A Lightweight Multi-BS Cooperation AKA Mechanism for Fully Decoupled RAN

Ning Wang, *Graduate Student Member, IEEE,* Jiacheng Chen, Wenchao Xu, *Member, IEEE,* Liquan Chen, Haibo Zhou, *Senior Member, IEEE*

***Abstract*—The Fully Decoupled Radio Access Network (FD-RAN) divides the base station (BS) into three components: the Uplink Data Base Station (UBS), the Downlink Data Base Station (DBS), and the Control Base Station (CBS) to achieve an ultra flexible network. FD-RAN can easily realize dynamic multi-BS cooperation to boost throughput and guarantee users' quality of experience. However, as the number of cooperating BSs and concurrently accessed Internet of Things (IoT) devices increases, significant Authentication and Key Agreement (AKA) overheads will be incurred, and the system becomes vulnerable to various security threats. This paper proposes a novel lightweight AKA protocol that employs secret value sharing for secure key negotiation among BSs, UE and the core network (CN). Furthermore, multi-device of IoT access is optimized through Aggregated Message Authentication Codes with Detecting Functionality (AMAD) to efficiently manage and aggregate access requests. By utilizing interpolation polynomials and multi-party key agreement techniques, the proposed solution improves key negotiation efficiency while mitigating risks from man-in-the-middle (MitM) and Distributed Denial of Service (DDoS) attacks. Security analyses are conducted to validate the protocol while showcasing its superiority on computation, communication and transmission efficiency.**

***Index Terms*—FD-RAN, AKA, multi-BS cooperation, multi-user access, group key negotiation**

I. Introduction

THE future of communication networks will be driven by the needs of billions of users and trillions of connected devices [1], requiring a robust and efficient architecture. Traditional networks confront challenges due to inadequate uplink coverage, inefficient resource scheduling, and limited transmission modes. The Fully Decoupled Radio Access Network (FD-RAN) [2] emerges as an innovative solution to enhance network performance and user experience. As illustrated in Fig. 1, FD-RAN evolves from the fifth-generation networks (5G) by fully decoupling the control and data planes, and disaggregating the traditional base station (BS) into three distinct types: Uplink Data Base Station (UBS), Downlink Data Base Station (DBS), and Control Base Station (CBS). Owing to its flexibility, FD-RAN can realize advanced resource scheduling and flexible multiple BSs cooperation, enhancing network capability and improving user's quality of service (QoS) [3].

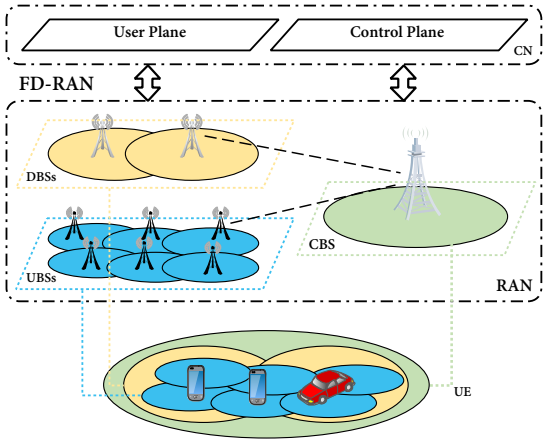


Fig. 1. A Multi-device Access Scenario in Fully Decoupled Radio Access Network.

Despite its unique advantages, the FD-RAN architecture introduces new security issues. Instead of serving the user with a single BS, FD-RAN is featured by the flexible cooperation of multiple BSs to serve users [4]. Consequently, significant security costs will be incurred for key negotiation, key computation and key transmission, and the network may be exposed to security threats such as Distributed Denial of Service (DDoS) attacks. Thus, a reliable and efficient multi-BS Authentication and Key Agreement (AKA) mechanism is required to verify the identities and establish trust relationships among the core network (CN), cooperative Data BSs and each accessing user [5].

Multi-BS AKA in FD-RAN architecture faces several major challenges. First, unlike the control BS and CN, which are considered root of trust, data BSs are untrustworthy, since the control and data BSs are physically decoupled in FD-RAN. So, Data BSs need to be authenticated to verify their identity.

Second, the authentication procedure for user equipment (UE) access to Data BSs is more complex than that of traditional AKA [6]. In FD-RAN, given that user identity

This work was supported in part by the National Natural Science Foundation Original Exploration Project of China under Grant 62250004, the Natural Science Foundation of China (NSFC) under Grant 62271244, Innovation and Entrepreneurship of Jiangsu Province High-level Talent Program, Summit of the Six Top Talents Program of Jiangsu Province, The Major Key Project of PCL, and The Basic and Frontier Research Project of PCL. *(Corresponding author: Haibo Zhou and Ning Wang.)*

Ning Wang and Liquan Chen are with the School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China (e-mail: ningwang2022@seu.edu.cn; lqchen@seu.edu.cn).

Jiacheng Chen is with the Department of Strategic and Advanced Interdisciplinary Research, Peng Cheng Laboratory, Shenzhen 518000, China (e-mail: chenjch02@pcl.ac.cn).

Wenchao Xu is with the Department of Computing, Hong Kong Polytechnic University, Hong Kong 100872, China (e-mail: wenchao.xu@polyu.edu.hk).

Haibo Zhou is with the School of Electronic Science and Engineering, Nanjing University, Nanjing 210023, China (e-mail: haibozhou@nju.edu.cn).

information is exclusively stored in the control plane, mutual authentication between Data BSs and UE must be conducted through the CBS. Upon receiving the authentication request for the UE from Data BS, the CBS must first verify the legitimacy of Data BS and then confirm the legitimacy of UE. The results are then transmitted to both the UE and Data BS by CBS respectively. Obviously, the process for authentication becomes more complicated. Moreover, since FD-RAN provides data transmission through multi-BS cooperation, UEs must undergo mutual authentication with each of these BSs. The frequent authentication among the UE and multi-BS could result in more overheads, increasing system burden and adversely affecting communication quality.

Lastly, in massive machine-type communication scenarios, such as the Internet of Things (IoT) and the Industrial Internet [7], multiple UEs from the same user or entity need to initiate simultaneous access requests [8], which increases access overheads and reduces access efficiency of FD-RAN. All these requests will be forwarded to the CBS for AKA negotiation. This redundant verification process leads to significant waste of resources, increases access authentication costs and adversely affects the communication efficiency of FD-RAN.

To address the above issues, we propose a novel AKA mechanism that utilizes group key negotiation for efficient mutual authentication between the Data BS and CBS, as well as among Data BSs themselves. This mechanism reduces redundant interactions for authentication information, thereby also improving the efficiency of UE's access to multi-BS. Furthermore, by employing group key agreement and aggregation techniques, we optimize the AKA scheme for multi-UE by selecting a single representative UE to perform the AKA process with the BS, rather than requiring each UE to undergo the AKA individually. In this way, we significantly reduce the AKA authentication overheads during multi-UE access FD-RAN and mitigate the risk of DDoS attacks. To the best of our knowledge, we are among the earlier researchers to investigate the authentication security of multi-UE access tailored for multi-BS cooperation in FD-RAN. This work aims to ensure not only the efficient and secure access of multiple UEs but also the effective and secure cooperation among multiple BSs. The key contributions of this paper are as summarized follows:

- Lightweight Authentication Mechanism: We introduce a new lightweight symmetric key algorithm combined with Shamir's secret sharing and verifiable secret sharing technologies to create stable Data BSs group. This mechanism significantly reduces the authentication overheads while guaranteeing the security of multi-BS cooperation. Secret information is transmitted using interpolation polynomials, and a designated group leader is appointed to facilitate efficient cooperation.
- Lightweight Authentication for Single UE: To minimize access overheads for individual UEs, the derived key from the Data BS group key negotiation is utilized as the root key for authentication and session establishment between the UE and the Data BS group. This process allows for 0-Round Trip Time (0-RTT) access authentication, drastically reducing overheads related to security keys distribution, computation, storage, and management.
- Lightweight Authentication for Multiple UEs: To address the security risks and overheads associated with multiple UEs accessing FD-RAN, we employ a contributory broadcast encryption (CBE) technique. This method establishes a group for UEs that are in close proximity and share the same access needs. An aggregate message authentication code (AMAD) with detection capabilities is implemented to facilitate the aggregation of access requests, ensuring UE anonymity while enabling the traceability of malicious UEs.
- Security and Performance Analysis: Security assessment demonstrates the advantages of forming cooperative Data BS groups with lightweight dense value sharing. AMAD effectively identifies malicious identities and enhances group robustness. Performance analysis shows that our solution significantly reduces the access and authentication overheads for multi-BS cooperation in FD-RAN.

The remainder of this paper is organized as follows. Section II reviews the related work. Section III introduces the system model, security assumption, design goals and overview of our scheme. Section IV introduces the preliminaries and related technologies. Section V details the proposed scheme, including group establishment, and UE authentication. The security analysis is performed in Section VI. The performance evaluation is described in Section VII. Finally, we draw the conclusion in Section VIII.

II. Related Work

A. Security of Multi-AP Transmission

In the context of ensuring the security of multi-AP cooperation, most related works focus on constructing groups and emphasize mobile handover authentication. For example, a vehicle anonymity handover authentication scheme based on aggregated proxy signature technology is proposed in [9]; [10] introduces a pre-handover authentication mechanism for high-speed rail user groups based on the Chinese Remainder Theorem (CRT); [11] presents an access authentication protocol primarily aimed at addressing user anonymity and traceability issues. Additionally, [12] utilizes a lightweight group key agreement mechanism based on secret sharing technology, focusing on achieving better handover authentication without conducting in-depth research on interactions within satellite groups. [13] proposes two pre-handover authentication schemes for fixed orbit groups used by mobile relay nodes with an Software Defined Networking (SDN) controller, resulting in negligible handover delays. [14] proposes a group authentication scheme based on multiple signatures and AMAD technology. [15] introduces a robust and universal handover authentication scheme for 5G HetNets, which leverages the characteristics of chameleon hash functions and the tamper-proof features of blockchain to achieve anonymous authentication. [16] presents a fast and secure handover authentication scheme suitable for all mobile scenarios in Long-Term Evolution (LTE) networks, offering perfect forward secrecy (PFS), master key forward secrecy (MKFS), and user anonymity security guarantees. Lastly, [17] outlines a comprehensive network roaming scheme that spans from the Third Generation Partnership Project

(3GPP) to worldwide interoperability for microwave access (WiMAX), encompassing handover authentication and secure channel establishment while accounting for transitions between different types of access points within LTE network. These works have their advantages in providing anonymity for group communications and reducing overheads. However, as analyzed in Section VII, these schemes incur significant overheads when applied to the FD-RAN architecture, failing to meet the security communication requirements for flexible and efficient multi-BS cooperation.

B. Security of Multi-UE Accessing

Ensuring user access security is relatively straightforward for users. Grouping user equipments or devices with similar mobility patterns or resource requests allows for more efficient group authentication, significantly reducing overheads. Consequently, there is a growing consensus in the literature on the necessity of designing authentication schemes that support multi-user equipments access. Chen et al. [18] pioneered a group authentication and key agreement (GAKA) method based on Secure Context Transfer (SCT), designed for a large number of UEs. In [19], their machine-type communication (MTC) AKA protocol transmits a group temporary key (GTK) to the Serving Node (SN) for local authentication among Mobile Devices (MDs) after the first MD completes access authentication. However, these protocols lack privacy protection. To address this, Lai et al. [20] introduced a Lightweight Group Authentication Protocol (LGTH) that employs Aggregate Message Authentication Code (AMAC) technology. This protocol enables the Home Subscriber Server (HSS) to authenticate the MTC group by verifying the group's AMAC, thus optimizing the authentication process. Similarly, Cao et al. [21] presented the Group-Based Aggregate Authentication Mechanism (GBAAM) for MTC in LTE networks, which can verify the MTC group through aggregated signatures. While these aggregation methods reduce signaling and communication costs, the LGTH protocol is vulnerable to internal forgery attacks and does not adequately protect identity privacy. Conversely, the GBAAM protocol incurs high computational costs due to its reliance on public key cryptography.

