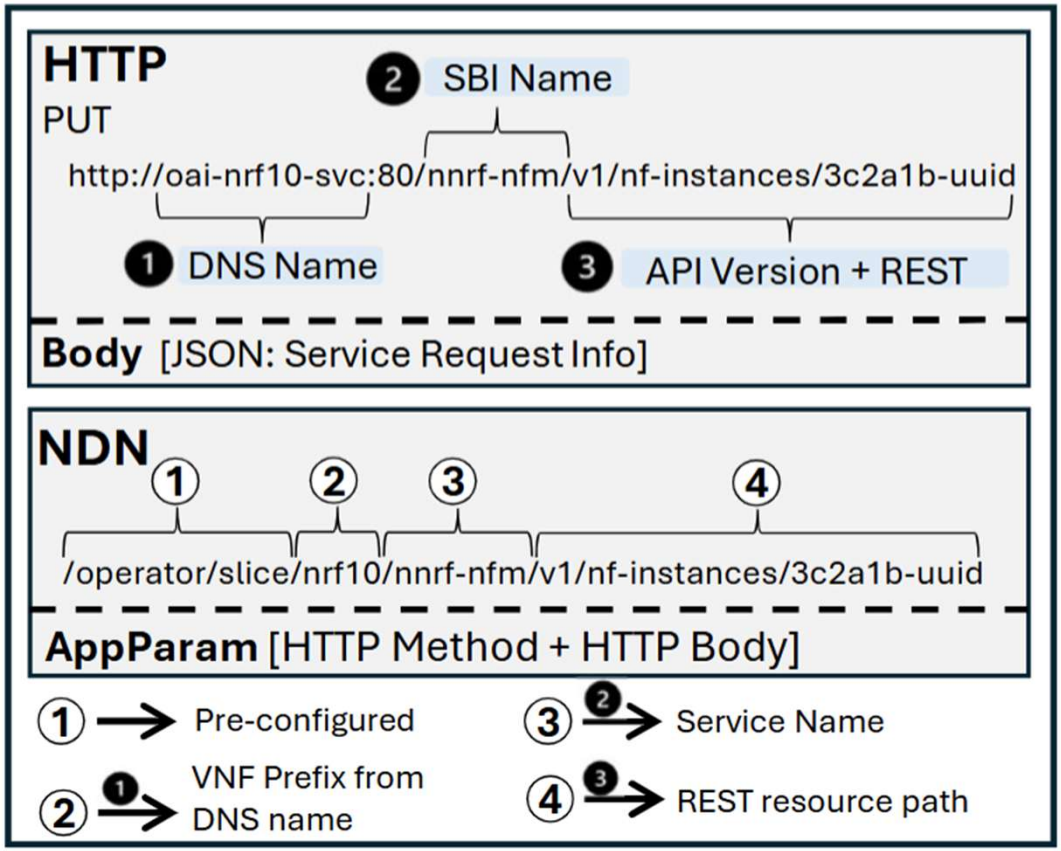
TrustNG Overview



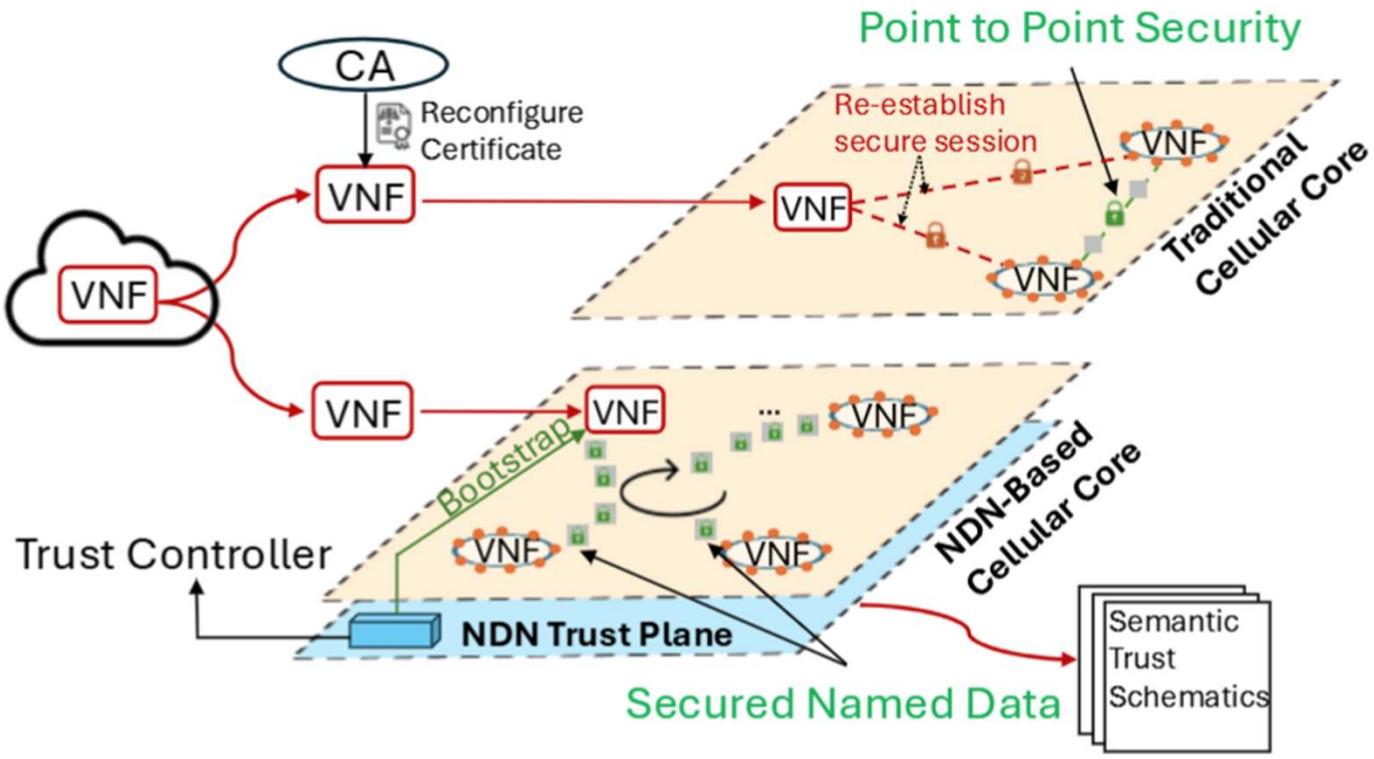
NDN-SCP Sidecar Architecture



HTTP-to-NDN Translation



Architectural Comparison with IP-Based 5G



End-to-End Workflow

1. Consumer VNF sends a normal **HTTP request**
2. Consumer **NDN-SCP** intercepts the request and translates it into a **signed Interest**
3. The Interest is forwarded through the **NDN overlay**
4. Producer **NDN-SCP** verifies the signature and checks **trust-schema authorization**
5. The request is delivered to the producer VNF as a normal **HTTP request**
6. Producer response is converted into **signed Data** and returned through NDN
7. Consumer **NDN-SCP** verifies the Data and reconstructs the **HTTP response**

Security Analysis

Security Analysis – Threat Model

- TrustNG operates in a **cloud-native 5G core** deployed on Kubernetes
- Following **zero trust**, no component or network segment is implicitly trusted
- Attacker may **compromise or deploy a pod** inside the cluster
- Attacker may **generate arbitrary requests, inject/observe packets, replay messages, and attempt unauthorized access**
- Attacker **cannot compromise the root trust anchor** or break the underlying cryptography

Security Analysis – Threat Model

Trusted components

- Trust anchor
- NDN-SCP sidecars
- Cryptographic primitives and certificate validation

