A Multi-Layered Zero Trust Microsegmentation Solution for Cloud-Native 5G & Beyond Networks

Chafika Benzaïd*, Nawal Guerd‡, Nour El Houda Rehouma‡, Khaled Zeraoulia‡, and Tarik Taleb§
*University of Oulu, Oulu, Finland
‡University of Sciences and Technology Houari Boumediene, Algiers, Algeria
§Ruhr University Bochum, Bochum, Germany
Emails: chafika.benzaid@oulu.fi, {nawal.guerd, nourelhouda.rehouma}@etu.usthb.dz, kzeraoulia@usthb.dz, tarik.taleb@rub.de

***Abstract*—Zero Trust (ZT) is poised as a promising paradigm to effectively deal with the envisioned security risks of cloud-native 5G and beyond (B5G) architectures. However, integrating a ZT security model into B5G is still in its nascent stages, with most proposals remaining largely theoretical or limited to a single domain. This paper presents THAALOUB, a novel ZT framework that empowers 3GPP-compliant, end-to-end ZT security in cloud-native B5G networks. The framework leverages the advanced security features of Service Mesh and Container Network Interface (CNI) technologies to enable a multi-layered ZT microsegmentation security model. Moreover, it adopts an intent-based access control approach to foster proactive ZT security management. The experimental results show THAALOUB's high effectiveness in enhancing B5G security stance with minimal impact on latency and resource usage.**

***Index Terms*—B5G, Cloud-Native, Zero Trust, Microsegmentation, and Service Mesh.**

I. Introduction

A cloud-native architecture, typically built on stateless microservices deployed as containers, is poised as a promising technology for achieving flexibility, cost-efficiency, and scalability in the operation and management of 5G and future 6G networks [1]. However, the shift to cloud-native architectures expands the attack surface of 5G and beyond (B5G) networks, elevating the risk of privilege escalation and lateral movement by malicious actors within the network. This makes traditional perimeter-based security measures insufficient, highlighting a dire need for advanced security strategies to protect cloud-native B5G networks against external and internal threats.

A zero-trust (ZT) security model, grounded in the core tenet of "never trust, always verify", is a promising solution for establishing an effective end-to-end security stance in cloud-native B5G networks [2]. Indeed, ZT allows the proactive safeguarding of critical assets (e.g., data, computing resources, and services) by continuously authenticating and authorizing each access request, enforcing the principle of least privilege, implementing micro-segmentation, and maintaining continuous monitoring [3].

Driven by its benefits, there has been a growing research interest in recent years in incorporating the ZT security model in B5G networks [4]–[10]. The main focus was on improving authentication and access control schemes [4]–[8] and investigation of the potential of micro-segmentation as a key ZT enabler [9], [10]. Nevertheless, contributions made so far have been limited to a single network segment, such as Multi-access Edge Computing (MEC) [5], [6] and Open Radio Access Network (O-RAN) [4], [7], [8], and have primarily leveraged early 5G technologies, particularly Software Defined Networking (SDN) (e.g., [9], [10]). Furthermore, many of the proposed solutions remain largely theoretical, with limited practical implementation and testing, especially when it comes to deliver end-to-end ZT security for cloud-native B5G networks.

To bridge these gaps, we propose a novel ZT framework that aims to empower a truly end-to-end ZT security capable of thwarting both external and internal threats in cloud-native B5G service-based architectures. The proposed framework, dubbed THAALOUB, capitalizes on the security features offered by the emerging Service Mesh technology [11] to individually secure B5G network functions (NFs) with micro-perimeters, enforce robust authentication and fine-grained service-to-service access policies, and protect the confidentiality and integrity of data. To further refine access policies and deal with traffic heterogeneity, THAALOUB adopts a multi-layered ZT security approach by combining the capabilities of Service Mesh and Container Network Interface (CNI) technologies to implement micro-segmentation policies at layers L7 and L3/L4, respectively. To tame the complexity of building ZT secure B5G networks, THAALOUB framework encompasses an automation layer that facilitates fully automated, intent-based authentication and authorization policy generation and enforcement in compliance with 3GPP specifications. To the best of our knowledge, this is the first fully implemented, end-to-end ZT framework tailored specifically for cloud-native B5G networks.

The key contributions of this paper can be summarized as follows:

- We propose THAALOUB, a novel ZT framework that empowers 3GPP-compliant, end-to-end ZT security in cloud-native B5G networks.
- We promote a multi-layered ZT microsegmentation security model leveraging the advanced features of Service Mesh and CNI technologies.
- We introduce a 3GPP-compliant intent-based access control approach to foster proactive and fully automated ZT security management.
- We develop and deploy a full prototype of the

THAALOUB framework in a Kubernetes cluster, demonstrating its effectiveness in empowering resilient B5G networks with minimal impact on latency and resource usage.

