A Novel Authentication Scheme Supporting Multiple User Access for 5G and Beyond

Chengzhe Lai, *Member, IEEE,* Yixiao Ma, Rongxing Lu, *Fellow, IEEE,* Yinghui Zhang, *Member, IEEE,* and Dong Zheng

Abstract—The deployment of ultra-dense networks in the fifth-generation (5G) network architecture can significantly improve the quality of wireless links, but this will cause frequent handovers of mobile users and increase authentication delays. Furthermore, the simultaneous influx of a large number of mobile users may cause serious network congestion. Aiming at these problems, this paper proposes a novel authentication scheme supporting multi-user access, which fully considers the scenarios of intra-domain handover and inter-domain handover across AMF. Using the characteristics of the network architecture integrated with mobile edge computing (MEC) and software-defined networks (SDN), the user's moving path can be predicted in advance to speed up the handover process. Most importantly, the proposed scheme can perform secure, efficient and flexible mutual authentication and key agreement between the group and the core network by using aggregated message authentication codes with detecting functionality (AMAD) and contributory broadcast encryption technique. Through the use of BAN Logic and Scyther tool verification, the proposed scheme can not only realize multiple user authentication and key agreement, but also fulfill various security goals. Performance evaluations demonstrate that the proposed scheme has moderate computational and communication overhead, and lower transmission overhead compared with existing schemes, which can effectively reduce authentication delay.

Index Terms—5G, Multi-user access, Handover authentication, BAN Logic, Scyther

1 Introduction

The development of mobile Internet and smart terminal equipment has promoted the explosive growth of wireless data traffic and the continuous upgrading of wireless communication network architecture. The current 5G networks support full-spectrum access. Using such a hybrid network can fully tap the advantages of low-frequency and high-frequency, providing higher data transmission rates and spatial reuse rates of spectrum resources [1]. So that mass machine communication (mMTC), Internet of Things (IoT), Internet of vehicles (V2X) and other emerging applications have greater development space under 5G networks [2] [3]. However, the use of high-frequency bands will greatly shorten the transmission distance of base stations (BS) and reduce the coverage capacity. To solve these problems, ultra-dense networking can be used to increase system capacity.

In the 5G era, mobile edge computing (MEC) will promote the integration of cloud computing platforms and mobile networks [4]. It was reported in [5] that with the improvement of technical standards in the IoT industry and the continuous breakthrough in key technologies, the connection of a large number of network edge devices will inevitably generate a large amount of real-time data. While the distance between the cloud and the devices will cause high bandwidth consumption and processing delay, which is unacceptable for many delay-sensitive edge-side data. MEC solves these problems to a certain extent by sinking computing, storage and business resources to the edge of the network. It is of great significance for achieving traffic offloading, flexible and fast service deployment, and reducing latency [6]. For ultra-dense deployment scenarios in 5G networks, 3GPP has proposed a network architecture that can decouple the control plane and data plane of devices: software-defined networks (SDN). SDN's programmability and centralized network management enable it to collect traffic in the network. With the help of a unified and real-time network topology map, SDN can use different positioning and data analysis technologies to predict the location of mobile devices and plan different paths for different network traffic, so as to make full use of the link.

In addition, a large number of highly dynamic mobile devices in 5G may access the network simultaneously, but numerous devices competing for a limited number of wireless channels will increase the probability of collisions and cause network congestion. Therefore, the network needs to correctly authenticate such mobile users to avoid distributed denial of service (DDoS) attacks and should have the ability to control a large amount of signaling traffic. However, 5G-AKA [7], a standardized authentication protocol that has been defined in 3GPP, only supports the authentication of single user and cannot handle the situation where numerous users access the network simultaneously. Therefore, it is necessary to design a novel multi-user access scheme to achieve lower handover authentication delay [8]. Although some handover authentication schemes supporting group access have been proposed, there are still security and performance issues when these schemes are implemented in multi-user access scenarios. Most existing schemes lack some strong security properties such as freedom of key escrow and malicious user identity detection, and cannot provide more flexible security functions supporting group communication. In addition, the performance still needs to be optimized in terms of computational overhead, communication overhead, and transmission overhead. Based on MEC and SDN, we design a multi-user access authentication scheme by using aggregated message authentication codes with detecting functionality (AMAD) [9] and contributory broadcast encryption (CBE) technique [10]. The main contributions are as follows:

- **Firstly**, to efficiently achieve multi-user access authenti-

- *Chengzhe Lai, Yixiao Ma, Yinghui Zhang and Dong Zheng are with School of Cyberspace Security, Xi'an University of Posts and Telecommunications.*
- *Rongxing Lu is with Faculty of Computer Science, University of New Brunswick.*

cation, the process of secure group establishment is considered. Equipped with CBE technique, group members can generate their decryption key and group public key PK_G cooperatively. Particularly, these stages can be performed offline, paving the way for the handover authentication that support multi-user access, avoiding the introduction of additional overhead during handover authentication.

- **Secondly**, the proposed scheme fully considers initial authentication, intra-domain handover authentication, and inter-domain handover authentication. In particular, we utilize the pre-prepared PK_G combined AMAD technique to design a novel multi-user access authentication protocol, which can optimize the signaling process and reduce authentication delay. Moreover, the proposed scheme can provide the function of the base station flexibly designating group members to securely communicate with it. And the base station can effectively identify the malicious identities, improving the robustness of the group.
- **Finally**, the BAN logic and Scyther tool are used to formally verify the proposed initial authentication and handover authentication protocols. The security analysis shows that the proposed scheme can guarantee the additional security properties: group's anonymity, traceability, key escrow freedom, perfect forward/backward secrecy and can resist a variety of protocol attacks. Comprehensive performance evaluations demonstrate that comparing with the similar schemes, the proposed initial authentication and handover authentication has advantages in terms of computational, communication and transmission overhead, while can provide rich functions.