Security Analysis – Representative Attacks & Defenses

Attack	Primary Defense Mechanism	Protection	Audit
Producer impersonation	Name–key binding and trust-schema validation ensure that only authorized VNFs can produce specific named data.	●	✓
Data tampering in transit	Each NDN Data packet carries a cryptographic signature verified by the consumer sidecar.	●	✓
Unauthorized cross-VNF access	Trust-schema authorization restricts which VNFs may access particular namespaces.	●	✓
Replay attacks	Versioned naming and freshness constraints prevent acceptance of stale responses.	●	✓
Unsolicited data injection	NDN forwarding requires a matching Interest entry in the Pending Interest Table.	●	✗
Cache poisoning	Consumers verify signatures on cached content before acceptance.	●	✓
Interest flooding	Detection based on abnormal Interest request patterns and unresolved Interest ratios.	◐	✓
Namespace information leakage	Semantic packet names may reveal service relationships.	◐	✗
Prefix hijacking via routing manipulation	Signed routing announcements prevent unauthorized prefix advertisements.	●	✓

Security Analysis – Auditing Report

```
{ "threat_level": "<low | medium | high>",
"attack_type": "<detected attack class>",
"affected_service": "<target NF service>",
"source_nf": "<requesting NF identity>",
"observation": "<detected anomaly description>",
"recommended_action": "<mitigation guidance>" }
```