The rest of this paper is structured as follows. Section II provides a critical review of related work. Sections III and IV elaborate, respectively, on the design and implementation specifics of the proposed ZT framework. Section V details the experimental setup and provides an in-depth performance assessment of the proposed solution. Finally, Section VI concludes the paper and outlines potential avenues for future research.

II. Related work & Limitations

The adoption of ZT security model in B5G networks has recently attracted significant attention from the research community. Most research efforts have been devoted to enhancing authentication and authorization methods to meet ZT principles, leveraging techniques such as single packet authentication [5], entropy-based [6] or machine learning-based [4], [7] user behavior profiling, and multi-factor authentication [8]. Furthermore, the focus has zeroed in on the MEC and O-RAN domains, with an emphasize on establishing ZT between user equipment (UE) and a 5G network. Thus, an end-to-end solution that enforces ZT security not only between UE and the network but also among B5G NFs has yet to be developed.

Interest in micro-segmentation as key enabler of ZT in B5G networks is also gaining momentum [9], [10], [12], driven by its potential to establish micro-perimeters around critical resources and enforce fine-grained security policies. With existing work focusing on SDN architectures, a notable gap remains in end-to-end ZT micro-segmentation solutions for cloud-native environments.

Recognizing its pivotal role in emerging cloud-native architectures, the integration of Service Mesh in 5G networks has been explored to enhance load balancing, flexibility, and latency, fostering a shift toward more dynamic, high-performance B5G architectures [13], [14]. Nevertheless, leveraging the advanced security features of Service Mesh in building ZT secure B5G networks remains largely unexplored.

Despite the growing interest, there is still a need for a truly end-to-end ZT security model that can bring in the potential of emerging inter-service communication technologies to counter both external and internal threats in cloud-native B5G networks.

III. Thaaloub – A B5G End-to-End ZT Security Framework

A. Framework Architecture

The framework comprises six functional layers that provide security, visibility, automation and orchestration capabilities essential for building a resilient cloud-native B5G architecture aligned with the ZT security principles. Fig. 1 illustrates the high-level architecture of the framework.

1) Orchestration Layer: The proposed ZT framework is designed for an end-to-end B5G architecture, encompassing a service-based Core Network (5GC) and a New Generation Radio Access Network (NG-RAN). The B5G architecture consists of loosely coupled and independent network functions (NFs) running as containerized microservices on a cloud-native platform. The cloud-native platform acts as a Container Infrastructure Service Management (CISM) function, overseeing the orchestration of the containerized B5G NFs in terms of deployment, monitoring, and lifecycle management [11]. In 5GC, Service Mesh technology is leveraged to implement the Service Communication Proxy (SCP) functionality, introduced by 3GPP in Release 16 [15] to facilitate seamless routing and communication among NFs. A Service Mesh setting allows for a distributed SCP deployment model, effectively addressing the inherent limitations of a centralized SCP such as single points of failure and latency bottlenecks.

2) 5G Microsegmentation Layer: THAALOUB's ZT security model operates on the principle of micro-segmentation, which entails partitioning the B5G network into smaller, isolated logical security zones. This approach aims to prevent unauthorized access by defining granular governance policies tailored to each micro-segment. In this vein, the B5G network is segmented into four distinct zones, namely UE, NG-RAN, 5GC control plane, and 5GC User Plane Function (UPF). Beyond enhancing security posture, decoupling UPF from 5GC control plane also fosters greater flexibility, scalability, and performance. Each segmented zone employs dedicated Ingress and Egress gateways to enable fine-grained scrutiny of incoming and outgoing traffic. Furthermore, the microsegmentation is implemented at the microservice level, ensuring that each B5G NF, with its distinct function and specific security requirements, operates within its own isolated segment. To this end, a Policy Enforcement Point (PEP) is placed in front of each B5G NF to enforce strict control and monitoring of inter-NF communications. Individually securing B5G NFs with micro-perimeters allows to contain security breaches within NF boundary, preventing lateral movement within the network [16].

3) Authorization and Authentication Layer: In compliance with NIST ZT architecture standards [17], this layer comprises a Policy Engine (PE), a Policy Administrator (PA) and a Public Key Infrastructure (PKI) to manage authentication and authorization processes. The PKI is responsible for issuing certificates and keys to enable mutual authentication between the micro-segments. The PE has the role of making real-time decisions on authorizing or denying access to micro-segments (i.e., B5G NFs) based on the defined access control policies. Finally, the PA is in charge of implementing the PE's decisions by configuring the associated PEPs to initiate or terminate communication sessions with B5G NFs. Only authenticated and authorized access requests are deemed trustworthy and granted access to the requested NFs.