The rest of this paper is organized as follows: Section 2 reviews the related work. Section 3 introduces the system model. Section 4 details the proposed scheme, including group establishment, and multi-user authentication. In Section 5, we demonstrate the security and correctness of the scheme. Section 6 evaluates the performance of the proposed scheme and compares it with existing schemes. Finally, we draw the conclusion in Section 7.

2 Related Work

At present, many researchers have tried to combine some emerging technologies to enhance the security and performance of handovers in ultra-dense networks. Designing handover authentication schemes that support multi-user access for alleviating channel congestion and reducing handover delay is a ctitical challenge. In this paper, we divide existing handover authentication schemes into single-user access and multi-user access handover authentication.

2.1 Handover Authentication for Single-user Access

Handover authentication for single-user access refers to mutual authentication and session key agreement between a single user and different BSs when moving. J. Cao et al. [11] proposed a handover authentication scheme using the identity-based cryptosystem without pairing operations, which can be applied to all mobile scenarios between E-UTRAN and non-3GPP access networks. L. Cai et al. [12] proposed a user-assisted authentication context transmission scheme. The mobile users actively participate in the handover authentication process, which significantly promotes the context transmission to reduce delay. In order to ensure the seamless handover and reasonable allocation of resources, the user's attribute combinations have been reported to the BS as non-cryptographic schemes, which can be faster and simpler than the widely used cryptographic exchange mechanisms [13].

X. Duan et al. [14] used an SDN-based non-encrypted scheme for handover authentication and privacy protection. Since SDN can monitor and predict the user's movement status to prepare for handover according to the security context, when monitoring the user's traces, if not entirely, the risk of impersonation will be greatly reduced. J. Cao et al. [15] proposed a capability-based privacy-protection handover authentication scheme using SDN. Due to the characteristics of the SDN controller, an appropriate BS can be selected for 5G users before they arrive to ensure seamless handover authentication, without the need for complex communication protocols between BS, which can greatly simplify the signaling process. K. Xue et al. [16] proposed a lightweight group key scheme for software-defined space information networks based on (t, n) secret sharing, which can establish secure channels between satellites and between controllers and satellites to ensure security and applicability. This scheme aims to reduce the redundant handover authentication process across different satellites.

Some schemes apply the characteristics of blockchain decentralization, anti-tampering of historical records, transaction information privacy protection, and traceability to handover authentication, which can protect user identity and data security. A. Yazdinejad et al. proposed a scheme [17], after the user registers in the blockchain center, the blockchain generates encrypted materials and assigns a public/private key pair to the user, and sends the user's data to the SDN controller to verify the identity of the user. In this way, even if the handover is performed between heterogeneous cells, there is no need to perform complete authentication again, reducing the handover time. Unlike the scheme [17], in scheme proposed by Y. Zhang et al. [18], the user's private key is chosen by itself. Meanwhile, the scheme uses the trapdoor collision feature of chameleon hash functions and anti-tampering function recorded in the blockchain to achieve handover authentication anonymously. V. Sharma et al. [19] used three blockchains to deal with the hierarchical security issues and user logout issues without affecting the network layout, greatly reducing the signaling burden.

With the growth of massive data, MEC can effectively alleviate the big data processing problems at the edge of the network and the cloud center [20] [21]. Another advantage of MEC is that it breaks through the limitations of terminal hardware, enabling portable devices such as mobile terminals to participate in a large number of calculations, achieving intelligent load balancing and reducing management costs. C. Wang et al. [22] proposed the SHAS scheme combining MEC and SDN. The edge computing node and the target BS use the symmetric key distributed by the SDN platform to complete seamless handover. Among them, the edge computing node has certain computing capabilities, so it only needs to perform mutual authentication between the edge computing node and the BS. Y. Sun et al. [23] designed a user-centric mobility management scheme in the ultra-dense network that supports MEC, providing users with a way to select BSs and MEC servers, and predict when to perform handover.

2.2 Handover Authentication for Multi-user Access

If users with the same moving trajectory or resource request are formed into a group, then it will be more convenient and