Cao et al. [22] enhanced the LGTH mechanism with a Lightweight Privacy-Preserving Access Authentication (LPPA) protocol for large-scale devices in LTE-Advanced networks. However, the LPPA requires numerous key identifiers, leading to significant storage and communication costs while failing to achieve identity anonymity. Further advancements by Cao et al. [7] incorporated Chebyshev chaotic mapping and the CRT into a new access authentication scheme (LSAA) that supports both single UEs and large-scale MDs. Nonetheless, this scheme falls short in securing multi-BS cooperation within the FD-RAN architecture, resulting in increased computational and storage demands for keys. The access authentication protocol in [23] primarily addresses user anonymity and traceability. [24] proposes a handover authentication scheme for mobile multi-users that utilizes AMAD and contributory broadcast encryption, focusing on handover operations, such as the transitions between different Access and Mobility Management Functions (AMFs) brought about by mobility. [25] presents an authentication scheme for large-scale vehicular devices in 3GPP networks that minimizes network congestion by using mobile relay nodes to enhance link quality and reduce latency. Further, [26] proposes grouping users based on their signal-to-noise ratios and historical handover information, allowing group members to bypass authentication phases during BS access. Additionally, pseudonyms are changed at each handover to enhance privacy. [27] integrates user capabilities with SDN technology in ultra-dense heterogeneous network (HetNet) scenarios, proposing a privacy-preserving handover authentication mechanism. [28] employs pairing-based cryptography and batch signatures to secure handover processes, supporting user revocation and reducing overheads. [29] designs a region-based fast handover protocol ensuring identity randomization.

Despite the improvements in efficiency and reductions in overheads that these solutions offer for secure multi-UE access, they are primarily tailored for the current single-BS access scenarios. Different from the above works, we aim to realize secure multi-UE access in a decoupled multi-BS cooperation architecture within FD-RAN, while also ensuring security and efficiency for multi-BS cooperation.

III. System Model And Design Goals

This section introduces the system model studied in this paper, along with the corresponding security assumptions and security objectives.

A. System Model

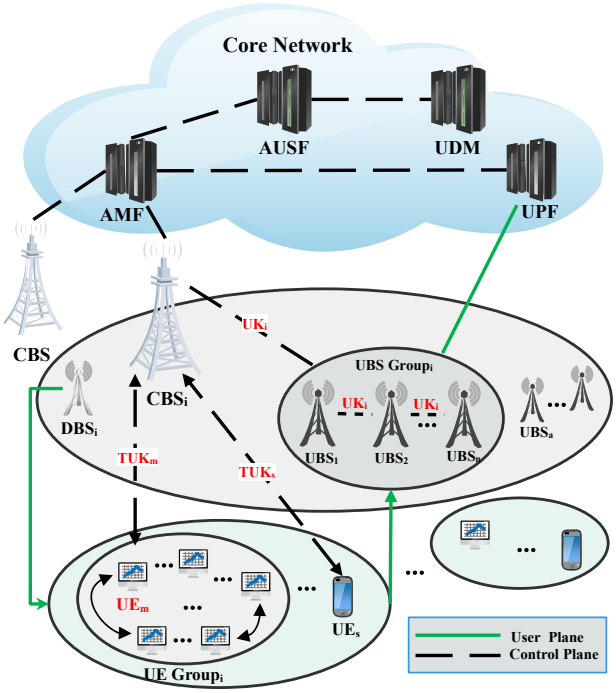


Fig. 2. System Model.

The system model is illustrated in Fig. 2, the key security entities include Data BSs, CBS, AMF, Authentication Server

Function and Unified Data Management (AUSF/UDM), and UEs as described below:

- Core Network (CN): Comprising AUSF/UDM and AMF, the CN manages UE access. The AUSF handles authentication requests and provides relevant vectors, while UDM facilitate identity verification and user data management. The AMF establishes control plane session with the user and acts as a multi-BS group manager.
- CBS: The CBS collects signaling messages from UEs and Data BSs, forwarding instructions from the CN. Trusted for its reliability, the CBS ensures accurate transmission of signaling messages between various nodes and the CN.
- Data BS Group: Comprising UBSs and DBSs, Data BSs are responsible for transmitting user data. These BSs are considered untrusted due to their vulnerability to attacks and limited computational resources. They do not communicate directly with the CN's control plane but and utilize relay through the CBS.
- UE and UE Group: UEs can include various devices equipped with adequate computational capabilities and wireless transceivers. These devices can form groups based on trust relationships and similar access needs.

To fulfill the security requirements of FD-RAN, the proposed solution employs AMAD and secret sharing technology to facilitate mutual authentication and key negotiation among the Data BS group, CBS, UE groups, and the CN.

We assume that the CN and its components cannot be compromised by adversaries. However, Data BSs may be impersonated by malicious entities, potentially deceiving other Data BSs into providing access and session services to unauthorized UEs. In our system model, we assume secure connections among the CBS, AMF, and AUSF/UDM. The CBS is deemed fully trustworthy, reliably forwarding signaling messages between Data BSs and the AMF.

We also assume that adversaries can modify, inject, or intercept messages in transit, posing threats to the proposed scheme. All Data BSs may be vulnerable to virus attacks or hijacking, allowing attackers to execute replay, impersonation, and MitM attacks. If encryption or session keys are compromised, the security of message transmission is at risk.

B. Our Scheme and Its Design Goals

In the proposed scheme, a lightweight group key negotiation technique based on secret sharing is first employed to establish a cooperation group of multi-BS, ensuring efficient and secure cooperation among them within the FD-RAN architecture. This group key is designated as UK. Subsequently, for individual UE accessing FD-RAN, the access key is derived from the BS group key UK to facilitate secure access. For multi-UE seeking access to FD-RAN, a flexible UE group is constructed with the CBE technique, and access requests are aggregated through the AMAD technique. During the access process, UE negotiate keys ξ with the CBS to ensure control plane data transmission. The secure key TUK between UE and the Data BS is derived by the AMF using the BS group key UK along with the identity and other information of the UEs. Our scheme aims to achieve the following objectives:

- Mutual Authentication and Key Negotiation: Initial authentication involves AUSF/UDM authenticating UE groups while the AMF authenticates Data BS groups, relaying results back to the AMF and CBS. The UE group must also verify the identities of AUSF/UDM, AMF, and CBS. When accessing a target Data BS, both the UE group and the Data BS's legitimacy must be confirmed. Additionally, a secure session key must be established to ensure confidentiality in subsequent transmissions. Sensitive data within the FD-RAN must remain protected, necessitating secure channels among Data BSs and between Data BSs and CBS during communication.
- Malicious Identity Detection: If the CBS cannot authenticate the UE group, it should refrain from issuing a direct authentication failure message. Instead, it must identify potentially malicious members and provide feedback to the group with a list of these identities. Similarly, the AMF should record any unverified members of the Data BS group and relay this information back.
- Anonymity and Traceability: UEs should operate under anonymous identities that are updated regularly. Only AUSF/UDM should be capable of computing these identities in case of disputes.
- Key Escrow Freedom (KEF): Each member of the UE and Data BS groups retains its key material, eliminating the need for a trusted third party outside the CN for key distribution.
- Resistance to Protocol Attacks: The proposed solution must withstand various protocol attacks, including replay attacks, impersonation attacks, MitM and DDoS attacks.
- Performance Optimization: To minimize authentication latency, we consider computational, communication, and transmission overheads. The overall performance of our multi-BS collaborative authentication and UE access authentication should surpass existing solutions.

IV. Preliminaries

This section introduces preparatory techniques employed. In Sections IV and V, several symbols related to the proposed mechanism and frequently utilized throughout the discussion are presented, as summarized in Table I.

A. Group Key Negotiation of Secret Sharing Technology

In our previous work [5], we focused on group key negotiation technology based on secret sharing to propose an AKA mechanism for FD-RAN. A group of nodes, such as Data BSs in the same area, negotiates a shared key with the help of a CBS. The n members send randomly selected values to the CBS, which securely forwards this information to the AMF. The AMF selects a group key UK and constructs an interpolation polynomial $f(x)$ of degree N, regenerating the n points for each member. Group members then recover UK through polynomial reconstruction, enabling secure intra-group communication and establishing trust among the BSs.

B. Contributory Broadcast Encryption Scheme

Multiple mobile devices belonging to the same user or within a trusted group often share similar mobility patterns

TABLE I
SYMBOLS USED IN OUR SCHEME

Notation	Definition
UE_i	the i-th user equipment. UE_h is the group leader
$SUCI_i$, $GUTI_i$	anonymous identity of UE_i
$SUPI_i$	identity of UE_i
ID_{UBS_i}	the identity of UBS_i
G	the UEs' group
F, h, h^*	the MAC and the hash function, respectively.
K_i	UE_i and AUSF/UDM own this key in advance
PK_i	the public key of UE_i in UE group
α_i	Group secret key of UE
χ, χ^T	χ is a $(l+1) \times n$ matrix, χ^T is its transpose
UK, TUK	UK is the group key of Data BS Group, TUK is the session key between UE and Data BS
(x_i, y_i), (u_i, v_i)	the secret value of UBS_i and UE_i respectively
m_i	message sent by UE_i
c_i	message authentication code of UE_i
$C = (C_1, C_2)$	the AMAC of UE group
AU_i	UE_i uses AU_i to verify the AUSF/UDM
MAC^i_{AMF}	The AMF message authentication code utilized for protecting integrity
CK_i, IK_i	encryption and integrity key obtained by UE_i
$\Lambda \in \{1, 2, ..., n\}$	the CBS communicates with UE_i in Λ
E	the encrypted text
ξ	session key of CBS and UE_i
δ	digital signature
ts, TS	timestamp
r, R	random number

* Subscription Permanent Identifier (SUPI), Subscription Concealed Identifier (SUCI), Globally Unique Temporary Identifier (GUTI).

and resource requests, enabling their collective grouping. This approach streamlines authentication and resource requests, significantly reducing wait times and wireless channel usage. Extensive research has focused on group formation and mobile gateway selection for such configurations [30]–[39]. In addition to communication, computational, and storage capabilities, selecting a secure mobile gateway UE_h should also consider factors like trust levels [40]–[42].

A proposed solution by [43] introduces a grouping mechanism where the next Generation Node B (gNB) leverages information from the SDN controller, such as distances between UEs to organize all UEs within its coverage area. This grouping information is then relayed to the trust-level superior UE_h, which broadcasts it to nearby members.

Wu et al. [44] presented a contributory broadcast encryption scheme, establishing a group key negotiation system among mutually authenticated members. Each member UE_i in group G receives a unique index $i (i \in M, M = 1, 2, \ldots, n)$. The process of CBE scheme is as follows:

- Group Key Negotiation (GKA): For $\omega \in M$, each UE_ω randomly selects $G_{i,\omega} \in G, s_{i,\omega} \in Z_p^*$ and computes $S_{i,\omega} = g^{-s_{i,\omega}}, M_{i,\omega} = e(G_{i,\omega}, g)$. The public key for UE_ω is then PK_ω = $((S_{0,\omega}, M_{0,\omega}), \ldots, (S_{n,\omega}, M_{n,\omega}))$. For $i = 0, \ldots, n, l \in M$, where $i \neq l$ and $l \neq \omega$, UE_ω computes $\mu_{i,l,\omega} = G_{i,\omega} h_l^{s_{i,\omega}}$ and sets $\alpha_{l,\omega} = (\mu_{0,l,\omega}, \ldots, \mu_{l-1,l,\omega}, \mu_{l+1,l,\omega}, \ldots, \mu_{n,l,\omega})$. After completing these calculations, UE_ω publicly sends $(PK_\omega, \alpha_{1,\omega}, \ldots, \alpha_{\omega-1,\omega}, \alpha_{\omega+1,\omega}, \ldots, \alpha_{n,\omega})$.
- Public Key Derivation (PKD): The public group key is computed as: $PK_G = ((S_0, M_0), \ldots, (S_n, M_n))$, where $S_i = \prod_{\omega=1}^n S_{i,\omega}, M_i = \prod_{\omega=1}^n M_{i,\omega}$ $(i = 0, \ldots, n)$ and the calculation is among the group key space.
- Decryption Key Derivation (DKD): UE_l will calculate the key: $\alpha_l = (\mu_{0,l}, \ldots, \mu_{l-1,l}, \mu_{l+1,l}, \ldots, \mu_{n,l})$ $(0 \leqslant i \leqslant n, l \in M, i \neq l)$, where $\mu_{i,l} = \mu_{i,l,l} \prod_{\omega=1,\omega\neq l}^n \mu_{i,l,\omega}$.

In the CBE scheme, new keys are generated in a homomorphic manner, meaning that when there are changes in the group members, all keys associated with the group can be maintained simply by modifying the key materials of the changing participants, thereby eliminating the complex process of regrouping. Once the above phases are completed, the group G will use the group key for secure communication.