Given the heterogeneity of B5G network protocols and interfaces, the adoption of a multi-layered filtering approach is deemed crucial to achieving robust security posture. To this

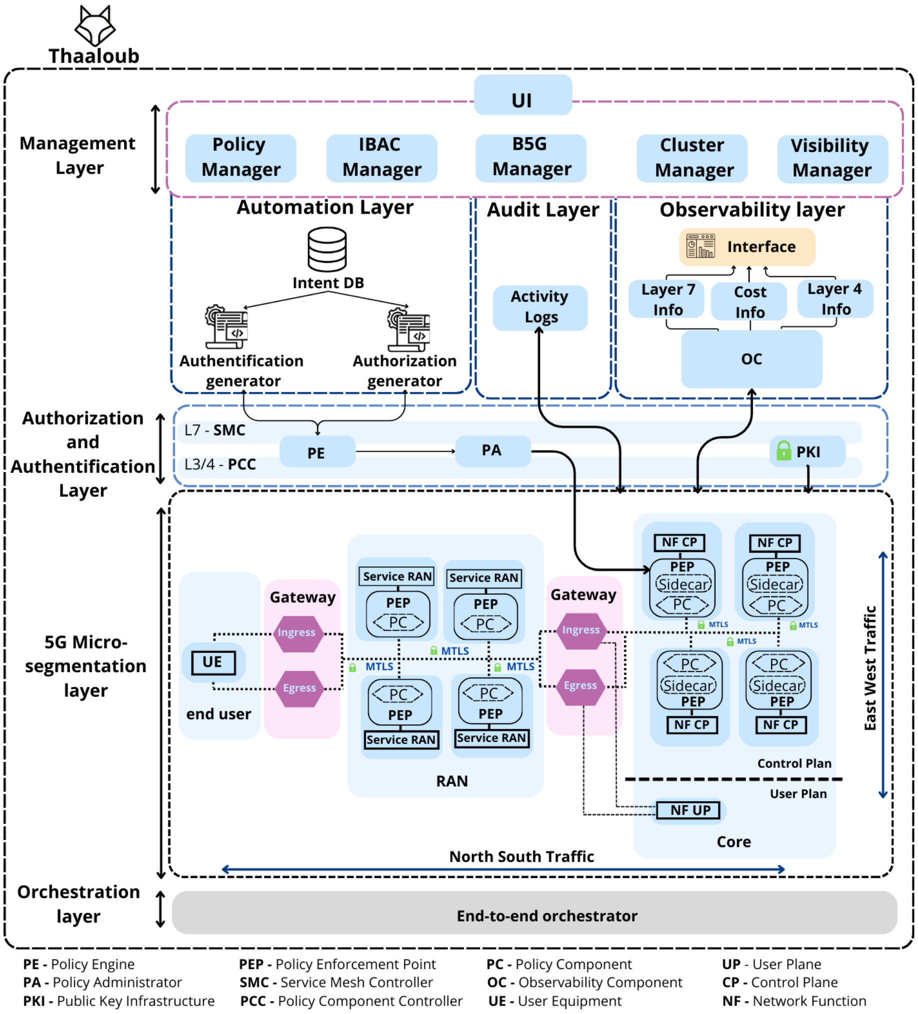


Fig. 1: High-Level Architecture of THAALOUB Framework.

end, we introduce two logical components – Service Mesh Controller (SMC) and Policy Component Controller (PCC) – that provides PE, PA, and PKI functionalities at L7 and L3/L4, respectively. The PCC oversees Policy Components (PCs), acting as PEPs, to enforce authentication and authorization policies at L3/L4, effectively filtering out malicious access requests based on protocols such as Internet Control Message Protocol (ICMP), TCP, UDP, Stream Control Transmission Protocol (SCTP), Packet Forwarding Control Protocol (PFCP), and Next Generation Application Protocol (NGAP). The SMC enables authentication and filtering of L7 traffic thanks to its sidecar, which serves as PEP for HTTP/2.

4) Automation Layer: This layer aims to abstracts the complexity arising from manual configurations by automating the generation of authentication and authorization policies through an Intent-Based Access Control (IBAC) approach. By focusing on "what" access control is desired rather than "how" to achieve it, IBAC fosters proactive, agile, and scalable ZT security management in B5G networks [18]. The access control intentions of B5G NFs adhere to 3GPP specifications. The automation layer incorporates two generators in charge of automatically translating the declared access control intents into corresponding authorization and authentication policies that can be enforced by SMC and PCC components.