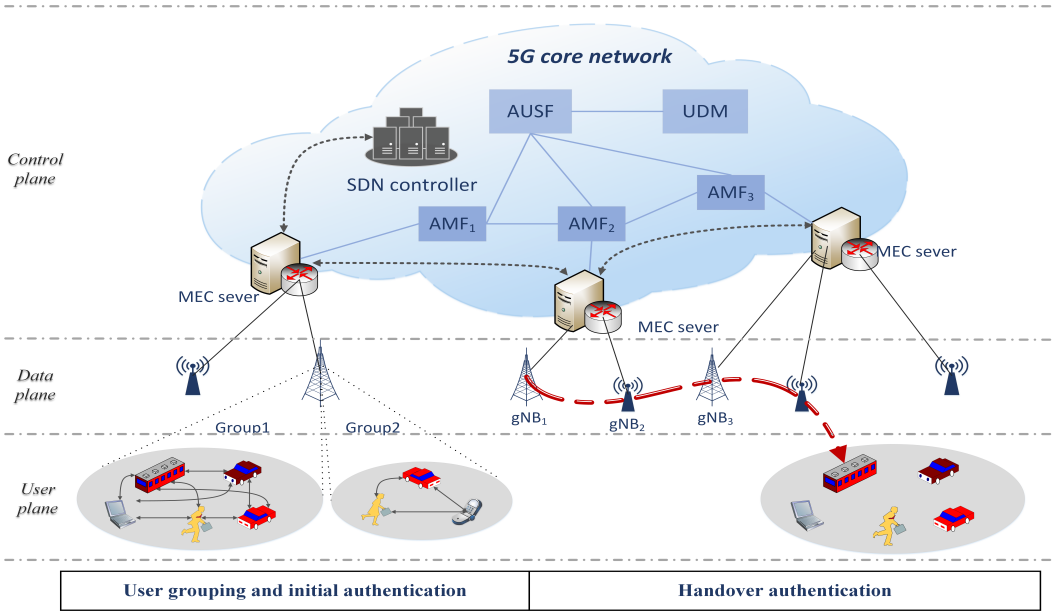


Fig. 1. System model

faster to perform handover authentication for the group than for a single-user, and all aspects of the overhead will be greatly reduced. Therefore, it is necessary to design handover authentication schemes that support multi-user access. I. Gharsallah et al. [24] proposed a handover authentication scheme to support large-scale vehicle equipment in the 3GPP networks, which can minimize network congestion. The mobile relay nodes introduced by this scheme can improve link quality and reduce handover delay. J. Cao et al. [25] proposed two fixed-track group pre-handover authentication schemes for mobile relay nodes. In these two schemes, since all mobile relay nodes are in the same train and the next BS can use the SDN controller to complete the pre-handover authentication, the handover delay can be ignored.

To provide group anonymity, A. Fu et al. [26] grouped users according to their Signal-Noise Ratio and historical handover information. When a member of the group moves, the security context information of other group members will be sent to the new BS for authentication. When other members also need to access the BS, they can bypass the authentication stage. Additionally, users change their pseudonyms during each handover authentication stage to prevent tracking and protect privacy. D. He et al. [27] used pairing-based cryptography and batch signatures to protect the safety of the handover process, support user revocation, and reduce the communication and computational overhead. To protect user anonymity, the server will select a set of unlinkable pseudo-identities to send to the user. C. Fan et al. [28] designed a region-based fast handover authentication protocol. This scheme uses a blinding factor to ensure identity randomization to avoid traceability of communication footprints. C. Lai et al. [29] proposed a novel group signature technique that enables anonymous identity authentication among vehicles, fog nodes, and servers.

Since each terminal sends a large amount of data, even if a group leader is selected as a representative to send group information to the BS, high communication bandwidth is still required. Therefore, some schemes aggregate multiple communication data into a shorter massage and send it to the recipient. J. Cao et al. [30] proposed two lightweight authentication schemes for a single mobile device and a large number of mMTC devices in 5G networks. The serving network can use aggregated message authentication codes (AMAC) and extended Chebyshev chaotic maps to complete the authentication of a group of devices, and negotiate a different session key with each device. C. Lai et al. [31] used multi-signature and AMAC to perform authentication and key agreement for a group of users, which is suitable for all mobile scenarios in LTE-A network. However, AMAC can only guarantee the reliability of the message source, and cannot prevent mutual denial and deception between the communicating parties in the system. Therefore, C. Lai et al. proposed a group roaming scheme between 3GPP and WiMAX networks [32]. By adopting certificateless aggregation signature, the BS and the core network can simultaneously trust a large number of mobile users, and obtain an independent session key with each user during the handover process, realizing dual authentication of messages and entities.

3 System Model, Security Model and Design Goals

In this section, we first introduce the system model, and then describe the security model and design goals.

3.1 System Model

As shown in Fig.1, the system model consists of 1) 5G core network. Including AUSF/UDM which implements authentication server functions and unified data management, and AMF which implements access and mobility management functions. 2) MEC Server. It can provide users with network resources nearby, reducing time delays. In our scheme, MEC servers are deployed at the edge of the core network close to users and establish physical connections with nearby gNBs. 3) SDN controller. Use the characteristics of SDN to monitor network traffic and predict the appropriate handover path. 4) Base stations. For a unified description, this paper uses gNB to represent the BS in 5G, which is responsible for feeding back the user's network request

to the core network and authenticating the users. 5) User group G. Mobile users in G can be any edge computing node (ECN) with certain computing capabilities and equipped with corresponding wireless transceiver devices, such as on-board units in vehicles, mobile phones, laptops, personal wearable devices, etc. Based on the corresponding grouping strategy, such devices can establish temporary groups with similar attributes or access requirements anytime and anywhere without the support of existing information infrastructure network facilities.

In order to provide nearby network resources to mobile users, we integrate SDN and MEC. This network architecture is divided into three layers [33], respectively: $control\ plane$: The SDN global controller is deployed in the core network for centralized control. As the local controller of SDN, the MEC server assists SDN to collect the dynamic topology of users within its range and make decisions according to the network status. $Data\ plane$: Each gNB has a local database to store user information in its unit and updates regularly, such as group information, user location. The information collected from multiple local databases constitutes the global database, which is used by the SDN controller to design network-level policies and update local application modules. $User\ plane$: It is composed of different mobile users. Data streams are separated and forwarded between users. These data streams are composed of data packets indicating the key characteristics of users.

Based on the securely established group, the proposed scheme uses AMAD [9] to realize mutual authentication and session key agreement [10] among the group, gNB and core network. In particular, the integrated network architecture of MEC and SDN [33] can predict whether the group reaches the handover threshold, and transmit the group information to the target gNB in advance.

3.2 Security Model

As described in [7], each ECN has a Subscription Permanent Identifier $SUPI$ and a pre-shared key K_i with AUSF/UDM. To guarantee anonymity, the ECN uses the Subscription Concealed Identifier $SUCI$ to initiate an authentication request to the core network during initial registration. After successful authentication, the core network will calculate a temporary identity $GUTI$ for subsequent group anonymous communication. In the above system model, it is assumed that a security association among gNB, AMF, and AUSF/UDM has been established, and the communication channel between ECN and other gNBs is a public channel. AUSF/UDM can use an authentication mechanism based on Internet Key Exchange Protocol Version 2 (IKEv2) or other simple authentication mechanisms based on public key cryptography to authenticate the gNBs. Here, AUSF/UDM has a master public/private key pair (PK_{HN}/SK_{HN}) and generates a public/private key pair (PK_{gNB}/SK_{gNB}) based on RSA for each gNB, then pre-distributes (PK_{gNB}/SK_{gNB}) to each gNB securely. The gNBs in the same AMF domain trust each other according to the pre-established security tunnel, and there is no trust relationship between gNBs in different AMF domains. The inter-domain handover authentication occurs between different AMF domains.