Performance Evaluation

Performance Evaluation – Experimental Setup

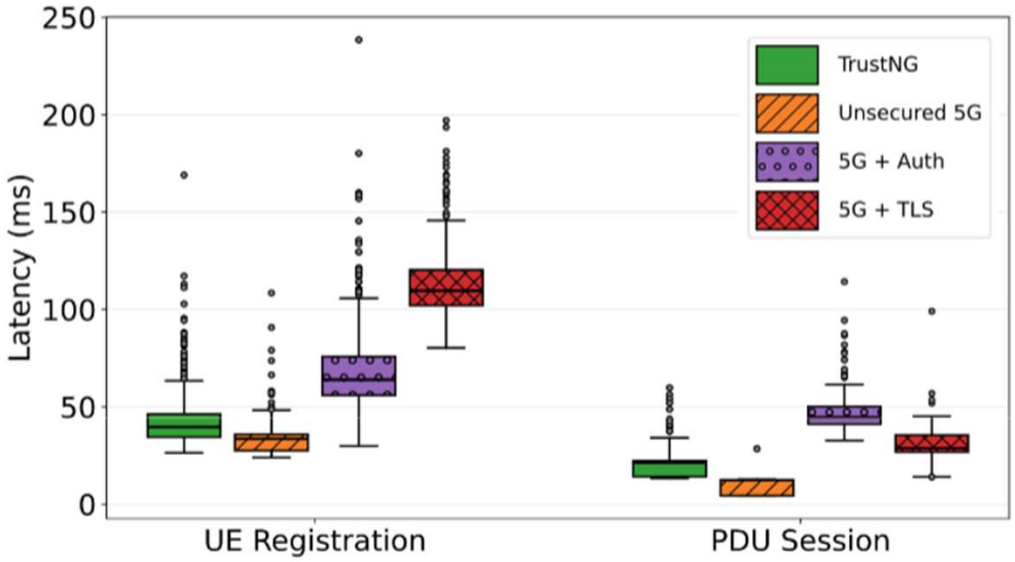
Setups

- Unsecured 5G — HTTP over TCP, no authentication
- 5G + TLS — mutual TLS-protected service communication
- 5G + Auth — token-based authorization
- TrustNG — HTTP translated into signed NDN Interest/Data communication

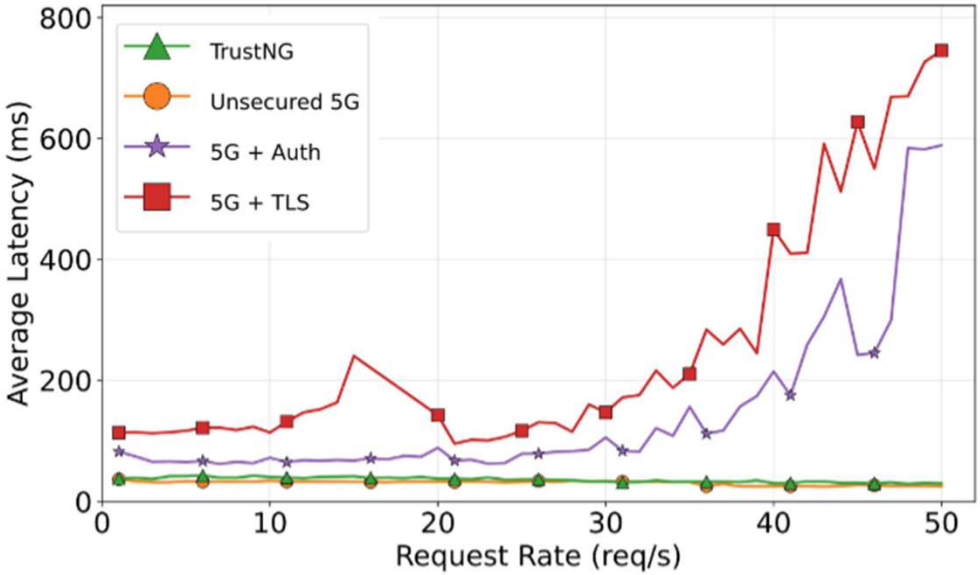
Test Scenarios

- Steady load — 5 req/s for 300 s
- Rate ramping — 1 to 50 req/s
- Burst load — 5, 10, 25, and 50 req/s