5) Observability and Audit Layers: A core principle of ZT is to maintain a continuous visibility into network resources and activities, yielding valuable insights into the network's security posture. THAALOUB framework embodies this principle through observability and audit layers, which collect relevant data from PEPs. The observability layer consists in a real-time monitoring system providing comprehensive oversight of network flows, enforced access control policies, and system performance metrics (e.g., latency, CPU, and RAM). As for the audit layer, it delivers full audit trails of all activities occurring within the B5G network, promoting accountability and ensuring ZT compliance and regulatory adherence.

6) Management Layer: This layer aims to simplify network and ZT security management complexities by exposing a set of management functions via a user-friendly Graphical User Interface (GUI). Thanks to the exposed functions, the management layer facilitates the automation of the entire process of provisioning a cloud-native platform, deploying a B5G network, specifying and updating access control intents, and managing applied authentication/authorization policies.

It also offers a comprehensive visibility into B5G system, featuring detailed security and performance indicators.

B. Authentication & Authorization Approaches

1) Authentication Approach: In the ZT concept, resource authentication is crucial for verifying the identity of each resource seeking to communicate and exchange data. Thus, unlike traditional methods where authentication is typically performed at the network entry point, THAALOUB framework entails individual authentication at the level of each microsegment, enabling mutual authentication between source and destination. Each microsegment has its own certificate issued by a Certificate Authority (CA), which is used to prove its identity during data exchanges. In THAALOUB framework, the role of CA is fulfilled by the PKI, with SMC filling this role for 5GC domain and PCC for NG-RAN domain. The authentication procedure begins with a handshake protocol, wherein the PEPs exchange certificates to verity each other's identities. Subsequently, asymmetric encryption is used to establish a shared symmetric key that can be then utilized to establish secure communication channels.

2) Authorization Approach: As mentioned earlier, THAALOUB implements authorizations at both L3/L4 using network policies and L7 via a Service Mesh. Unlike traditional use of IP addresses, THAALOUB utilizes labels to dynamically define and control access to B5G resources. This allows for defining policies based on service and user attributes rather than static IP addresses, offering greater flexibility and security for managing access and communications within a cloud-native B5G system. In fact, IP addresses in cloud-native environments are ephemeral and cannot be used to identify micro-services.

At L3/L4, network policies define access rules based on criteria such as labels, ports, and protocols, ensuring fine-grained, dynamic segmentation of the network. The following is an example of a L4 authorization for the NG-RAN's Control Unit-Control Plane (CU-CP) service, allowing 5GC's Access and Mobility Function (AMF) to exchange data with CU-CP via port "38412" using SCTP protocol:

```
authorization-name: allow-sctp-AMF-CUCP
destination: CU-CP
source: AMF
rules:
    action: ALLOW
    protocol: SCTP
    ports: "38412"
```

In addition to labels, ports and protocols, L7 authorizations are further defined by HTTP/2 methods and paths. The following example illustrates a L7 authorization for the nnrf interface of the 5GC's Network Repository Function (NRF), allowing AMF to communicate with NRF via port "80" using HTTP protocol, PUT method, and accessing path "/nnrf-nfm/v1/nf-instances/*":

```
authorization-name: allow-sctp-AMF-NRF
destination: NRF
source: AMF
rules:
    action: ALLOW
    protocol: HTTP
    method: PUT
    ports: "80"
    path: "/nnrf-nfm/v1/nf-instances/*"
```

IV. IMPLEMENTATION DETAILS

A full prototype of THAALOUB framework has been developed and deployed in a Kubernetes cluster, leveraging a set of open source tools to implement its different functionalities as illustrated in Fig. 2. Driven by their capabilities, Istio and Cilium have been used as the Service Mesh and CNI, respectively. Istio stands out for its enhanced traffic management, advanced security features, and comprehensive observability for mciroservices [11]. Fueled by the Kernel extended Berkeley packet filter (eBPF) technology, Cilium delivers high-performance packet processing, fine-grained network policies, and deep visibility into network traffic for containerized environments. In what follows, we highlight key implementation details of the proposed ZT framework.

A. 5G Network Deployment

The proposed micro-segmentation approach has been applied to the OAI's NG-RAN and Open5GS's 5GC. A coarse isolation is first established between NG-RAN and 5GC microservices by deploying them into two distinct namespaces. The NF microsergments are then set leveraging Istio and Cilium for Open5GS's 5GC and Cilium for OAI's NG-RAN.

We introduced several improvements to the original Open5GS Helm chart[1] in order to support the devised ZT security model. This includes (i) replacing the Calico's static addressing with a dynamic addressing based on Cilium; (ii) the use of service DNS names instead of IP addresses for gNB and AMF, enhancing communication robustness and reliability; (iii) incorporating an application label, naming service ports and containers, and versioning deployment manifests and services to meet Istio's requirements, thereby ensuring better management and collection of metrics; and (iv) adding a service account for each NF to identify micro-segments within the Service Mesh.