C. Aggregate Message Authentication Code

[45] presents the AMAD scheme to improve information compression rates and detect erroneous MACs using j-degree double orthogonal codes. [24] employed the AMAD algorithm to construct an effective aggregation access scheme. We adopt the Construction II algorithm from [45] and describe it using the notation from the proposed mechanism. Let R be a comprehensive generating matrix of double orthogonal code with parameters $(n, \omega, \alpha_{min}) = (2^j, j + 1, 2^{j-1})$, where $j \geqslant 3$. Let Σ be the extended comprehensive generating matrix of R. Let $R_i = (R_{i,1}, \ldots, R_{i,n}) \in \{0,1\}^n$ $(i = 1, \ldots, j+1)$, and $\chi_i = (X_{i,1}, \ldots, X_{i,n}) = (R_{i,1}, \gamma R_{i,2}, \gamma^2 R_{i,3}, \ldots, \gamma^{n-1} S_{i,n})$, where γ belongs to $GF(2^h)$. The Construction II algorithm in the AMAD includes the operations $(KGen, Tag, Agg, TVrfy)$:

- KGen: Generate the key for initial authentication of UE with AUSF/UDM based on the UE's identity information.
- Tag: For each UE_i in the group, compute the tag $c_i = F(K_{ID_i}, m_i)$ with the MAC function, where m_i and K_{ID_i} are UE_i's message and key respectively.
- Agg: Given the tuples of senders $(ID_i, m_i, c_i) i \in M$ as inputs, calculate $C_1 = (C_{1,1}, C_{1,2}, \ldots, C_{1,j+1}) = cR^C$ and $C_2 = (C_{C,1}, C_{2,2}, \ldots, C_{2,j+1}) = c^* \chi^C$, where $c = (c_1, \ldots, c_n)$ and c_i^* is the last h bits of c_i. Then we get the aggregate message authentication code $C = (C_1, C_2)$.
- TVrfy:The receiver calculates $c = (c_1, \ldots, c_n) i \in M$ and verifies $r = C - cR^C$. If $r = 0$, the verification is passed; otherwise, it invokes the Construction II algorithm and output the list of malicious users.

V. PROPOSED SCHEME

This section introduces the detailed description of the proposed scheme, which consists of two parts: group key negotiation for Data BSs and FD-RAN access authentication, which is introduced separately for single UE access and multi-UE aggregated access to FD-RAN.

A. Data BS Group Key Negotiation

Since the group key negotiation process for uplink and downlink Data BSs is the same, for convenience, we will describe the process using the uplink Data BS UBS_i as an example, which does not affect our explanation. The process is shown in Fig. 3.

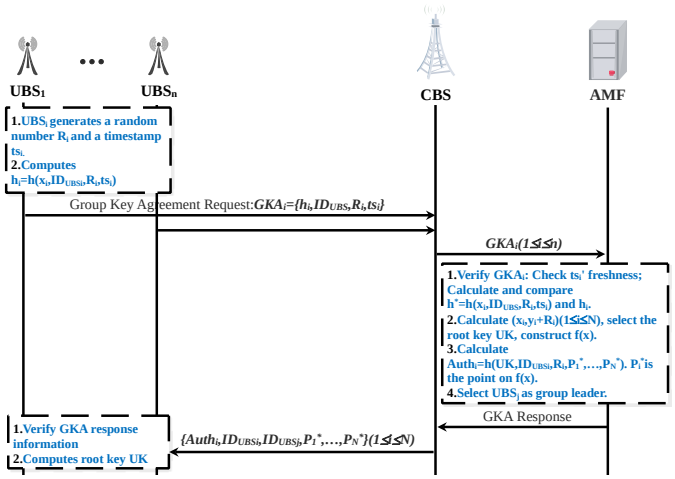


Fig. 3. Group Key Negotiation Process.

1) System Initialization Phase: During this phase, each UBS_i is authorized by the AMF, which acts as the group manager, and shares a secret value (x_i, y_i) with the AMF. In order to ensure security, these secret values are saved in trusted hardware configured within the AMF and Data BS, ensuring that adversaries cannot read the stored data.

2) Group Key Negotiation Phase: During this phase, the group key is shared between the AMF and each UBS_i of the group. The process is as follows:

- Each UBS_i generates a random number R_i and a timestamp ts_i, which are stored in a trusted secure hardware module. This module computes $h(x_i, ID_{UBS_i}, R_i, ts_i)$ and returns it to the Data BS UBS_i, where $h()$ is a hash function. The Data BS then sends a group key negotiation request to AMF via the CBS, formatted as:

$$GKA^i_{req} = \{h_i = h(x_i, ID_{UBS_i}, R_i, ts_i), \\ ID_{UBS_i}, R_i, ts_i\}. \quad (1)$$

- Upon receiving the request $GKA^i_{req}(1 \leqslant i \leqslant n)$, the AMF authenticates the data source and verifies its integrity. It computes $h^*(x_i, ID_{UBS_i}, R_i, ts_i)$ using the x_i saved locally along with the parameters $\{ID_{UBS_i}, R_i, ts_i\}$ that have been received, and compares h_i with the computed h^*. After verification, the AMF calculates the point $(x_i, y_i + R_i)$ for each authenticated UBS_i. Assuming all N BSs pass authentication, the AMF randomly selects a group key UK and constructs an N-degree interpolation polynomial $f(x)$ using $N+1$ points: $(0, UK)$ and $(x_i, y_i+R_i)(1 \leqslant i \leqslant N)$. The AMF selects N points P_i^* on $f(x)$ and computes

$$Auth_i = h(UK, ID_{UBS_i}, R_i, P_1^*, \ldots, P_N^*). \quad (2)$$

  It then broadcasts the key negotiation response $\{Auth_i, ID_{UBS_i}, ID_{UBS_j}, P_1^*, \ldots, P_N^*\}(1 \leqslant i \leqslant N)$ to all of the UBS_i in the group, where ID_{UBS_j} is the group leader designated by the AMF.
- Upon receiving the response, each UBS_i calculates $(x_i, y_i + R_i)$ using the trusted hardware module, and recovers the polynomial $f(x)$ using the point (x_i, y_i+R_i) and the received points $\{P_1^*, \ldots, P_N^*\}$ from AMF to retrieve the group key UK: $UK = f(0)$. Then, it computes $Auth_i^* = h(UK, ID_{UBS_i}, R_i, P_1^*, \ldots, P_N^*)$ and checks whether $Auth_i^*$ matches the $Auth_i$. If they match, UBS_i accepts UK; otherwise, it terminates the negotiation.

Upon completion, the N members of the UBS group use UK as a shared key for secure group communications. The Data BS UBS_j serves as the group leader for efficient information transmission, while secure interactions with CBS/AMF are conducted using UK. This negotiation establishes trust relationships within the CBS/AMF and the Data BS group, enabling secure subsequent interactions.

B. FD-RAN Access Authentication

The process for UE access to the FD-RAN can be divided into three primary steps: initialization, access authentication, and secure session establishment. Below, we detail the access authentication process for both multiple UEs and a single UE.

1) Initialization Phase

This phase primarily focuses on completing the initialization, including group key negotiation and the initial process.

1) Group Key Negotiation:

- The Data BS group negotiates a group key UK with the AMF by sharing secret values, establishing trust relationship within the group.
- UEs with similar access requirements and close proximity negotiate keys through CBE, securing the corresponding encryption and decryption keys.

2) Initial Process: Each legitimate UE_i is authorized by the AMF, which serves as administrator of the group. The UE_i and the AMF possess a common secret value (u_i, v_i) to facilitate access to the UBS_i. These secret values are securely stored in the UE's trusted hardware module, ensuring protection against adversaries.

2) Multi-UE Access Authentication

During the multi-UE access process, two main types of authentication occur: between the Data BSs, CBS, and UEs, as well as secure transmission of user data and control signaling. The process is described in Fig. 4.

Multi-UE access authentication consists of three steps:

Step 1: Initialization Phase

This stage completes the aforementioned initialization. For convenience, we use the uplink Data BS UBS as an example, which does not affect the analysis.

Step 2: Key Negotiation Phase

In this phase, multiple UEs establish trust with the CBS, AMF, and AUSF/UDM through AMAD and shared secret values, negotiating key ξ_i between UE_i and CBS_i. Simultaneously, UE_i sends an initial session key negotiation request to the AMF, sharing the initial session key TUK_i with UBS_i.

Step 2.1: UE Layer

- $UE_i \rightarrow UE_h : (m_i || c_i || GKA^{SUCI_i}_{req})$

Each UE_i uses $SUCI_i$ to conceal its identity, selecting a random number r_i and generating $m_i = (SUCI_i || PK_i || r_i)$ for authentication, in which PK_i is UE_i's public key calculated during the CBE negotiation of UEs. The message authentication code $c_i = F(K_i, m_i)$ is computed. Next,

UE_i generates a random number R_{UE_i} and a timestamp ts_{UE_i}, which are stored in the trusted secure hardware. The hardware calculates $h(u_i, SUCI_i, R_{UE_i}, ts_{UE_i})$ using secret values (u_i, v_i) and sends it back to UE_i. The initial session key negotiation request is generated as:

$$GKA_{req}^{SUCI_i} = \{h_i = h(u_i, SUCI_i, R_{UE_i}, ts_{UE_i}), SUCI_i, R_{UE_i}, ts_{UE_i}\}. \quad (3)$$

Finally, UE_i sends $(m_i||c_i||GKA_{req}^{SUCI_i})$ to UE_h.

- $UE_h \rightarrow AMF_1 : (M_G)$

As mentioned in section IV, after receiving messages from all UE_i, UE_h calculates $C_1 = cR^C$ where $c = (c_1, \ldots, c_n)$, and choose the last h bits of c_i to form c_i^* and set $c^* = (c_1^*, \ldots, c_n^*)c_i^* \in GF(2^h)$. UE_h computes $C_2 = c^*\chi^C$. Then, UE_h generates the AMAC $C = (C_1, C_2)$ and transmits the group authentication information M_G to the AMF.

$$M_G = (m_1||\ldots||m_n||GKA_{req}^{SUCI_1}||\ldots||GKA_{req}^{SUCI_n}||C||PK_G). \quad (4)$$

Step 2.2: Control Plane

- $AMF \rightarrow AUSF/UDM : (M_G||ID_{AMF})$

The AMF retains

$$GKA_{req}^{G} = \{GKA_{req}^{SUCI_1}||\ldots||GKA_{req}^{SUCI_n}\} \quad (5)$$

and forwards $(M'_G||ID_{AMF})$ (where M'_G does not contain GKA from M_G) to $AUSF/UDM$.

- $AUSF/UDM \rightarrow AMF : (AU_G = (AU_1||\ldots||AU_n||r_{HN}))$

a) Upon the receipt of the message: $AUSF/UDM$ retrieves UE_i's true identity $SUPI_i$ associated with $SUCI_i$ and checks it. Based on K_i and m_i, $AUSF/UDM$ calculates c_i and get $c = (c_1, \ldots, c_n)$. Subsequently, it checks $r = C = cR^C$. If $r = 0$, then the authentication for group G is successful. Otherwise, it will invoke the Construction II algorithm to generate the index catalog J matching deleterious the UEs in G.

b) Upon UE group G authenticated: $AUSF/UDM$ generates new temporary identity $GUTI_i = h(SUPI_i, r_i, ID_{AMF})$ for all UE_i. It then selects a random number r_{HN} and computes CK_i, IK_i, K_{AUSF}^i and K_{AMF}^i. Finally, it generates the UE authentication signaling AU_i and the group authentication token AU_G.

$$\begin{aligned} CK_i &= f_2(K_i, r_{HN}), \\ IK_i &= f_3(K_i, r_{HN}), \\ K_{AUSF}^i &= KDF(CK_i, IK_i, ID_{AMF}, SUPI_i), \\ K_{AMF}^i &= KDF(K_{AUSF}^i, ID_{AMF}), \\ AU_i &= ((r_i, SUPI_i)_{K_{AUSF}^i}, K_{AMF}^i, GUTI_i), \\ AU_G &= (AU_1||\ldots||AU_n||r_{HN}). \end{aligned} \quad (6)$$

- $AMF \rightarrow CBS_1 : (AUTH_G = (AUTH_1||\ldots||AUTH_n||PK_G||r_{HN}||GKA_{res}^{SUCI_G}))$