The security of the proposed scheme is based on the widely used Dolev-Yao threat model. Under the above conditions, an attacker is completely in control of the communication channel over the air interface and may use the messages sent by ECN to launch various attacks, such as replay attacks, impersonation attacks, and man-in-the-middle attacks. In addition, if the negotiated encryption/decryption key or session key is leaked, the security of message transmission cannot be guaranteed.

3.3 Design Goals

To achieve secure and efficient multi-user handover authentication for 5G and beyond networks, our scheme should fulfill the following design goals.

Mutual Authentication and Key Agreement: During initial authentication, the AUSF/UDM authenticates the identity of the group, and sends the authentication result to AMF and gNB. To improve security, the group needs to authenticate the identities of AUSF/UDM, AMF and gNB at the same time. When the group moves to target gNB, the identities of the group and target gNB need to be verified to be legal. In addition, in initial authentication and handover authentication, a secure session key must be established between the group and the gNB to ensure the confidentiality of subsequent information transmission.

Anonymity and Traceability: ECN should use an anonymous identity, and the anonymous identity should be updated during inter-domain handover. Except for ECN, this anonymous identity can only be calculated by AUSF/UDM. In the event of a dispute, AUSF/UDM can retrieve and identify its specific location and trajectory based on the anonymous identity of the ECN.

Key Escrow Freedom (KEF): Each member's decryption key is kept by itself, and there is no need for trusted third parties to distribute key materials.

Perfect Forward/Backward Secrecy (PFS/PBS): PFS implies that even if the current key is compromised, the adversary cannot extract any valid information from the previous ciphertext. While PBS means that the compromise of the current key should not compromise future ciphertexts and session keys.

Protocol Attack Resistance: The designed scheme must be able to resist protocol attacks, such as *replay attacks*, *impersonation attacks*, *man-in-the-middle attacks*, *DDoS attacks*, etc.

Malicious User Identity Detection: When the gNB fails to authenticate the group, it should not directly return an authentication failure message. Instead, the gNB detects the identity of the group members and feeds back a list of malicious identities to the group.

Performance Optimization: In order to reduce the authentication delay, the proposed scheme needs to comprehensively consider the computational overhead, communication overhead and transmission overhead. Therefore, the overall performance of initial and handover authentication in our scheme should outperform the existing schemes.

4 Proposed Scheme

Assuming that the group size is *n*, each member ECN_i has a unique index i corresponding to it, and these indexes constitute the set $\mathbf{A} = \{1, 2, ..., n\}$. The system parameters are $\pi = (\lambda, \gamma, n, g, h_1, ..., h_n, F, f_1, f_2, f_3)$. Where $\gamma = (p, \mathbf{G}, \mathbf{G_T}, e)$, $\mathbf{G}$ and $\mathbf{G_T}$ are multiplicative groups with the same prime order p, and $e : \mathbf{G} \times \mathbf{G} \rightarrow \mathbf{G_T}$ is an efficient non-degenerate bilinear map. Let $h_i \in \mathbf{G}$ be randomly chosen for ECN_i, where $i \in \mathbf{A}$. And g, h_i be independent generators of $\mathbf{G}$, F is a MAC function and the functions f_1, f_2, f_3 are independent one-way trapdoor functions, completely unrelated to each other. The symbols with high frequency in our scheme are described in TABLE 1.

TABLE 1
Notations used in the proposed scheme

Notation	Definition
ECN_i	the i-th edge computing node, and ECN_h is the secure mobile gateway selected in the group
$SUCI_i, GUTI_i$	anonymous identity of ECN_i
$\mathbf{G}$, $\mathbf{G_T}$	multiplicative group
G	the group with *n* ECNs
F, H	F is a MAC function. H is a hash function
f_1, f_2, f_3, KDF	f_1, f_2, f_3 are independent one-way traodoor functions. KDF is a key derivation function
K_i	pre-shared key between ECN_i and AUSF/UDM
PK_i	the public key of ECN_i negotiated in group G, and PK_G is the group public key
d_i	decryption key of ECN in group G
$\mathbf{S}$, $\mathbf{s}$	$\mathbf{S}$ is a syndrome generation matrix of a l-order biorthogonalcode, and $\mathbf{s}$ is the syndrome
Σ, ε	Σ is an extended syndrome generation matrix of $\mathbf{S}$, and ε is the extended syndrome
$\mathbf{X}$, $\mathbf{X}^T$	$\mathbf{X}$ is a matrix of order $(l+1)\times n$, $\mathbf{X}^T$ is the transpose matrix of $\mathbf{X}$
m_i	message sent by ECN_i
t_i	message authentication code generated by ECN_i
$T=(T_1,T_2)$	the aggregation message authentication code of group G calculated by ECN_h
AU_i	ECN_i uses AU_i to verify the identity of AUSF/UDM
$AUTH_i$	ECN_i uses $AUTH_i$ to verify the identity of AMF
MAC^i_{AMF}	the message authentication code of the AMF , used for integrity protection
r_x	random number selected by x
CK_i/IK_i	encryption/integrity key obtained by ECN_i
k^x_y	shared key between x and y
$(x)_k$	encrypt x with symmetric key k
$\mathbf{A}$	$\mathbf{A}=\{1,2,...,n\}$ and $i\in\mathbf{A}$
Ω	$\Omega\subseteq\mathbf{A}$, The gNB communicates with ECN_i in this set
C	Ciphertext
ξ	session key negotiated between gNB and ECN_i in Ω
δ	digital signature based on ECDSA or RSA algorithm
TS	timestamp

4.1 Preliminaries

In this section, we recall several techniques that will be used in our proposed scheme.