B. Authentication & Authorization

1) L7 Authentication with Istio: Upon deploying Istio, its control plane (i.e., istiod) generates a root certificate to sign service certificates. Acting as a CA, Istiod issues short-lived X.509 certificates to new services via Citadel, the component in charge of managing certificates and secure mTLS authentication. These certificates are then distributed to the services' Envoy proxies by Pilot, which responsible for the service mesh configuration, routing rules, and service discovery. The issued certificates are used to enable service-to-service mTLS authentication. Istio supports three mTLS authentication modes – Permissive, Strict, and Disable – that respectively specify whether mTLS traffic is optional, required, or completely

[1] https://bitbucket.org/infinitydon/opensource-5g-core-service-mesh/src/main/

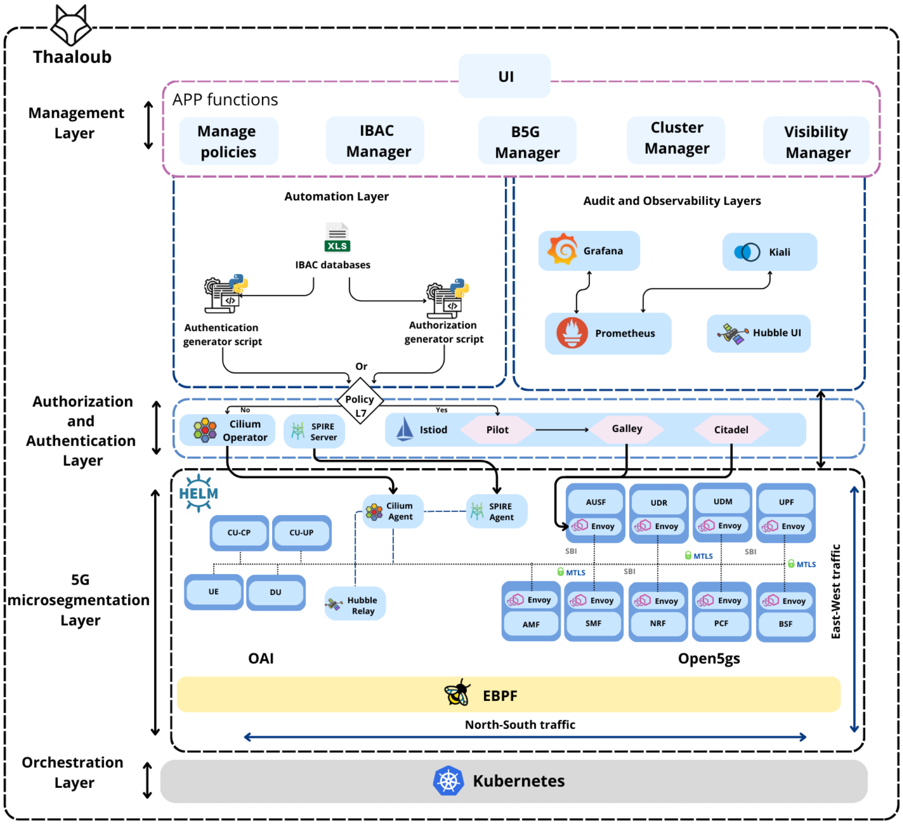


Fig. 2: THAALOUB framework deployment.

disabled. In this study, the Strict mode is enforced for inter-service communication within the deployed 5G network.

2) L3/L4 Authentication with Cilium: For non-HTTP inter-service communications, such as between SMF and UPF, gNB and AMF, and within the disaggregated RAN, Istio's authentication is not applicable. Thus, mutual authentication at L3/L4 is enforced using Cilium in conjunction with SPIRE, an implementation of the Secure Production Identity Framework for Everyone (SPIFFE) specification. During service deployment, SPIRE provisions SPIFFE IDs and short-lived X.509 certificates in the form of SPIFFE Verifiable Identity Documents (SVIDs) to services. Cached by the SPIRE Agent running on each compute node, the issued SVIDs serve for performing mTLS authentication between services.

3) L7 Authorization with Istio: Upon generation by the automation layer, the L7 authorization policies remain on hold in Istiod until the associated services are deployed. Once this occurs, these authorizations are distributed to the services' Envoy proxies, which enforce access control at runtime. Access requests to a service are assessed by its Envoy proxy against the enforced policies to determine whether to grant or deny access. Only those explicitly permitted by "ALLOW" rules in each service are accepted, while all others are denied.

4) L3/L4 Authorization with Cilium: Once generated by the automation layer, L3/L4 authorization policies are managed by the Cilium Operator, which stores and transmits a copy of them to Cilium Agents. Cilium leverages extended Berkeley packet filter (eBPF) technology to enforce network authorizations, allowing to support label-based identification of resources instead of IP address-based identification. An eBPF program, loaded into the Linux kernel by the Cilium agent, intercepts packets and instructs the kernel to drop any packets not conforming to the microsegment's authorization rules.