Once receiving the token AU_G, AMF retains legitimate UEs' requests in GKA_{req}^G to generate key for UBS authentication and session. To simplify clarity, let's assume that all UEs in the group are authenticated as legitimate by $AUSF/UDM$. After retrieving $GKA_{req}^{SUCI_i}$, AMF first verifies access UBS authorization and data integrity. In this process, AMF computes $h^*(u_i, SUCI_i, R_{UE_i}, ts_{UE_i})$ using the locally stored u_i and the received parameters $\{SUCI_i, R_{UE_i}, ts_{UE_i}\}$, comparing h_i with the computed h^*. For convenience, let's assume that UE_i passes authentication. AMF then computes the point $(u_i, v_i + R_{UE_i})$ for UE_i, assigns servicing UBS group for UE, and derives the UBS group key UK, obtaining $TUK_i = KDF(UK, GUTI_i, ts_{new})$ where ts_{new} is a timestamp. Then it constructs the polynomial $U(x)$ with $(0, TUK_i)$ and $(u_i, v_i + R_{UE_i})$. Next, it selects a point Q_i^* on $U(x)$ and computes $Auth_{UE_i} = h(TUK_i, GUTI_i, ts_{new}, R_{UE_i}, Q_i^*)$ to obtain $Auth_G$ for the UE group. Finally, it generates the session key negotiation response information $GKA_{res}^{GUTI_G} = \{Auth_G, GUTI_G, ts_{new}^G, R_{UE_G}, Q_G^*\}$ and sends

$$h_{new} = \{ENC_{UK}(SUCI_G, GUTI_G, ts_{new}^G), ts_{new}^G\} \quad (7)$$

to the corresponding UBS group, which can decrypt it to use $SUCI_i$ along with UK to obtain the session key TUK_i. Afterward, AMF retains K_{AMF}^i, calculates $MAC_{AMF}^i = f_1(K_{AMF}^i, r_{HN}, r_i, (r_i, SUPI_i)_{K_{AUSF}^i})$ and computes $AUTH_i = (MAC_{AMF}^i, GUTI_i)$ for each $GUTI_i$, ultimately sending the token $AUTH_G = (AUTH_1||\ldots||AUTH_n||PK_G||r_{HN})$ and $GKA_{res}^{GUTI_G}$ to CBS_1.

- $CBS_1 \rightarrow UE_h : (AUTH_G||GKA_{res}^{GUTI_G}||ID_{CBS_1}||\delta||E||\Lambda||TS_1)$

Upon receiving $AUTH_G$, CBS_1 considers that UE group G has been accepted as genuine. Currently, CBS_1 can interact with several members of the group, and these members form a set $\Lambda \in \{1, 2, ..., n\}, \bar{\Lambda} = \{0, 1, ..., n\}/\Lambda$. Then, CBS_1 randomly selects $\tau \in Z_p^*$ and computes the ciphertext $E = (e_1, e_2)$ where $e_1 = g^\tau$ and $e_2 = (\prod_{i \in \bar{\Lambda}} S_i)^\tau$. The session key of CBS_1 and the members in Λ is given by $\xi_i = (\prod_{i \in \bar{\Lambda}} M_i)^\tau$. Finally, CBS_1 signs the authentication data using its private key and forwards δ to UE_h: $\delta = (ID_{CBS_1}||TS_1||E||\Lambda||GKA_{res}^{GUTI_G}||AUTH_G)_{SK_{CBS_1}}$ where TS_1 denotes a timestamp produced by CBS_1.

Step 2.3: UE Layer

- *Generate Secure Key δ for UE and CBS*:

Upon receiving the message, UE_h first verifies the freshness of TS_1 then broadcasts to group G. Each UE_i calculates $CK_i, IK_i, K_{AUSF}^i, K_{AMF}^i$ similarly to $AUSF/UDM$ and validates the accuracy of $AUTH_i$ and ξ. When all validations are confirmed, UE_i deems $AUSF/UDM, AMF$, and CBS_1 to be legitimate. At this moment, mutual authentication is complete among these entities, and UE_i applies α_i to derive the key with CBS from the ciphertext E:

$$\xi_i = e(\sigma_{0,i}, e_1)e(h_i, e_2). \quad (8)$$

- *Generate Secure Key TUK_i for UE and UBS*:

Upon receiving $GKA_{res}^{GUTI_i}$, UE_i computes the point $(u_i, v_i + R_{UE_i})$ with the trusted hardware module. Subsequently, UE_i recovers $U(x)$ with $(u_i, v_i + R_{UE_i})$ and the received point Q_i^*, thereby obtaining the initial session key $TUK_i = U(0)$. Afterward, UE_i computes

$Auth^*_{UE_i} = h(TUK_i, GUTI_i, ts_{new}, R_{UE_i}, Q^*_i)$ and checks whether $Auth^*_{UE_i}$ matches the received $Auth_{UE_i}$. If the two values are equal, UE_i believes the initial session key is trustworthy; otherwise, UE_i terminates the key negotiation.

After ***Step 2***, UE_i, UBS group, and AMF retain $GUTI_i$. UE_i confirms trust relationship and generates session key ξ for interaction with CBS_1. Simultaneously, UE_i and UBS_i independently generate the initial access and session key TUK_i. In ***Step 3***, UBS_i verifies the accessing UE_i through TUK_i and completes the secure session.

Step 3: Data BS Secure Access and Session

In this study, the downlink and uplink mechanisms are the same. Using the uplink as an example, we describe the situation where the UE group accesses the UBS group:

Step 3.1: Multi-UEs Session with UBS

- $UE_i \rightarrow UE_h : (Message_e||ts_{new_e}||GUTI_i||R_{AC_i})$

UE_i requires different keys for different UBS and completes the process by deriving key $TUK_{i,i}$

$$TUK_{i,i} = KDF(TUK_i, GUTI_i, R_{AC_i}, ts_{new_e}), \quad (9)$$

where R_{AC_i} and ts_{new_e} are random number and timestamp generated by UE_i. Different keys are generated by different random numbers. Each UE_i accesses UBS with $GUTI_i$ to prevent the leakage of real identity. UE_i generates the authentication message $AC_i^{UBS} = (ENC_{TUK_{i,i}}(Message_e)||ts^i_{new_e}||GUTI_i||R_{AC_i}||PK_i)$, where PK_i is the public key of UE_i, and $Message_e$ is the initial session information. Afterward, each member of the UE group G sends its AC_i^{UBS} to UE_h. This step can be executed offline.

- $UE_h \rightarrow UBS_j : AC_{req}$

After receiving AC_i^{UBS} and decrypting it, UE_h reorganizes the information and sends an access request for group G to any UBS_x. This request includes the group access authentication requests and session information encrypted with the TUK of each UE. The two pieces of information are aggregated into:

$$\begin{aligned} AC_{req} = \{&ENC_{TUK_G}(Message_G), h_{UE_h} = \\ &h(TUK_{h,h}, GUTI_h, R_{AC_h}, ts^h_{new_e}), \\ &GUTI_G, GUTI_h, R_{AC_G}, ts^G_{new_e}\}. \end{aligned} \quad (10)$$

- $UBS_x \rightarrow UBS : ENC_{UK}\{ENC_{TUK_{x,x}}(Message), GUTI_x, ts^x_{new_e}, R_{AC_x}\}$

Upon receiving AC_{req}, UBS_x retrieves the corresponding UE_h information sent by AMF and derive UK to obtain TUK_h. Then, it obtains the key $TUK_{h,h}$ with TUK_h and the received information. By computing $h^* = h(TUK_{h,h}, GUTI_h, R_{AC_h}, ts^h_{new_e})$, UBS_x compares h^* with h_{UE_h} for verifying data source and data integrity. If the verification is successful, the legitimacy of group G is confirmed, and UE_h can session with UBS_x using $TUK_{h,h}$. Subsequently, UBS group leader UBS_j allocates UEs and sends the corresponding information $ENC_{UK}\{ENC_{TUK_{x,x}}(Message), GUTI_x, ts^x_{new_e}, R_{AC_x}\}$ to different UBSs based on their transmission capabilities.

- UBS_i *Generates* $TUK_{i,*}$ *and Receives* $Message^*_e$:

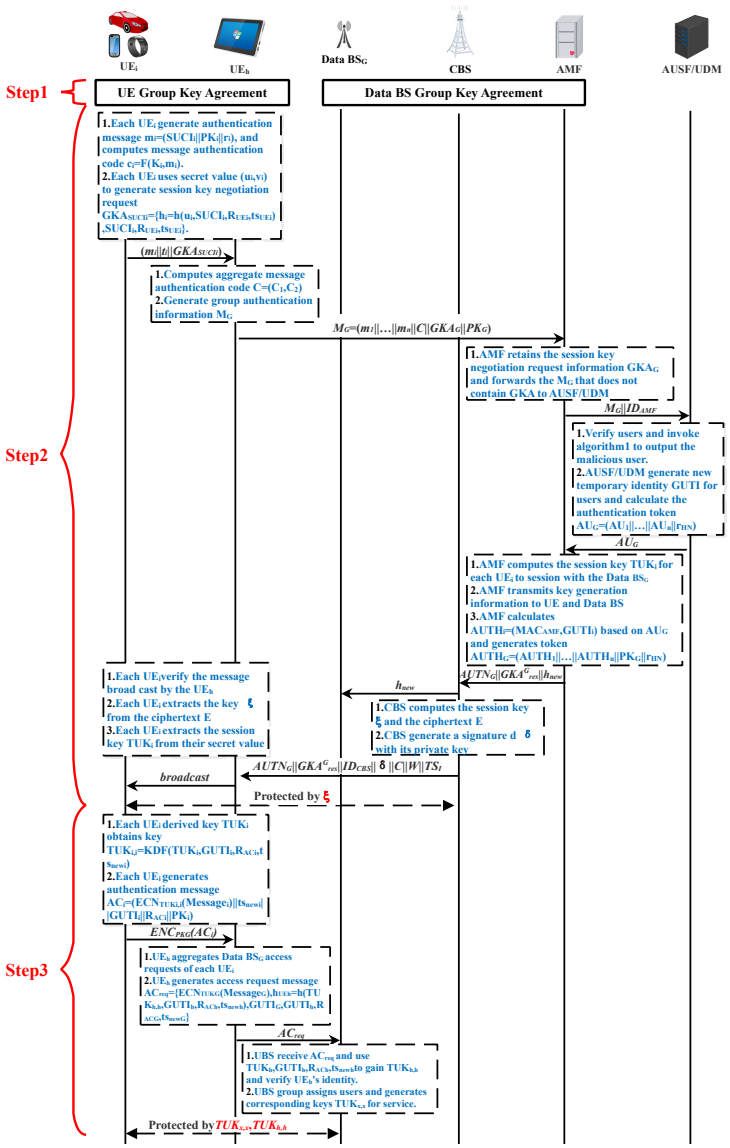


Fig. 4. Multi-UE Access Process in FD-RAN.

When any data BS uses UK to decrypt the information $\{ENC_{TUK_{x,x}}(Message), GUTI_x, ts^x_{new_e}, R_{AC_x}\}$ assigned by UBS_j, it first assumes that the data source is legitimate and the data is intact. Then, based on $GUTI_x$, it generates the key TUK_x, and together with $GUTI_x, R_{AC_x}, ts^x_{new_e}$, it obtains the key $TUK_{x,x}$. After that, it uses $TUK_{x,x}$ to decrypt the session information $Message_x$. If decryption fails, it reports the abnormal UE to CBS. If decryption is successful, it subsequently communicates with UE_x with $TUK_{x,x}$.

In summary, this completes the aggregate access authentication and secure session of the UE group with the data BS group, achieving 0-RTT access authentication.

Step 3.2: Multi-UEs Session with DBS

In the FD-RAN architecture, it is common for a single DBS to serve multi-UE. Therefore, different keys are needed to encrypt data between DBS and different UEs. The session between DBS and multi-UE is actually a session between a single UE and DBS, and the process is as follows:

- DBS_i session with UE_i securely: The first data sent from DBS_i to UE_i must be encrypted with $TUK_{DBS_i} = KDF(TUK_i, GUTI_{UE_i}, ID_{DBS_i}, ts_{DBS_i}, R_{DBS_i})$, where ts_{DBS_i} and R_{DBS_i} are the timestamp and random number generated by DBS_i, and TUK_i is generated by DBS_i based on $GUTI_{UE_i}$.
- The data sent to UE_i takes the form: $\{\{Message_D, ts_{DBS_i}, R_{DBS_i}, GUTI_{UE_i}, ID_{DBS_i}\}_{TUK_{DBS_i}}, ts_{DBS_i}, R_{DBS_i}, GUTI_{UE_i}, ID_{DBS_i}\}$.
- After UE_i receives the above information, It can generate TUK_{DBS_i} by combining ts_{DBS_i},R_{DBS_i},$GUTI_{UE_i}$,ID_{DBS_i} with TUK_i, then it can decrypt and obtain the corresponding information.