A. Wu's Contributory Broadcast Encryption Scheme (CBE)

In 2016, Wu et al. proposed a contributory broadcast encryption scheme [10] in which the group key agreement system is jointly established by a group that already mutually authenticated. The index range of each group user U_i is $i\in\mathbf{A}$. The CBE consists of the following four polynomial time algorithms:

- **ParaGen:** The algorithm is used to generate global parameters, taking the safety parameter λ as the system input. And finally outputs system parameters including group size *n*.
- **Setup:** This stage is run jointly by all group members to build the system in a public channel. Each U_i randomly chooses x_i or other random values that can represent its internal state information as private inputs. If the algorithm is successfully terminated, the system will output the decryption key d_i kept privately by each U_i and the group public key PK_G shared by all group members. PK_G is publicly accessible. If the algorithm is interrupted, the system outputs NULL.
- **GEncrypt:** The GEncrypt is performed by the sender who is assumed to know the PK_G. The sender can be a member of the group or any user outside the group who knows PK_G. Additionally, the sender can communicate with the specified group members U_i and negotiate the same session key with those members, where $i\in\Omega$ and $\Omega\subseteq\mathbf{A}$. This algorithm takes Ω and PK_G as input, and outputs (C,ξ), where C is the ciphertext and ξ is the session key negotiated by the sender and receiver. Finally, the sender sends (C,Ω) to the specified receiver.
- **GDecrypt:** After the corresponding receiver $U_i(i\in\Omega)$ receives (C,Ω), This algorithm takes the receiver set Ω, the index i, receiver's decryption key d_i, and ciphertext C as input, and outputs session key ξ.

B. Aggregated Message Authentication Codes with Detecting Functionality (AMAD)

The AMAD scheme proposed in [9] achieves a better message compression rate and realizes the function of detecting wrong MACs through l-order biorthogonal code. This paper uses the Construction II algorithm in the AMAD scheme, and describes this algorithm according to the notations used in our scheme. Let $\mathbf{S}$ be a syndrome generation matrix of a biorthogonal code having $(n,k,d_{min})=(2^l,l+1,2^{l-1})$ with $l\geq 3$, and $\mathbf{s}$ be the syndrome. Let Σ be an extended syndrome generation matrix of $\mathbf{S}$, and ε be the extended syndrome. For each $i=1,2,...,l+1$, let $\mathbf{S_i}=(S_{i,1},S_{i,2},...,S_{i,n})\in\{0,1\}^n$ be the i-th row of the matrix $\mathbf{S}$. After that, we define $\mathbf{X_i}=(X_{i,1},X_{i,2},X_{i,3},...,X_{i,n})=(S_{i,1},\alpha S_{i,2},\alpha^2 S_{i,3},...,\alpha^{n-1}S_{i,n})$, where α is a primitive element of $GF(2^h)$. Then, we define an $(l+1)\times n$ matrix $\mathbf{X}$ whose i-th row is given by $\mathbf{X_i}$, and let Γ be a $(2^{l+1}-1)\times n$ matrix whose rows compose of all codewords generated by $\mathbf{X}$ except for the zero-vector. Construct II in the AMAD scheme consists of polynomial-time algorithms (KGen, Tag, Agg, TVrfy):

- **KGen:** Takes a security parameter and the sender's ID as input, and generates a key K_{ID} for the sender. This key is the pre-shared key $K_i(i\in\mathbf{A})$ between ECN_i and AUSF/UDM in the initial authentication of this paper.
- **Tag:** For each $i\in\mathbf{A}$, takes the ith sender's message m_i and its key K_{ID_i} as input, then calculates a tag $t_i=F(K_{ID_i},m_i)$ based on the underlying MAC fuction and outputs t_i.
- **Agg:** For each $i\in\mathbf{A}$, takes tuples of sender's ID, messages and MAC tags from multiple senders $(ID_1,m_1,t_1),...,(ID_n,m_n,t_n)$ as input and outputs an aggregated tag T. For $t=(t_1,...,t_n)$, it computes $T_1=(T_{1,1},T_{1,2},...,T_{1,l+1})=t\mathbf{S}^T$. For each i, let $t_i^*\in GF(2^h)$ be the last h bits of t_i, and set $t^*=(t_1^*,...,t_n^*)$. Then it computes $T_2=(T_{2,1},T_{2,2}...,T_{2,l+1})=t^*\mathbf{X}^T$. Subsequently, the executor of the algorithm **Agg** generates a aggregated message authentication code $T=(T_1,T_2)$.
- **TVrfy:** For each $i\in\mathbf{A}$, the message receiver computes $t=(t_1,...,t_n)$. Finally, it verifies $\mathbf{s}=T-t\mathbf{S}^T$. If $\mathbf{s}=0$, it outputs the malicious identity list $J=\emptyset$; Otherwise, calls **Algorithm** 1 to output the malicious user identity list J.

4.2 Secure Group Establishment

In multi-user access scenarios, the secure group establishment can be divided into two stages: user grouping and group key agreement.

4.2.1 User Grouping

Users that can be grouped into a group often have similar movement trajectories and resource requests. Treating such a group as a whole for authentication and requesting network resources will greatly shorten the authentication waiting time and reduce the wireless channel occupancy rate. The user grouping stage consists of *Initial Grouping* and *Intra-Group Trust Establishment*.