C. Automation layer

Four IBAC databases have been created in Excel format. The first database is generic and includes IBACs extracted from 3GPP TS specifications. As we noticed that existing 5G open source solutions do not cover the full range of 3GPP specifications, three implementation-specific databases have been created, containing L7 and L3/L4 IBACs for Open5GS and L3/L4 IBACs for OAI, respectively. The authentication and authorization generators are developed in Python, facilitating the automatic creation of Istio's and Cilium's authentication and authorization policies from theses databases.

D. Observability & Audit

THAALOUB leverages a set of open source tools to provide a comprehensive view of the 5G system's security and performance across metrics, logs and tracing. Prometheus ingests metrics from Istio and the Hubble instance within Cilium Agent, and Grafana is used to visualize the collected metrics. Network traffic flows and security events at L3/L4 are displayed using Hubble UI. Finally, Kiali is leveraged to visualize service health as well as network flow graphs and logs collected from Istio.

V. Performance Evaluation

A. Experimental Settings

Thaaloub was deployed and tested on a single-node Kubernetes cluster created using Minikube on a physical machine running Ubuntu 22.04. The cluster is configured with 7 vCPU and 25GB RAM. Due to incompatibility between OAI's NG-RAN and Open5GS's 5GC, we tested each part separately. To this end, two 5G setups have been created: one using Open5GS as 5GC and UERANSIM as UE and RAN simulator, the other utilizing the entire OAI 5G stack to simulate UEs, a disaggregated RAN, and 5GC.

B. Evaluation Results

The effectiveness of Thaaloub in building ZT secure B5G networks is evaluated by investigating its capacity to bolster 5G network resilience to reconnaissance, Man-in-the-Middle (MITM), HTTP path injection, and Denial of Service (DoS) attacks. The attacks have been conducted against both Open5GS and OAI's NG-RAN NFs. Alongside its effectiveness, we assess the framework's efficiency by measuring the latency, CPU and RAM overhead incurred by ZT micro-segmentation.

1) Resilience to Attacks: The *reconnaissance* attack was performed by conducting port scan against 5G services using Nmap tool. Without Thaaloub, the attack succeeded in identifying open ports across the 5G network, heightening the risk of vulnerability exposure. However, the multi-layered ZT micro-segmentation in Thaaloub effectively prevented the identification of port states by dropping the illicit scan probes.

The *MITM* attack was simulated by deploying a Tcpdump pod between two network services. The captured traffic has revealed that Open5GS is vulnerable to MITM attack, allowing to disclose sensitive information, including the International Mobile Subscriber Identity (IMSI) and NF instance IDs. Nevertheless, the encrypted communications in OAI and in 5G with Thaaloub defeated sensitive data interception.

The *HTTP path injection* attack demonstrated the risk posed by unrestricted access in exposing 5G NFs to unauthorized manipulation and disturbance, jeopardizing the security and availability of the network. Leveraging the NF instance IDs captured with MITM and the lack of authentication check of requests sent to NRF in Open5GS, we were able to send malicious DELETE requests, successfully de-registering 5GC NFs from NRF. The mutual authentication and least-privilege principle in Thaaloub helped in thwarting this attack.

The *DoS* attack was carried out against 5G NFs at both network and application layers. Scapy and curl tools were used to launch SCTP-based and HTTP-based flooding attacks against NRF and CU-CP, respectively. Without Thaaloub, the DoS attacks succeeded in disrupting the availability of the target NFs. Thaaloub effectively deterred DoS attacks, owing to implemented micro-perimeters and robust access controls.

Table I summarizes the resilience to common 5G attacks with and without the proposed framework, demonstrating its high effectiveness in bolstering 5G security posture.

2) RAM and CPU Overhead: Fig. 3 reports the CPU and RAM usage in 5GC and NG-RAN domains, with and without the proposed multi-layered ZT security model. The use of Thaaloub induces the highest computation and storage overhead compared to the deployment of 5GC and NG-RAN alone, or with only Cilium or Istio. Note that for NG-RAN, the overhead of Thaaloub is similar to that of Cilium-based scenario, as both apply only L3/L4 policies. The results show that the majority of Thaaloub's additional overhead stems from the deployed Cilium CNI and Istio Service Mesh components as well as the visibility modules, particularly Grafana and Prometheus services. Nonetheless, the integration of CNI and Service Mesh is deemed crucial for cloud-native B5G networks, providing not only resilience but also enhanced scalability and flexibility. Furthermore, the significant improvements in the network's security posture provided by Thaaloub outweigh the associated overhead, which remains within acceptable limits. In fact, enforcing authentication and authorization policies accounts for less than 37% of CPU and 24% of RAM usage in 5GC, and less than 14% of CPU and 10% of RAM usage in NG-RAN. It is worth noting that despite the 37% increase, the total CPU usage in 5GC remains below 0.08 core.