Thus, different DBS_i use different keys to conduct secure sessions with different UE_i.

3) Single UE Access Authentication

The access of a single UE can also be divided into three steps: initialization, key negotiation, and Data BS group secure session. The specific procedure is the same as that for the multi-UE case with UE_h, except that there is no need for group negotiation among UEs. Instead, the single UE directly interacts with the AMF to obtain the key TUK with the UBS by constructing an interpolation polynomial. Due to space limitations, this process will not be elaborated upon here.

VI. Security Analysis

This section conducts a security analysis of the proposed scheme and verifies it with the formal model of BAN logic.

A. Security Analysis:

1) Mutual Authentication: In the proposed scheme, each UE_i computes CK_i, IK_i, K^i_{AUSF}, and K^i_{AMF} similarly to AUSF/UDM, verifying the correctness of $AUTH_i$ and δ to ensure mutual authentication among UE_i, CBS, AMF, and AUSF/UDM. This mutual authentication extends to the target Data BS group. Legitimate UEs can upload or download data through the Data BS, which verifies UE_i by checking $TUK_{i,i} = KDF(TUK_i = KDF(UK, SUCI_i, ts_{new}), GUTI_i, R_{AC_i}, ts_{new_e})$, with UK being the shared key of the Data BS group. Only UEs validated by AMF can derive the initial session key TUK_i for encryption and decryption of user plane data. Additionally, UE_i verifies DBS_i by ensuring received data is encrypted with TUK_i or its derived keys, confirming that only legitimate DBS_i can decrypt $h_{new} = \{h_{UK}(ID_{UE_i}, ts_{new}), ts_{new}\}$ to obtain TUK_i with UK. Thus, the scheme ensures mutual authentication between UEs and the target Data BS group.

2) Key Negotiation: In our scheme, during access authentication to CBS, CBS randomly selects $\tau \in Z_p^*$ to generate unique ciphertexts C and session keys ξ. Subsequently, UE_i uses the decryption key d_j to extract material from C and generate ξ_i, enabling secure interaction between both parties. During access to the Data BS, UE_i negotiates the initial session key TUK_i with AMF using the secret value (u_i, v_i). The target Data BS group then negotiates the shared group key UK with AMF, allowing each Data BS to derive TUK_i from UK, $SUCI_i$, and ts_{new}. Only legitimate UEs and Data BS can generate and obtain TUK_i, ensuring secure session establishment. Additionally, adversaries cannot access key materials, as keys are computed independently at each end without transmission over any link.

3) Resistance to Eavesdropping Attacks: The information for generating key ξ_i is embedded in ciphertext C and encrypted with CBS's key before being sent to UE_i. Upon receiving the corresponding information δ, UE_i uses its decryption key to extract the material needed for key generation and combines it with its secret value $\delta_{0,i}$ to derive ξ_i. In this process, adversaries are unable to obtain the key due to their lack of both the decryption key and the secret value. The information for generating TUK_i is encrypted by AMF with the shared group key UK and encapsulated in $h_{new} = \{ENC_{UK}(ID_{UE_i}, ts_{new}), ts_{new}\}$. Even if intercepted, adversaries cannot derive TUK_i since UK remains unknown to them. Additionally, keys protecting sensitive information is not conveyed through communication channels and secret values are not accessible, thwarting eavesdropping attempts.

4) Resistance to Replay Attacks: Adversaries often attempt to intercept and replay messages. However, if the timestamps in the reply messages are checked and found invalid, authentication fails. Timestamp values cannot be altered or replaced, as they are hashed to derive key negotiation information like $Auth_{U_i}$ and h_{new}. Thus, by verifying the validity of timestamps and key negotiation data, replay messages can be easily detected. UE group members generate message authentication codes with random numbers r_i to ensure freshness. CBS also employs timestamp TS to maintain message freshness during authentication, further thwarting replay attacks. The security of the group key protocol relies on the n-BDHE assumption, proven to resist collaborative attacks [45]. Additionally, the proposed scheme enables multi-UE authentication, contributing to the mitigation of DDoS attacks as well.

5) Resistance to Man-in-the-Middle (MitM) Attacks: During the UE access to CBS process, all authentication data are secured using shared keys, hash functions, or digital signatures, ensuring confidentiality and integrity while resisting impersonation and MitM attacks. During the interaction between UE and Data BS, a MitM attacker is unable to extract the initial session key TUK_i by eavesdropping on the public data of the wireless communication link, as TUK_i is generated from key UK once mutual authentication is successfully achieved. As a result, an attacker finds it impractical to carry out a MitM attack to compromise an established connection. Additionally, an attacker cannot create valid key negotiation request information without sharing secret values (x_i, y_i) or (u_i, v_i). Therefore, it is impossible for anyone to pretend to be legitimate Data BSs or UEs.

6) Anonymity and Traceability: UE_i initiates the initial authentication with the anonymous identity $SUCI_i$. Once the group authentication is successful, to ensure anonymity, AUSF/UDM applies a hash function to derive a new temporary identity $GUTI_i = h(SUPI_i, r_i, ID_{AMF})$ for all members. When the data base station group is updated, UE_i updates its $GUTI_i$, ensuring that the user's temporary identity is known only to the data base stations providing the service. AUSF/UDM then transmits the generated $GUTI_i$ to the target

AMF. In contentious situations, the one-wayness and crash avoidance properties of the hash function can demonstrate that only valid AUSF/UDM knows the user's real identity and can trace the process of how the $GUTI_i$ was computed to clarify the user's identity.

7) Perfect Forward/Backward Secrecy (PFS/PBS): In step 2.2, step 4 of Section V, CBS randomly selects $\tau \in Z_p^*$ to calculate unique ciphertexts and keys. The decryption key α_l is applied to generate the key from ciphertext E:

$$\begin{aligned} \xi = e(\mu_{0,l}, e_1)e(h_l, e_2) = e(\prod_{\omega=1}^{n} G_{0,\omega} h_l^{s_{0,\omega}}, g^{\tau}) \cdot \\ e(h_l, \prod_{\omega=1}^{n} S_{0,\omega^{\tau}}) = \prod_{\omega=1}^{n} e(G_{0,\omega}, g) = (M_0)^{\tau} = \xi. \end{aligned} \tag{11}$$

If the current decryption key α_l of UE_l is compromised, an adversary must extract $\mu_{0,l} = \prod_{\omega=1}^{n} G_{0,\omega} h_l^{s_{0,\omega}}$ from α_l. While the adversary is aware of $s_{0,l}$, the other $s_{0,\omega}(\omega \in M)$ are securely calculated and stored by the other $n-1$ members. Our scheme maintains a secure authentication link, rendering it impractical for all group members' secret parameters $s_{0,\omega}$ to be compromised. Thus, the adversary cannot extract $\mu_{0,l}$ or session keys from prior or future ciphertexts. Overall, the scheme ensures PFS and PBS.

8) Malicious UE Detection: In most authentication schemes, a group authentication failure denies network access to all members. In contrast, the proposed scheme utilizes AMAD to identify malicious members. If $s \neq 0$, it indicates that some members of M_G have sent harmful messages. The receiver can then use Construction II to recognize and enumerate these malicious identities, thereby aiding the group in troubleshooting and enhancing robustness. According to [45], the detection scheme with AMAD can achieve high data compression and effective malicious UE detection rates.

B. BAN Logic Verification

BAN logic [46] is a formal model extensively utilized to evaluate the security of authentication protocols. In this subsection, we apply this model to prove authentication and present how our scheme of access authentication meets security objectives. Since the security processes of UBS and DBS are identical, we focus on verifying the security of UE accessing UBS. Table II lists the symbols and logical assumptions used in our BAN logic analysis. To analyze BAN logic, the first step is to establish security goals based on the proposed scheme. Next, the initial authentication messages are outlined, excluding those irrelevant to the protocol's security proof. To enhance authentication security, group members UE_i authenticate both CBS and AMF using the authentication token $AUTH_i$, and $AUSF/UDM$ using AU_i. It is believed that a secure link exists between CBS, AMF, and $AUSF/UDM$. Then, once security hypotheses are established, logical reasoning verification can proceed.

1) Security Goals: The proposed scheme is required to achieve mutual identity verification between UE_i and $AUSF/UDM$, as well as CBS. So, the security goals are:

- G1. $AUSF/UDM| \equiv UE_i| \equiv m_i$

TABLE II
SYMBOLS AND LOGICAL RULES

Symbole	Description
$P\| \equiv X$	P trust X
$P \lhd X$	P can see X
$\sharp X$	X's id is fresh
$P\| \sim X$	P mentioned X
$P \mid\Longrightarrow X$	P manage X
(X,Y)	X,Y is a part of (X,Y)
$\{X\}_K$	X is encrypted by key K
$P \overset{K}{\longleftrightarrow} Q$	P,Q communicate with the key K
Rules	**Formular**
R1.1 Message meaning rule	$\frac{P\|\equiv P \overset{K}{\longleftrightarrow} Q, P\lhd\{X\}_K}{P\|\equiv Q\|\sim X}$
R1.2	$\frac{P\|\equiv P \overset{K}{\longrightarrow} Q, P\lhd\{X\}_{K^{-1}}}{P\|\equiv Q\|\sim X}$
R2 Random verification rule	$\frac{P\|\equiv \sharp(X), P\|\equiv Q\| \sim X}{P\|\equiv Q\|\equiv X}$
R3 Decomposition rule	$\frac{P\|\equiv (X,Y)}{P\|\equiv X}$
R4 Message sending rule	$\frac{P\|\equiv Q\|\sim (X,Y)}{P\|\equiv Q\|\sim X}$
R5 Message receiving rule	$\frac{P\lhd (X,Y)}{P\lhd X}$
R6 Freshness enhancement rule	$\frac{P\|\equiv \sharp(X)}{P\|\equiv \sharp(X,Y)}$
R7 Application of jurisdiction rule	$\frac{P\|\equiv (Q\|\Longrightarrow X) , P\|\equiv (Q\|\equiv X)}{P\|\equiv X}$

- G2. $UE_i| \equiv CBS| \equiv E$
- G3. $UE_i| \equiv AMF| \equiv AUTH_i$
- G4. $UE_i| \equiv AUSF/UDM| \equiv AU_i$
- G5. $UBS_i| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- G6. $UBS_i| \equiv UE_i \mid\equiv UE_i \overset{TUK_{i,i}}{\longleftrightarrow} UBS_i$

2) Protocol Idealization: To facilitate derivation, the communication messages of the proposed scheme are converted into an idealized form, as follows:

- Message 1: $UE_i \longrightarrow AMF$: Initial session key negotiation request information:

$$\begin{aligned} AMF \lhd \{\{UE_i \overset{(u_i,v_i)}{\longleftrightarrow} AMF, SUCI_i, R_{U_i}, \\ ts_{u_i}\}_h, GUTI_i, R_{U_i}, ts_{u_i}\}. \end{aligned} \tag{12}$$

- Message 2: $UE_i \longrightarrow AUSF/UDM$:

$$\begin{aligned} AUSF/UDM \lhd \{m_i = (SUCI_i || PK_i || r_i), \\ c_i = F(K_i, m_i), PK_i, ID_{AMF}\}. \end{aligned} \tag{13}$$

- Message 3: $AUSF/UDM \longrightarrow UE_i$:

$$\begin{aligned} UE_i \lhd \{AU_G = (AU_i = (K^i_{AMF}, GUTI_i, (r_i, \\ SUPI_i)_{K^i_{AUSF}}))||r_{HN}\}. \end{aligned} \tag{14}$$

- Message 4: $AMF \longrightarrow UE_i$: Initial session key negotiation response information:

$$\begin{aligned} UE_i \lhd \{GUTI_i, R_{U_i}, ts_{new}, {Q_i}^*, \{GUTI_i, R_{U_i}, \\ ts_{new}, {Q_i}^*, UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i\}_h, \{AUTH_G = \\ (MAC_{AMF^i}, GUTI_i)||PK_G||r_{HN}\}\}. \end{aligned} \tag{15}$$

- Message 5: $AMF \longrightarrow UBS_i$: Transmission of initial session key generation information:

$$UBS_i \lhd \{\{ts_{new}, GUTI_i, UBS_i \overset{TUK_i}{\longleftrightarrow} UE_i\}_{UK}\} \tag{16}$$