Algorithm 1 Malicious user identity detection

Input: Group size is n; $\mathbf{X}$; Σ; Γ;
Initialize:
set $\mathbf{A} = \{1, 2, ..., n\}$ and $L = \{1, 2, ..., 2^{l+1} - 1\}$;
computing an extended syndrome $\varepsilon = (\varepsilon_1, \varepsilon_2, ..., \varepsilon_{2^{l+1}-1}) = e\varepsilon^T$;
/* where e is an error vector */
while $i = 1, 2, ..., 2^{l+1} - 1$ **do**
  if $\varepsilon_i = 0$ **then**
    set $\mathbf{A} \leftarrow \mathbf{A} \setminus \{j_{i,1}, j_{i,2}, ..., j_{i,\omega_i}\}$ and $L \leftarrow L \setminus \{i\}$ where $1 \le j_{i,1} \le j_{i,2} \le ... \le j_{i,\omega_i} \le n$ are integers and $\Sigma_{i,j_{i,1}} = \Sigma_{i,j_{i,2}} = ... = \Sigma_{i,j_{i,\omega_i}} = 1$ in the i-th row of Σ
  end if
end while
$\mathbf{g} = (g_1, g_2, ..., g_{l+1}) = T_2 - t^*\mathbf{X}^T = e^*\mathbf{X}^T$
/* where e^* is an error vector */
$\gamma = (\gamma_1, \gamma_2, ..., \gamma_{2^{l+1}-1}) = e^*\Gamma$
while $i = 1, 2, ..., 2^{l+1} - 1$ **do**
  $J = \{j | \Sigma_{i,j}\alpha^{j-1}\varepsilon_i^* = \gamma_i \quad for \quad i \in L, j \in \mathbf{A}\}$
  /* where ε_i^* is the last h bits of ε_i, and considering $\varepsilon_i^* \in GF(2^h)$*/
end while
Output: output a list J consisting of the index values of all ID_j, where the index value $j \in J$.

• ***Initial Grouping*:** For initial grouping, the formation of groups and the selection of mobile gateways have been well investigated [34] [35] [36] [37]. Besides communication, computing and storage capabilities, the selection of the secure mobile gateway ECN_h should be subject to additional policies, e.g., trust levels [38] [39] [40].

As a candidate solution, scheme [41] introduced a user grouping mechanism in which the base station gNB can initially group all ECNs within its range with the help of the network topology, received signal strength and inter-ECN distance provided by the SDN controller [34]. Then the grouping information can be returned to the ECN_h with a high trust level in the group. Finally, ECN_h broadcasts the initial grouping information to neighboring members. To avoid a single point of failure, the scheme [34] also proposed a selection method for alternative ECN_h to enhance network robustness.

• ***Intra-Group Trust Establishment*:** Intra-group trust establishment must be performed after the initial grouping, guaranteeing secure negotiation of the group key. According to the security level requirements of specific scenarios, strong intra-group authentication mechanisms using cryptography [42] [43] [44] can be applied. Alternatively, faster and simpler non-cryptographic mechanisms, such as [45], can be used to establish intra-group trust relationships in lightweight scenarios.

In solution [41], group members can achieve intra-group trust establishment through attribute matching and trust value calculation [45]. First, each ECN_i updates the trust value $R_{(i,j)}$ in order to interact with other users, where $R_{(i,j)}$ represents the trust value of ECN_j to ECN_i, and this value is stored in the local reputation database of ECN_i. When the value of $R_{(i,j)}$ is greater than the threshold specified by the group, ECN_j considers ECN_i to be legitimate and credible. The group G retains the group members whose $R_{(i,j)}$ reaches the threshold, and further calculates the intra-group trust degree $TD_{(i,j)}$ among members according to the member attribute set $UAS = \{uas_1, uas_2, ...\}$ (UAS includes the user's QoS, security level, location, moving speed and direction, etc.) and $R_{(i,j)}$.

4.2.2 Group Key Agreement

After trust relationships are established among group members in G, each member ECN_i has a unique index i ($i \in \mathbf{A}$). Afterwards, we use CBE to perform group key agreement, the group public key and the decryption keys corresponding to all ECNs are generated only by members in G. The specific negotiation process is divided into group key agreement (GKA), group public key derivation (PKD) and member decryption key derivation (DKD):

- **GKA:** For $k \in \mathbf{A}$, each ECN_k randomly choose $X_{i,k} \in \mathbf{G}$, $r_{i,k} \in \mathbf{Z}_p^*$, and compute $R_{i,k} = g^{-r_{i,k}}$, $A_{i,k} = e(X_{i,k}, g)$, then the public key of ECN_k is $PK_k = ((R_{0,k}, A_{0,k}), ..., (R_{n,k}, A_{n,k}))$. For $i = 0, ..., n$, $j \in \mathbf{A}$, with $i \neq j$ and $j \neq k$, ECN_k computes $\sigma_{i,j,k} = X_{i,k}h_j^{r_{i,k}}$, set $d_{j,k} = (\sigma_{0,j,k}, ..., \sigma_{j-1,j,k}, \sigma_{j+1,j,k}, ..., \sigma_{n,j,k})$. After completing the above calculation,the ECN_k sends $(PK_k, d_{1,k}, ..., d_{k-1,k}, d_{k+1,k}, ..., d_{n,k})$ publicly.
- **PKD:** The group public key is calculated publicly as follows:

$$PK_G = PK_0 \circledast PK_1 \circledast ... \circledast PK_n$$
$$= ((R_0, A_0), ..., (R_n, A_n))$$