TABLE I: Resilience to attacks with and without Thaaloub.

	Port Scan	MITM	Path Injection	DoS
Open5GS without Thaaloub	×	×	×	×
OAI without Thaaloub	×	✓	NA	×
5G with Thaaloub	✓	✓	✓	✓

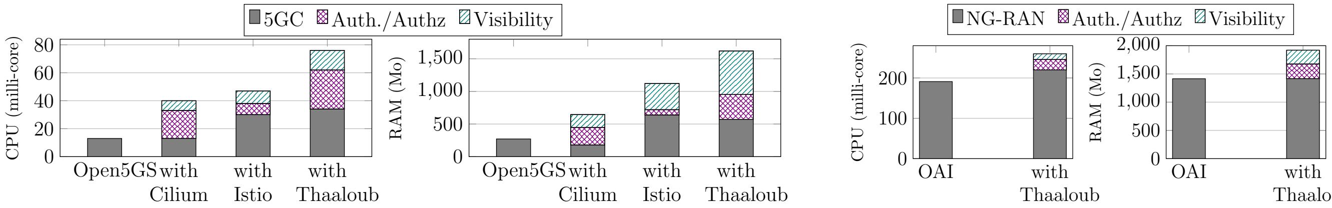
✓– Successful Mitigation, × – Unsuccessful Mitigation, NA – Attack Not Applicable.

3) Latency: We evaluate the impact of the proposed multi-layered ZT security model on both control plane latency and end-to-end latency. For the control plane latency, we focus on the 5GC domain due to its complex signaling and interactions among its NFs. Fig. 4 shows the 99th percentile latency of 5GC's microservices in handling UE attachment requests, encompassing both UE registration and Protocol Data Unit (PDU) session establishment procedures. Note that the scale on the y-axis is logarithmic. The results indicate that, regardless the number of simultaneous attachment requests, the use of Thaaloub incurs only minimal increase in control plane latency compared to the baseline deployment without ZT security, demonstrating Thaaloub's efficient scalability.

Fig. 5 shows the 50th, 95th, and 99th percentile end-to-end network latency measured using iPerf2 tool. iPerf2 is initiated in client mode at UE side and server mode on a distant machine accessed via 5G network. To our surprise, the use of Thaaloub yields lower end-to-end latency compared to the baseline setup without ZT security. We found that this improvement ensues from the efficient routing and traffic management of Cilium CNI, compared to the Minikube's default bridge network used in the baseline setup. However, Thaaloub exhibits only a slight impact on end-to-end latency compared to Cilium-based setup without ZT security.

VI. Conclusion and Future Research Direction

In this paper, we introduced Thaaloub, a novel ZT framework for empowering truly end-to-end ZT security in



(a) Open5GS's 5GC

(b) OAI's NG-RAN

Fig. 3: Resource usage of 5G network for session establishment.

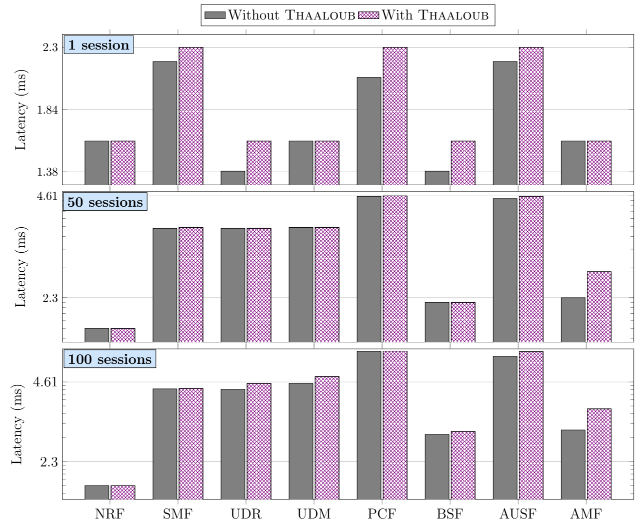


Fig. 4: Latency of 5GC's NFs with and without THAALOUB.