- Message 6: $CBS \longrightarrow UE_i$:

$$UE_i \triangleleft \{AUTH_G||ID_{CBS}||\delta||E||\Lambda||TS_1\} \quad (17)$$

- Message 7: $UE_i \longrightarrow UBS_i$: Secure Access and Sessions:

$$UBS_i \triangleleft \{GUTI_i, ts_{new_u}, R_{AC_i}, \{GUTI_i, ts_{new_u}, R_{AC_i}, UBS_i \overset{TUK_{i,i}}{\longleftrightarrow} UE_i\}_{TUK_i}, \{Message_u\}_{TUK_{i,i}}\}. \quad (18)$$

3) Security Assumption: The initial assumptions guarantee the successful logical analysis of the proposed scheme. Consequently, the following assumptions are made regarding the initial state of the scheme:

- A1. $AUSF/UDM| \equiv UE_i \overset{K_i}{\longleftrightarrow} AUSF/UDM$
- A2. $UE_i| \equiv \overset{PK_{CBS}}{\longrightarrow} CBS$
- A3. $AUSF/UDM| \equiv \sharp(r_i)$
- A4. $UE_i| \equiv \sharp(TS_1)$
- A5. $UE_i| \equiv \sharp(r_{HN})$
- A6. $UE_i| \equiv UE_i \overset{K^i_{AMF}}{\longleftrightarrow} AMF$
- A7. $UE_i| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- A8. $UE_i| \equiv AMF \overset{UK}{\longleftrightarrow} UBS_i$
- A9. $UBS_i| \equiv AMF \overset{UK}{\longleftrightarrow} UBS_i$
- A10. $UBS_i| \equiv \sharp(ts_{new})$
- A11. $UBS_i| \equiv (UE_i/AMF| \Longrightarrow UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i)$
- A12. $UE_i| \equiv \sharp(ts_{new})$
- A13. $UBS_i| \equiv \sharp(ts_{new_u})$
- A14. $GM| \equiv \sharp(ts_{u_i})$
- A15. $UE_i| \equiv \sharp(R_{U_i})$
- A16. $UBS_i| \equiv \sharp(R_{AC_i})$
- A17. $AMF| \equiv \sharp((u_i, v_i))$
- A18. $AMF| \equiv UE_i \overset{(u_i,v_i)}{\longleftrightarrow} AMF$

4) BAN Logical Verification: On the basis of the idealized message and hypothesis, the scheme is analyzed. The following is the main proof procedure:

- According to message 2, applying R5 yields: S1. $AUSF/UDM \triangleleft t_i$
- From S1, A1, and the message meaning rule R1.1, we obtain: S2. $AUSF/UDM| \equiv UE_i| \sim m_i$
- From M2, A3, and the freshness enhancement rule R6, we derive: S3. $AUSF/UDM| \equiv \sharp(m_i)$
- From S2, S3, and the single verification rule R2, we get: S4. $AUSF/UDM| \equiv UE_i| \equiv m_i$ **(Goal 1)**
- According to M6 and the message reception rule R5, we have: S5. $UE_i \triangleleft \delta$
- From S5 and A2, applying R1.2 yields: S6. $UE_i| \equiv CBS| \sim (ID_{CBS}, TS_1, E, \Lambda, AUTH_G)$
- From S6 and the message sending rule R4, we know: S7. $UE_i| \equiv CBS| \sim E$
- From M6, A4, and the freshness enhancement rule R6, we infer: S8. $UE_i| \equiv \sharp(AUTH_G, ID_{CBS}, \delta, E, \Lambda, TS_1)$
- According to S8, applying R3 yields: S9. $UE_i| \equiv \sharp(E)$
- From S7 and S9, applying R2 yields: S10. $UE_i| \equiv CBS| \equiv E$ **(Goal 2)**
- Using S6 and the message sending rule R4, we obtain: S11. $UE_i| \equiv CBS| \sim AUTH_i$
- From M4, we know that $AMF| \Longrightarrow AUTH_G$, and it is believed that a secure link is established among CBS, AMF, and $AUSF/UDM$, so S11 can be considered as: S12. $UE_i| \equiv AMF| \sim AUTH_i$
- From S8 and the decomposition rule R3, we have: S13. $UE_i| \equiv \sharp(AUTH_i)$
- From S12 and S13, applying R2 yields: S14. $UE_i| \equiv AMF| \equiv AUTH_i$ **(Goal 3)**
- According to M4, applying R5 yields: S15. $UE_i \triangleleft MAC^i_{AMF}$
- With the above S15 and the established assumption A6, we can apply R1.1 to derive: S16. $UE_i| \equiv AMF| \sim (K^i_{AMF}, GUTI_i, r_{HN}, r_i, (r_i, SUPI_i)_{K^i_{AUSF}})$
- According to S16, applying R3 yields: S17. $UE_i| \equiv AMF| \sim AU_i$
- From M3, we know that $AUSF/UDM| \Longrightarrow AU_G$. It is also assumed that a secure link is existed between AMF and $AUSF/UDM$, so S17 can be considered as: S18. $UE_i| \equiv AUSF/UDM| \sim AU_i$
- According to message 3 and A5, applying R6 and R3 yields: S19. $UE_i| \equiv \sharp(AU_i)$
- From S18, S19, and the single verification rule R2, we can prove: S20. $UE_i| \equiv AUSF/UDM| \equiv AU_i$ **(Goal 4)**
- According to message 3 and A3, applying R1 yields: S21. $UBS_i| \equiv AMF| \sim \{GUTI_i, ts_{new}, UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i\}$
- According to S2 and A4, applying R2 yields: S22. $UBS_i \mid \equiv AMF| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$
- According to S3 and A5, applying R3 yields: S23. $UBS_i| \equiv UE_i \overset{TUK_i}{\longleftrightarrow} UBS_i$ **(Goal 5)**
- According to message 4 and S4, applying R1 yields: S24. $UBS_i| \equiv UE_i| \sim \{GUTI_i, R_{AC_i}, ts_{new_u}, UE_i \overset{TUK_{i,i}}{\longleftrightarrow} UBS_i\}$
- According to S5 and A7, A10, applying R2 yields: S25. $UBS_i| \equiv UE_i| \equiv UE_i \overset{TUK_{i,i}}{\longleftrightarrow} UBS_i$ **(Goal 6)**

Through the assumptions and logical rules performed, the idealized protocol is derived: through $S4, S10, S14, S20, S23$, and $S25$, the goals are proven, concluding that the keys ξ, TUK_i, and $TUK_{i,i}$ are secure during the access process. Thus, the validity of the proposed scheme is verified.

VII. Performance Evaluation

In this section, we compare the proposed scheme with existing typical single-UE and multi-UE authentication schemes in the context of FD-RAN multi-BS cooperative access authentication. The comparison is conducted from the perspectives of computational overheads, communication overheads, transmission overheads, and a comprehensive functional comparison. To ensure a fair comparison, the entities engaged in access process are represented as UE, Service Network (SN: Data BS/CBS/AMF), and Home Network (HN: AUSF/UDM).

A. Computational Overhead

The computational overheads of the proposed scheme is defined as the time cost of the cryptographic operations

involved. We perform raw cryptographic operations using the OpenSSL library on a 13th Gen Intel(R) Core(TM) i9-13900HX 2.20 GHz processor. We installed Ubuntu version 24.04.1 LTS on this computer and subsequently compiled and ran the C/C++ OPENSSL library within the Linux environment. Finally, using the OPENSSL library, we assessed the time cost of the cryptographic operations utilized in both the proposed protocol and the comparative protocols. To enhance the accuracy of the experimental data, we conducted 10 trials for each cryptographic operation. In each trial, we executed the operations 500 times to obtain the average runtime. The results are presented in Table III. The analysis focuses solely on

TABLE III
COMPUTATIONAL OVERHEAD OF CRYPTOGRAPHIC OPERATIONS

	T_P	T_{ME}	T_{SM}	T_{RV}	T_H
UE	2.87	0.225	0.2025	0.127	0.0013
BS	0.7616	0.0337	0.030	0.019	0.00079

the computational costs of the encryption processes outlined in Table III, where T_P, T_{ME}, T_{SM}, T_{RV}, and T_H denote the overheads for pairing operations, modular exponentiation, elliptic curve scalar multiplication, RSA signature verification, and single hash or MAC operations, respectively.

In Table IV, we compare the proposed scheme's computational overheads with various single-UE schemes (SD-SIN [12], Robust [15], UHAEN [16], CPPHA [27], Scheme in [24], ReHand [29], 5G-AKA [6]) and multi-UE schemes (FTGPHA1 [13], FTGPHA2 [13], UGHA [14], SEGR [17], Scheme in [24]). Here, T_{tot} represents the total overheads for m UEs accessing n Data BSs. The computational overheads is visually represented across three FD-RAN scenarios: 1) Total overheads varies with the number of cooperating Data BSs, n, for a single UE; 2) Total overheads varies with n while keeping the number of UEs m fixed; 3) Total overheads varies with m while n is fixed. We multiply the computational overheads of the single-UE schemes by the number of UEs and BSs corresponding to the specific scenario in order to facilitate a comparison with the multi-UE, multi-BS access schemes. The results for these schemes are shown in (a), (b), (c) in Fig. 5, with the proposed scheme indicated by a red pentagram dashed line. The proposed scheme consistently exhibits the lowest computational overheads across above scenarios. This is because our scheme pre-negotiates the Data BS group and utilizes the AMAD to facilitate multi-UE aggregated access. As a result, with the increase in the number of UEs and cooperative BSs, the computational overhead is smaller compared to the repetitive accumulation observed in single-UE schemes. Similarly, the results for multi-UE schemes are illustrated in (d), (e), (f) in Fig. 5, again showing the proposed scheme's efficiency. The existing 5G-AKA protocol necessitates public key encryption for identity protection, resulting in higher computational overheads. Other schemes also incur additional costs due to chosen encryption algorithms and multi-BS cooperation guarantees. In contrast, the proposed scheme utilizes a lightweight encryption algorithm and pre-negotiates the Data BS group, making it more suitable for the multi-BS cooperation UE access architecture in FD-RAN. Overall, the proposed scheme demonstrates lower computational overheads compared to existing solutions.

TABLE IV
ACCESS OVERHEADS FOR DIFFERENT SCHEMES

Singal UE Scheme	T_{tot}
UHAEN [16]	$[18T_h + (10T_{SM} + 7T_h)n]m$
CPPHA [27]	$[18T_h + (9T_h)n]m$
SD-SIN [12]	$[18T_h + (9T_h)n]m$
Robust [15]	$[18T_h + (12T_{SM} + 9T_h)n]m$
ReHand [29]	$[18T_h + (7T_h)n]m$
[24]-singal UE	$11T_h * m + (mT_h + (m+1)T_{RV} + 2T_{ME})n$
5G AKA [6]	$[18(n+1)T_h]m$
Multi-UE Scheme	T_{tot}
FTGPHA1 [13]	$10mnT_h + 18mT_h$
FTGPHA2 [13]	$18mT_h + (3m+4)nT_{SM} + (5m+2)nT_h$
UGHA [14]	$18mT_h + (5m+4)nT_{ME} + (3m+3)nT_h$
SEGR [17]	$18mT_h + (7m+1)nT_{SM} + 5mnT_h + 3nT_P$
[24]-multi-UE	$11T_h * m + (mT_h + (m+1)T_{RV} + 2T_{ME})n$
Ours	$13mT_h + (4T_h + 4T_{sy})n * m$

B. Communication Overheads

This section focuses on comparing the sizes of authentication messages across different schemes. To maintain the same key strength, we assume AES encryption and decryption key lengths are 128 bits, ECC-based algorithms are 256 bits, and RSA algorithms are 3,072 bits. The lengths of identity information, such as SUCI, are set at 128 bits, while hash or MAC function outputs are 64 bits. The output size of Chebyshev chaotic mapping and random numbers is 128 bits, and timestamps are 17 bits. In our scheme, the size of AMAC C is $1n$ bits. Relevant parameters are presented in Table V.

TABLE V
MESSAGE SIZE

Parameters	**Size/bits**
Identity(ID_{BS}/ID_{AMF})	128
PID	256
p/q	1024/160
Key	128
SUCI/GUTI/TID/PCI	128
Hash/MAC	64
Random Number(R)	128
ECDH key	192
Timestamp(t_s)**/Expiration time** T_{exp}	17
ECC	256
AES	128
RSA	3072
Output size of the Chebyshev chaotic map	128

* Pseudo-ID (PID), Globally Unique Temporary ID (GUTI), Physical Cell Identity (PCI).