  Where $\circledast : \Phi \times \Phi \to \Phi$ is an efficient operations in the public key space Φ and $R_i = \prod_{k=1}^{n} R_{i,k}$, $A_i = \prod_{k=1}^{n} A_{i,k}$, for $i = 0, ..., n$.
- **DKD:** For $0 \le i \le n$, $j \in \mathbf{A}$ and $i \neq j$, ECN_j can compute decryption key:

$$d_j = (\sigma_{0,j}, ..., \sigma_{j-1,j}, \sigma_{j+1,j}, ..., \sigma_{n,j})$$

  where

$$\sigma_{i,j} = \sigma_{i,j,j} \prod_{k=1,k\neq j}^{n} \sigma_{i,j,k} = \prod_{k=1}^{n} \sigma_{i,j,k} = \prod_{k=1}^{n} X_{i,k}h_j^{r_{i,k}}$$

  The key generation of CBE is homomorphic, even if the members are dynamically updated, the group public key and decryption keys of other members only need to link or delete the key materials contributed by the updated members, without re-establishing the group.

After completing the above stages, G will maintain the same driving trajectory for a period of time.

4.3 Multi-User Access Authentication

The proposed scheme includes initial authentication, intra-domain handover and inter-domain handover authentication.

4.3.1 Initial Authentication

The initial authentication is triggered when G accesses the network for the first time. The specific authentication process is as follows:

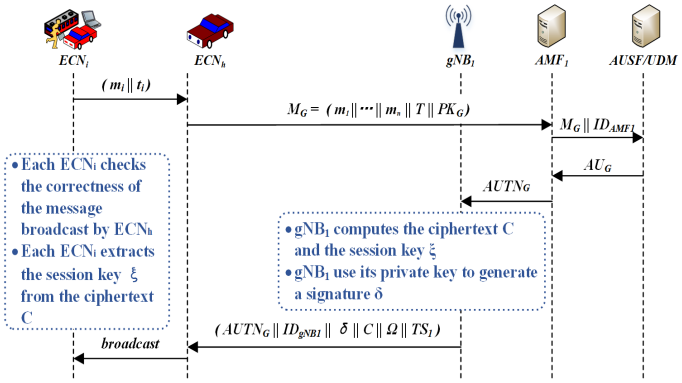


Fig. 2. Initial authentication

Step-1: $ECN_i \to ECN_h$: $(m_i||t_i)$

At the initial access, each ECN_i uses $SUCI_i$ to prevent leakage of real identity. ECN_i selects a random number r_i and

generates an authentication message $m_i = (SUCI_i||PK_i||r_i)$, where PK_i is the public key of ECN_i generated in the group key agreement process. After that, ECN_i calculates a message authentication code $t_i = F(K_i, m_i)$ respectively. Finally, each member sends its $(m_i||t_i)$ to ECN_h. This step can be performed offline.

Step-2: $ECN_h \rightarrow AMF_1$: (M_G)

Upon receiving messages from all ECN_i, where $t = (t_1, ..., t_n)$, ECN_h computes $T_1 = (T_{1,1}, T_{1,2}, ..., T_{1,l+1}) = t\mathbf{S}^T$. For each i, let $t_i^* \in GF(2^h)$ be the last h bits of t_i, and set $t^* = (t_1^*, ..., t_n^*)$. ECN_h computes $T_2 = (T_{2,1}, T_{2,2}..., T_{2,l+1}) = t^*\mathbf{X}^T$. Subsequently, ECN_h generates a aggregated message authentication code $T = (T_1, T_2)$ and sends group authentication information $M_G = (m_1||...||m_n||T||PK_G)$ to AMF_1.

Step-3: $AMF_1 \rightarrow AUSF/UDM$: $(M_G||ID_{AMF_1})$

AMF_1 forwards $(M_G||ID_{AMF_1})$ to $AUSF/UDM$.

Step-4: $AUSF/UDM \rightarrow AMF_1$: $(AU_G = (AU_1||...||AU_n||\ r_{HN}))$

1) After receiving the message: $AUSF/UDM$ can retrieve the real identity $SUPI_i$ corresponding to $SUCI_i$, and analyze whether ECN_i are within the range of AMF_1. According to K_i, m_i, $AUSF/UDM$ can compute t_i and $t = (t_1, ..., t_n)$. Subsequently, $AUSF/UDM$ verifies $\mathbf{s} = T - t\mathbf{S}^T$, if $\mathbf{s} = 0$, the authentication of G is passed. Otherwise, **Algorithm** 1 will be called to output the index value list J corresponding to the malicious ECN in G.

2) After the G is authenticated: $AUSF/UDM$ generates a new temporary identity $GUTI_i = H(SUPI_i, ID_{AMF_1}, r_i)$ for all ECN_i. After that it chooses a random number r_{HN} and calculates $CK_i = f_2(K_i, r_{HN})$, $IK_i = f_3(K_i, r_{HN})$, $K^i_{AUSF} = KDF(CK_i, IK_i, ID_{AMF_1}, SUPI_i)$, and $K^i_{AMF_1} = KDF(K^i_{AUSF}, ID_{AMF_1})$. Finally, it generates $AU_i = (K^i_{AMF_1}, GUTI_i, (r_i, SUPI_i)_{K^i_{AUSF}})$, and authentication token $AU_G = (AU_1\ ||...||AU_n||r_{HN})$.

Step-5: $AMF_1 \rightarrow gNB_1$: $(AUTH_G = (AUTH_1||...||AUTH_n||PK_G||r_{HN}))$

AMF_1 keeps $K^i_{AMF_1}$, calculates $MAC^i_{AMF_1} = f_1(K^i_{AMF_1}, r_{HN}, r_i, (r_i, SUPI_i)_{K^i_{AUSF}})$ and $AUTH_i = (MAC^i_{AMF_1}, GUTI_i)$ for each $GUTI_i$, and finally sends its authentication token $AUTH_G = (AUTH_1||...||AUTH_n||PK_G||r_{HN})$ to gNB_1.