Performance Evaluation - Latency

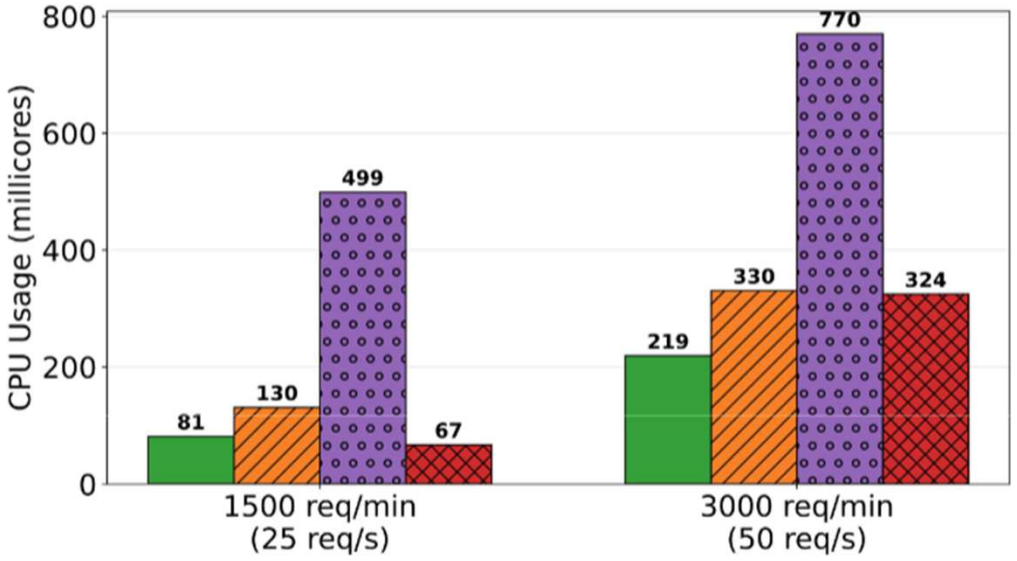


(a) Steady-load latency

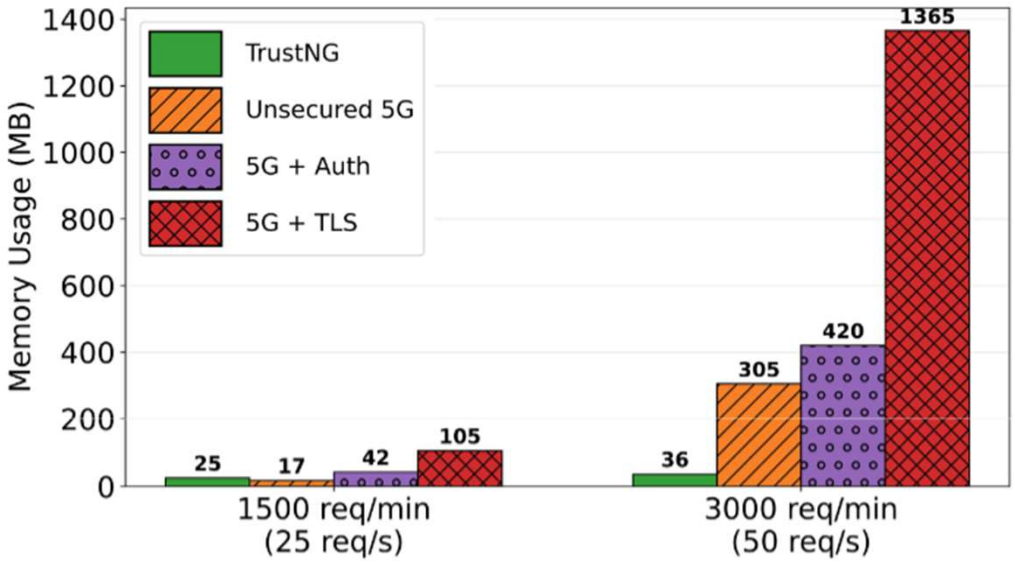


(b) Rate-ramping latency

Performance Evaluation – Resource Utilization



(a) CPU utilization



(b) Memory utilization

Discussion

Discussion – Key Takeaways

- 5G and FutureG need to become Zero-Trust
- Current 5G security remains fragmented across layers
- TrustNG uses NDN as a systematic Zero-Trust realization for 5GC
- Evaluation shows stronger security with low latency/resource overhead
- Some challenges remain, such as deployment complexity and namespace/privacy considerations
- What's next? From 5G core zero trust to end-to-end mobile zero trust

Research PATH

P — Problem

- Fragmented trust in cloud-native 5G cores

A — Approach

- NDN-based unified trust model through TrustNG

T — Trajectory

- From 5G core zero trust to end-to-end mobile zero trust

H — Horizon

- A data-centric trust plane for next-generation networks

Thank you!

Questions?