The communication overheads analyzed in this paper encompasses the initial access overheads to the FD-RAN CBS and the Data BS. For this calculation, we assume there are m UEs accessing n Data BSs, with a representing the number of authentication vectors transmitted by AUSF in 5G-AKA (typically, $a = 1$). The communication overheads for each scheme is detailed in Table VI. The results of the communication overheads comparison are illustrated in Fig. 6, where the red pentagram dashed line indicates the proposed scheme's overheads under varying conditions. From

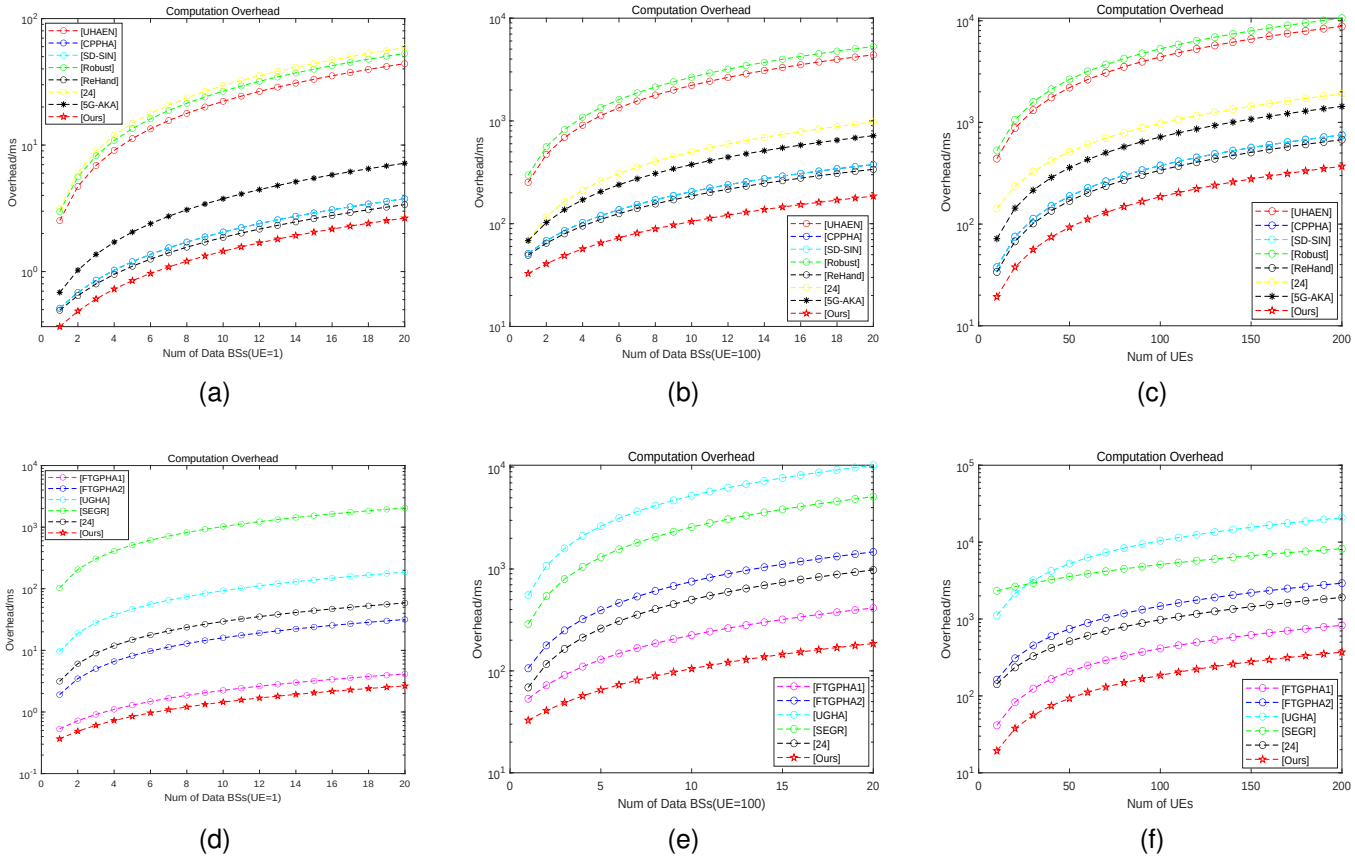


Fig. 5. Comparison of computational overheads.

TABLE VI
COMMUNICATION OVERHEADS

Scheme	Communication Overheads/bits
UHAEN [16]	$(1920+768a)m+1664m*n$
CPPHA [27]	$(1920+768a)m+1024m*n$
SD-SIN [12]	$(1920+768a)m+1728m*n$
Robust [15]	$(1920+768a)m+2112m*n$
ReHand [29]	$(1920+768a)m+1650m*n$
FTGPHA1 [13]	$(1920+768a)m+(896m+1792)*n$
FTGPHA2 [13]	$(1920+768a)m+(1536m+2304)*n$
UGHA [14]	$(1920+768a)m+(6912m+9856)*n$
SEGR [17]	$(1920+768a)m+(1920m+256)*n$
[24]	$1666m+1152+[(1154m+3744(RSA))/(1154m+928(ECDSA))]*n$
5G AKA [6]	$(1920+768a)m*(n+1)$
Ours	$774n+1794m+1408+906nm$

Fig. 6a, it is evident that with 100 UEs accessing the FD-RAN, the proposed scheme exhibits the lowest communication overheads compared to existing authentication schemes as the number of cooperative Data BSs varies. Similarly, Fig. 6b shows that with 20 cooperative Data BSs fixed, the proposed scheme maintains the minimum communication overheads as the number of accessing UEs changes. The proposed scheme employs a lightweight encryption algorithm, with keys generated independently by each party. This method allows only partial information about key generation to be transmitted, resulting in smaller authentication messages. Additionally, the scheme facilitates multi-BS key negotiation and access key derivation tailored to the FD-RAN architecture, further minimizing communication overheads. Consequently, the proposed scheme demonstrates lower communication overheads compared to various existing schemes.

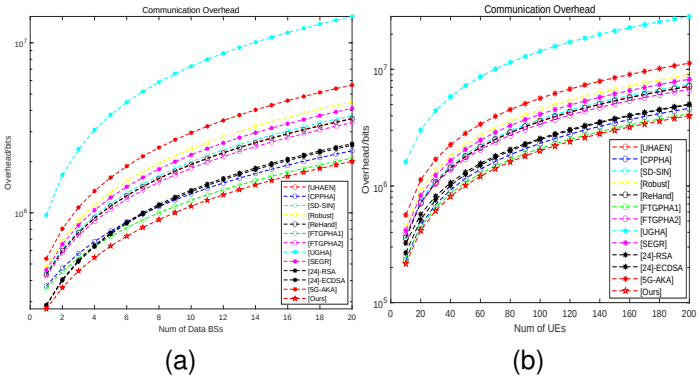


Fig. 6. Comparison of communication overheads.

C. Transmission Overhead

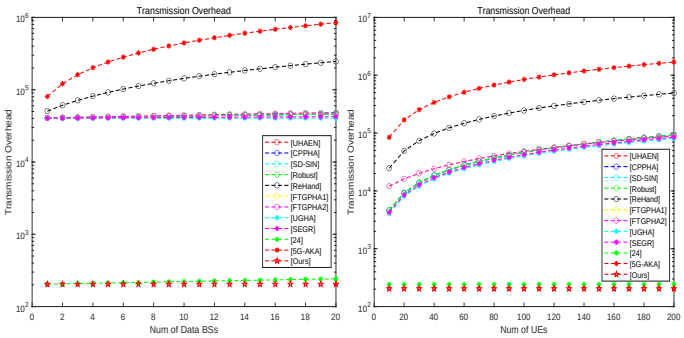
Assuming that the transmission overheads generated by signaling between the UE and SN amount to a units, and the transmission overheads between the SN and HN is b units, while the transmission overheads between UEs and between

Data BSs is ignored. Typically, the distance between the SN and HN is much greater than the distance between the UE and SN, i.e., $b >> a$. Table VII lists transmission overheads of authentication schemes of single-UE and multi-UE scenarios.

TABLE VII
TRANSMISSION OVERHEAD

Scheme	Transmission overheads
UHAEN [16]	$3ma * n + 3ma + 4mb$
CPPHA [27]	$3ma * n + 3ma + 4mb$
SD-SIN [12]	$3ma * n + 3ma + 4mb$
Robust [15]	$3ma * n + 3ma + 4mb$
ReHand [29]	$(3ma + mb) * n + 3ma + 4mb$
FTGPHA1 [13]	$(3a + 4b) * n + 3ma + 4mb$
FTGPHA2 [13]	$(3a + 4b) * n + 3ma + 4mb$
UGHA [14]	$3a * n + 3ma + 4mb$
SEGR [17]	$(ma + a) * n + 3ma + 4mb$
[24]	$2a * n + 2a + 2b$
5G AKA [6]	$(3ma + 4mb) * (n + 1)$
Ours	$2a + 2b + 2a$

Fig. 7 presents the comparison outcomes of transmission overheads when $a = 1$ and $b = 100$, with the red pentagram indicating the transmission overheads of the proposed scheme. The transmission overheads for all multi-UE schemes are lower than that of single-UE, as a result of employing mechanisms such as aggregate signatures or batch authentication, effectively reducing transmission overheads and alleviating channel congestion. Additionally, the ReHand, FTGPHA1, and FTGPHA2 need the HN to perform UE authentication and key agreement, causing significant transmission overheads. Moreover, in comparison to multi-UE schemes, when 100 UEs are fixed accessing, the transmission overheads in Fig. 7a varies with the number of cooperative Data BSs. Similarly, when 20 cooperative Data BSs are fixed, the transmission overheads in Fig. 7b varies with the number of accessing UEs. In both cases, the proposed scheme consistently demonstrates the lowest transmission overheads. In both scenarios, the proposed scheme consistently demonstrates the lowest transmission overhead. This is largely due to the preprocessing conducted for multi-BS collaboration, which means that an increase in the number of cooperative BSs has a minimal impact on the transmission overhead of the proposed approach.



(a) (b)

Fig. 7. Comparison of transmission overheads.

D. Comprehensive Discussion and Functional Comparison

In the context of the FD-RAN architecture, which involves multi-UE authentication in a multi-BS collaborative scenario, our scheme outperforms several existing authentication methods regarding computational, communication, and transmission overheads for both single-UE and multi-UE cases. The advantage in transmission overheads is particularly pronounced, being significantly lower than that of single-UE schemes, and it also shows slight advantages over the best-performing multi-UE scheme [24]. This reduction is primarily due to our method of establishing groups among multiple Data BSs.

As shown in Table VIII, our scheme achieves anonymity, traceability, KEF, PFS/PBS, and resilience against various protocol attacks. In contrast, existing schemes such as CPPHA, SD-SIN, ReHand, and FTGPHA1 lack KEF and PFS/PBS, with SD-SIN failing to ensure the anonymity of UE. The propesed approach enables communication with designated group members, allowing BSs to negotiate session keys with intended recipients. We also utilize AMAD to generate a list of malicious identities, aiding in group troubleshooting and enhancing robustness, while providing a higher message compression rate to reduce communication overheads. Our work thoroughly considers the initial access authentication under multi-BS cooperation. Although some existing schemes address initial authentication, they merely utilize the 5G-AKA from the 3GPP standards for key material transmission without designing authentication schemes suitable for multi-BS cooperation and multi-UE access. In summary, for multi-UE access scenarios in FD-RAN multi-BS collaborative environments, our scheme exhibits lower computation, communication, and transmission overheads while offering robust security features. Table VIII illustrates that our proposed access authentication scheme significantly outperforms existing methods in terms of security and overheads.

VIII. CONCLUSION

In the context of FD-RAN, which represents a promising architecture for enhancing network performance in the next generation access networks, we have proposed an efficient authentication scheme to secure multi-BS cooperation and multi-UE access based on secret sharing, CBE and AMAD techniques. The proposed scheme addresses the challenges of excessive overheads of multi-BS cooperation authentication and multi-UE access authentication, while also preventing DDoS attacks and ensuring user anonymity. The security analysis and the verification of BAN logic demonstrate that the proposed scheme is resistant to known attacks and possesses a variety of security features, while the simulation results highlight the advantages of our scheme in terms of cost savings and efficient authentication, showcasing its potential to significantly enhance the security and performance of FD-RAN. Moving forward, we will continue to investigate cooperation and authentication mechanisms in dynamic scenarios involving mobile UEs. This research aims to address the security requirements of BS cooperation and handover in high-speed mobile environments.