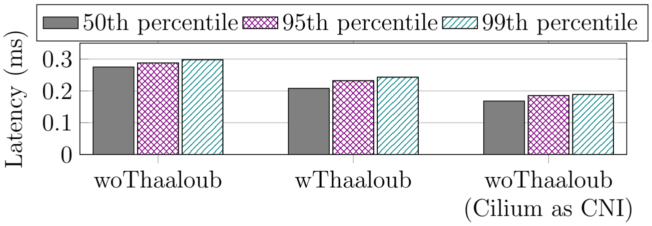


Fig. 5: End-to-End latency with (w) and without (wo) THAALOUB.

cloud-native B5G networks. Combining the advanced security features of the emerging Service Mesh and CNI technologies, THAALOUB promotes a multi-layered ZT micro-segmentation security model capable of enforcing robust authentication and fine-grained access control policies. Furthermore, it fosters proactive, agile, and scalable ZT security management through a 3GPP-compliant intent-based access control approach. The experimental results demonstrated the effectiveness of the proposed ZT framework in fortifying B5G security posture with minimal impact on latency and resource usage. In the future, we will explore the potential of Large Language Models (LLMs) to enable intelligent management of IBACs throughout their lifecycle, from extraction to enforcement and dynamic updating.

ACKNOWLEDGEMENT

This research work is partially supported by the Research Council of Finland (former Academy of Finland) under 6G Flagship program (Grant No. 369116), and the European Union's Horizon Europe research and innovation programme HORIZON-JU-SNS-2022 under the RIGOUROUS project (Grant No. 101095933). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] C. Benzaïd, T. Taleb, and J. Song, "AI-Based Autonomic and Scalable Security Management Architecture for Secure Network Slicing in B5G," *IEEE Network*, vol. 36, no. 6, pp. 165–174, 2022.

[2] C. Benzaïd, T. Taleb *et al.*, "Trust in 5G and Beyond Networks," *IEEE Network*, vol. 35, no. 3, pp. 212 – 222, May 2021.

[3] N. Nahar *et al.*, "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," *IEEE Access*, vol. 12, pp. 94 753 – 94 764, Jul. 2024.

[4] K. Ramezanpour and J. Jagannath, "Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the Context of O-RAN," *Computer Networks*, vol. 217, p. 109358, Nov. 2022.

[5] B. G. Jung *et al.*, "Zero trust black network access for mobile broadband mission-critical services," in *2023 14th Int. Conf. Inf. Commun. Technol. Convergence (ICTC)*, Oct. 2023, pp. 1416–1418.

[6] B. Ali *et al.*, "Zero Trust Security Framework for 5G MEC Applications: Evaluating UE Dynamic Network Behaviour," in *2023 33rd Intl. Telecommun. Net. and Appl. Conf.*, Nov. 2023, pp. 140–144.

[7] H. Moudoud and S. Cherkaoui, "Enhancing open ran security with zero trust and machine learning," in *Proc. of IEEE GLOBECOM 2023*, Dec 2023, pp. 2772–2777.

[8] A. S. Abdalla *et al.*, "Ztran: Prototyping zero trust security xapps for open radio access network deployments," *IEEE Wireless Communications*, vol. 31, no. 2, pp. 66–73, Apr. 2024.

[9] O. Mämmelä *et al.*, "Towards micro-segmentation in 5g network security," in *Proc. of EuCNC 2016 Workshop on Network Management, Quality of Service and Security for 5G Networks*, 2016.

[10] A. Osman *et al.*, "Transparent Microsegmentation in Smart Home IoT Networks," in *3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 2020)*, Jun. 2020.

[11] C. Benzaïd, T. Taleb, and J. Song, "AI-based Autonomic & Scalable Security Management Architecture for Secure Network Slicing in B5G," *IEEE Network Magazine*, vol. 36, no. 6, pp. 165 – 174, Nov./Dec. 2022.

[12] N. Basta *et al.*, "Towards a zero-trust micro-segmentation network security strategy: an evaluation framework," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2022, pp. 1–7.

[13] V.-B. Duong and Y. Kim, "A Design of Service Mesh Based 5G Core Network Using Cilium," in *2023 International Conference on Information Networking (ICOIN)*, Jan. 2023, pp. 25–28.

[14] S. Aldas and A. Babakian, "Cloud-Native Service Mesh Readiness for 5G and Beyond," *IEEE Access*, vol. 11, pp. 132 286–132 295, Nov. 2023.

[15] 3GPP TS 23.501 V19.0.0, "System Architecture for the 5G System (5GS); Stage 2 (Release 19)," June 2024.

[16] T. Theodoropoulos, L. Rosa, C. Benzaïd *et al.*, "Security in Cloud-Native Services: A Survey on Key Features," *J. Cyber Security and Privacy*, vol. 3, no. 4, pp. 758–793, Oct. 2023.

[17] S. Rose *et al.*, "Zero Trust Architecture," p. 50, Aug. 2020.

[18] C. Benzaïd and T. Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Network*, vol. 34, no. 3, pp. 124 – 133, May/June 2020.