TABLE VIII
COMPARISON OF SECURITY FEATURES AND PERFORMANCE

	UHAEN	CPPHA	SD-SIN	Robust	ReHand	FTGPHA	UGHA	SEGR	5G-AKA	[24]	Ours
Group Security	N	N	Y	N	N	Y	Y	Y	N	Y	Y
Resist Eavesdropping	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y
Resist Replay Attacks	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y
Resist MitM Attacks	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
KEF	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Security in FD-RAN	N	N	N	N	N	N	N	N	N	N	Y
BSs Efficient Collaboration	N	N	N	N	N	N	N	N	N	N	Y
PFS	Y	N	N	Y	N	Y	N	Y	-	Y	Y
PBS	N	N	N	N	N	Y	N	Y	-	Y	Y
Anonymity	Y	Y	N	Y	Y	Y	N	N	Y	Y	Y
Traceability	N	Y	N	Y	Y	Y	N	N	Y	Y	Y
Malicious User Detection	-	-	-	-	-	N	N	N	-	Y	Y

* UHAEN [16], CPPHA [27], SD-SIN [12], Robust [15], ReHand [29], FTGPHA [13], UGHA [14], SEGR [17], 5G-AKA [6].

REFERENCES

[1] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020–2030," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 449–453.

[2] Q. Yu, H. Zhou, J. Chen, Y. Li, J. Jing, J. J. Zhao, B. Qian, and J. Wang, "A fully-decoupled ran architecture for 6G inspired by neurotransmission," *Journal of Communications and Information Networks*, vol. 4, no. 4, pp. 15–23, 2019.

[3] J. Chen, X. Liang, J. Xue, Y. Sun, H. Zhou, and X. Shen, "Evolution of RAN architectures towards 6G: Motivation, development, and enabling technologies," *IEEE Communications Surveys & Tutorials*, 2024.

[4] J. Zhao, Q. Yu, B. Qian, K. Yu, Y. Xu, H. Zhou, and X. Shen, "Fully-decoupled radio access networks: A resilient uplink base stations cooperative reception framework," *IEEE Transactions on Wireless Communications*, vol. 22, no. 8, pp. 5096–5110, 2023.

[5] N. Wang, J. Chen, J. Ni, L. Chen, and H. Zhou, "Leveraging group secret sharing technology for FD-RAN: A lightweight AKA mechanism," in *2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*. IEEE, 2024, pp. 1–6.

[6] 3GPP, "5G; Security architecture and procedures for 5G system (3GPP Standard TS 33.501 V17.12.0 Rel.17)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 33.501, 2023.

[7] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "LSAA: A lightweight and secure access authentication scheme for both ue and mmtc devices in 5G networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.

[8] S. Basudan, "LEGA: A lightweight and efficient group authentication protocol for massive machine type communication in 5G networks," *Journal of Communications and Information Networks*, vol. 5, no. 4, pp. 457–466, 2020.

[9] C. Lai and Z. Chen, "Group-based handover authentication for space-air-ground integrated vehicular networks," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[10] Y. Yang, J. Cao, R. Ma, L. Cheng, L. Chen, B. Niu, and H. Li, "FHAP: Fast handover authentication protocol for high-speed mobile terminals in 5G satellite-terrestrial integrated networks," *IEEE Internet of Things Journal*, 2023.

[11] Y. Liu, L. Ni, and M. Peng, "A secure and efficient authentication protocol for satellite-terrestrial networks," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5810–5822, 2022.

[12] K. Xue, W. Meng, H. Zhou, D. S. Wei, and M. Guizani, "A lightweight and secure group key based handover authentication protocol for the software-defined space information network," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3673–3684, 2020.

[13] R. Ma, J. Cao, D. Feng, H. Li, and S. He, "FTGPHA: Fixed-trajectory group pre-handover authentication mechanism for mobile relays in 5G high-speed rail networks," *IEEE transactions on vehicular technology*, vol. 69, no. 2, pp. 2126–2140, 2019.

[14] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7246–7251.

[15] Y. Zhang, R. H. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G hetnets," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 858–874, 2019.

[16] J. Cao, M. Ma, and H. Li, "An uniform handover authentication between E-UTRAN and non-3GPP access networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3644–3650, 2012.

[17] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 1011–1016.

[18] Y.-W. Chen, J.-T. Wang, K.-H. Chi, and C.-C. Tseng, "Group-based authentication and key agreement," *Wireless Personal Communications*, vol. 62, no. 4, pp. 965–979, 2012.

[19] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine-type communication," *Transactions on emerging telecommunications technologies*, vol. 26, no. 3, pp. 414–431, 2015.

[20] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks," in *2013 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2013, pp. 832–837.

[21] J. Cao, M. Ma, and H. Li, "GBAAM: Group-based access authentication for MTC in LTE networks," *Security and communication networks*, vol. 8, no. 17, pp. 3282–3299, 2015.

[22] ——, "LPPA: Lightweight privacy-preservation access authentication scheme for massive devices in fifth generation (5G) cellular networks," *International Journal of Communication Systems*, vol. 32, no. 3, p. e3860, 2019.

[23] Y. Liu, L. Ni, and M. Peng, "A secure and efficient authentication protocol for satellite-terrestrial networks," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5810–5822, 2022.

[24] C. Lai, Y. Ma, R. Lu, Y. Zhang, and D. Zheng, "A novel authentication scheme supporting multiple user access for 5G and beyond," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 2970–2987, 2022.

[25] I. Gharsallah, S. Smaoui, and F. Zarai, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks," *IET Information Security*, vol. 14, no. 1, pp. 21–29, 2020.

[26] A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, "A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1744–1747, 2012.

[27] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets," *IEEE transactions on dependable and secure computing*, vol. 18, no. 3, pp. 1182–1195, 2019.

[28] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48–53, 2011.

[29] C.-I. Fan, J.-J. Huang, M.-Z. Zhong, R.-H. Hsu, W.-T. Chen, and J. Lee, "ReHand: Secure region-based fast handover with user anonymity for small cell networks in mobile communications," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 927–942, 2019.

[30] X. Duan, Y. Liu, and X. Wang, "SDN enabled 5G-VANET: Adaptive vehicle clustering and beamformed transmission for aggregated traffic," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 120–127, 2017.

[31] A. Benslimane, T. Taleb, and R. Sivaraj, "Dynamic clustering-based adaptive mobile gateway management in integrated VANET—3G heterogeneous wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 559–570, 2011.
[32] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of VANET clustering techniques," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 657–681, 2016.
[33] J. Yan, D. Wu, and R. Wang, "Socially aware trust framework for multimedia delivery in D2D cooperative communication," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 625–635, 2018.
[34] G. El Mouna Zhioua, N. Tabbane, H. Labiod, and S. Tabbane, "A fuzzy multi-metric QoS-balancing gateway selection algorithm in a clustered VANET to LTE advanced hybrid cellular network," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 804–817, 2014.
[35] A. Benslimane, T. Taleb, and R. Sivaraj, "Dynamic clustering-based adaptive mobile gateway management in integrated VANET—3G heterogeneous wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 559–570, 2011.
[36] S. A. Alghamdi, "Novel path similarity aware clustering and safety message dissemination via mobile gateway selection in cellular 5G-based V2X and D2D communication for urban environment," *Ad Hoc Networks*, vol. 103, p. 102150, 2020.
[37] G. Fortino, F. Messina, D. Rosaci, G. M. Sarné, and C. Savaglio, "A trust-based team formation framework for mobile intelligence in smart factories," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6133–6142, 2020.
[38] J. Xue, K. Yu, T. Zhang, H. Zhou, L. Zhao, and X. Shen, "Cooperative deep reinforcement learning enabled power allocation for packet duplication URLLC in multi-connectivity vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 23, no. 8, pp. 8143–8157, 2024.
[39] C. Kim and K.-I. Kim, "A comparative study on gateway selection in mobile-assisted sensor data collection," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–2.
[40] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1786–1797, 2016.
[41] Y. Li, Z. Zhang, H. Wang, and Q. Yang, "SERS: Social-aware energy-efficient relay selection in D2D communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5331–5345, 2018.
[42] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6692–6702, 2015.
[43] C. Lai and Y. Ma, "A novel group-oriented handover authentication scheme in MEC-enabled 5G networks," in *2021 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2021, pp. 29–34.
[44] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farràs, and J. A. Manjón, "Contributory broadcast encryption with efficient encryption and short ciphertexts," *IEEE Transactions on Computers*, vol. 65, no. 2, pp. 466–479, 2016.
[45] Y. Ogawa, S. Sato, J. Shikata, and H. Imai, "Aggregate message authentication codes with detecting functionality from biorthogonal codes," in *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020, pp. 868–873.
[46] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18–36, 1990.

IX. Biography Section

Ning Wang (Graduate Student Member, IEEE) received the B.S. degree in communication engineering from Northwestern Polytechnical University, Xi'an, China, in 2019, where he obtained the M.S. degree in communication and information systems in 2021. He is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. He was an intern at Peng Cheng Laboratory in Shenzhen, China, in 2023, and is serving as a research assistant for an exchange at The Hong Kong Polytechnic University now. His current research interests include zero-trust security architecture, federated learning, and fully-decoupled radio access network.

Jiacheng Chen (Member, IEEE) received his Ph.D. degree in information and communications engineering from Shanghai Jiao Tong University, Shanghai, China, in 2018. From 2015 to 2016, he was a visiting scholar at BBCR group, University of Waterloo, Canada. Currently, he is an assistant researcher in Pengcheng Laboratory, Shenzhen, China. His research interests include fully-decoupled radio access network technologies. He has served as the guest editor for IEEE IoTJ, and the Workshop Co-chair for IEEE/CIC ICCC from 2021 to 2024. He was the recipient of Journal of Communications and Information Networks (JCIN) Best Paper Award in 2016, and the Chinese Institute of Electronics (CIE) Outstanding Scientific Paper in the Field of Electronic Information in 2020.

Wenchao Xu (Member, IEEE) is a research assistant professor at The Hong Kong Polytechnic University. He received his Ph.D. degree from University of Waterloo, Canada, in 2018. Before that he received the B.E. and M.E. degrees from Zhejiang University, Hangzhou, China, in 2008 and 2011, respectively. In 2011, he joined Alcatel Lucent Shanghai Bell Co. Ltd., where he was a Software Engineer for telecom virtualization. He has also been an Assistant Professor at School of Computing and Information Sciences in Caritas Institute of Higher Education, Hong Kong. His research interests includes wireless communication, Internet of things, distributed computing and AI enabled networking.

Liquan Chen (Senior Member, IEEE) received the Ph.D. degree from Southeast University, China in 2005. He worked as a postdoc in Southeast University from 2005 to 2007, and an associate professor at Southeast University from 2008 to 2018. He worked as visiting scholar in National University of Singapore, Singapore from 2011 to 2012, and became a senior member of IEEE since 2022. He now is a professor in School of Cyber Science and Engineering, Southeast University, Nanjing, China. His research interests include information security, cryptography and network security protocol, etc.

Haibo Zhou (Senior Member, IEEE) received the Ph.D. degree in information and communication engineering from Shanghai Jiao Tong University, Shanghai, China, in 2014. From 2014 to 2017, he was a Postdoctoral Fellow with the Broadband Communications Research Group, Department of Electrical and Computer Engineering, University of Waterloo. He is currently a Full Professor with the School of Electronic Science and Engineering, Nanjing University, Nanjing, China. He was a recipient of the 2019 IEEE ComSoc Asia–Pacific Outstanding Young Researcher Award, 2023-2024 IEEE ComSoc Distinguished Lecturer, and 2023-2025 IEEE VTS Distinguished Lecturer. He served as Track/Symposium Co-Chair for IEEE/CIC ICCC 2019, IEEE VTC-Fall 2020, IEEE VTC-Fall 2021, WCSP 2022, IEEE GLOBECOM 2022, IEEE ICC 2024, IEEE GLOBECOM 2024. He is currently an Associate Editor of the IEEE Transactions on Wireless Communications, IEEE Internet of Things Journal, IEEE Network Magazine, and Journal of Communications and Information Networks. His research interests include resource management and protocol design in B5G/6G networks, vehicular ad hoc networks, and space-air-ground integrated networks.