Step-6: $gNB_1 \rightarrow ECN_h$: $(AUTH_G||ID_{gNB_1}||\delta||C||\Omega||TS_1)$

Once $AUTH_G$ is received, gNB_1 is considered that the group G has been successfully authenticated. At this time, gNB_1 can communicate with some members of G, which constitute a set $\Omega \subseteq \{1, 2, ..., n\}$, $\overline{\Omega} = \{0, 1, ..., n\}\backslash\Omega$. Subsequently, gNB_1 randomly picks $\beta \in Z_p^*$, and calculates the ciphertext $C = (c_1, c_2)$:

$$c_1 = g^\beta, c_2 = \left(\prod_{i\in\overline{\Omega}} R_i\right)^\beta$$

The session key between gNB_1 and members in Ω is:

$$\xi = \left(\prod_{i\in\overline{\Omega}} A_i\right)^\beta$$

However, in the proposed scheme, we assume that gNB_1 wants to communicate with all group members and share the same session key, so only the following calculations are required, at this time $\overline{\Omega} = \{0, 1, ..., n\}\backslash\Omega = \{0\}$:

$$c_1 = g^\beta, c_2 = (R_0)^\beta$$
$$\xi = (A_0)^\beta$$

Finally, gNB_1 signs the authentication information with its own private key and sends it to ECN_h: $\delta = (ID_{gNB_1}||TS_1||C||\Omega||AUTH_G)_{SK_{gNB_1}}$. Among them, TS_1 is a timestamp generated by gNB_1, which is used to indicate the freshness of the message.

Step-7: $ECN_h \rightarrow ECN_i$: $(AUTH_G||ID_{gNB_1}||\delta||C||\Omega||TS_1)$

After receiving the message, ECN_h broadcasts it to G. Each member first verifies the freshness of TS_1. Subsequently, each ECN_i calculates CK_i, IK_i, K^i_{AUSF}, K^i_{AMF} in the same way as $AUSF/UDM$, and verifies the correctness of $AUTH_i$ and δ according to the above calculation results. If all verifications are correct, ECN_i considers that $AUSF/UDM$, AMF_1, and gNB_1 are all legal. At this point, mutual authentication is completed, and ECN_i uses its d_i to extract the session key from the received C:

$$\xi = e(\sigma_{0,i}, c_1)e(h_i, c_2)$$

Finally, ECN_i and AMF_1 retains $GUTI_i$ and uses this temporary identity in future intra-domain handovers. If an inter-domain handover occurs, ECN_i updates $GUTI_i^{''} = H(SUPI_i, ID_{AMF_2}, K^i_{AMF_1})$.

4.3.2 Intra-domain Handover

In the 5G scenario, user movement is accompanied by multiple cell traversal. Intra-domain handover refers to handover between different gNBs within the same AMF. Once the threshold for handover authentication is reached, the MEC server as the local controller will notify gNB_1 and G to perform handover authentication based on the group signal strength report.

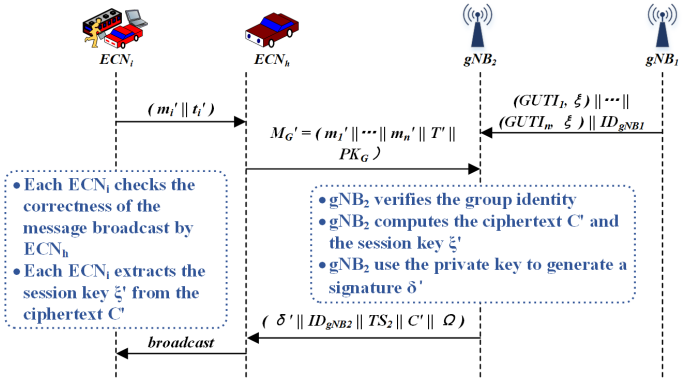


Fig. 3. Intra-domain handover

Step-1: $gNB_1 \rightarrow gNB_2$: After receiving the notification from the MEC server, gNB_1 will send G's authentication information to the target gNB in advance. That is, gNB_1 sends $((GUTI_1, \xi)||...||\ (GUTI_n, \xi)||ID_{gNB_1})$ to gNB_2.

Step-2: $ECN_h \rightarrow gNB_2$: $(M'_G = (m'_1||...||m'_n||T'||PK_G))$

Each ECN_i pre-select a new random number r'_i, and calculate the authentication message $m'_i = (GUTI_i||PK_i||r'_i)$ and $t'_i = F(\xi, m'_i)$. ECN_h aggregates after receiving all $(m'_i||t'_i)$, where $T'_1 = t'\mathbf{S}^T$, $T'_2 = (t^*)'\mathbf{X}^T$ and $T' = (T'_1, T'_2)$. Then ECN_h sends T' to gNB_2.

Step-3: $gNB_2 \rightarrow ECN_h$: $(\delta'||ID_{gNB_2}||TS_2||C'||\Omega)$

gNB_2 verifies $GUTI_i$ according to the messages sent by gNB_1 and ECN_h. Subsequently, gNB_2 calculates whether $t'\mathbf{S}^T$ is equal to the received T', if not, gNB_2 outputs the malicious identity list J and refuse this group to access. If $\mathbf{s} = T' - t'\mathbf{S}^T = 0$, gNB_2 uses the same method as Section 4.3.1 to calculate the ciphertext $C' = (c_1', c_2')$ and the session key $\xi' = (A_0)^{\beta'}$ in the same way, where $\beta' \in Z_p^*$ is randomly selected. Finally, gNB_2 calculates a signature $\delta' = (ID_{gNB_2}||TS_2||C'||\Omega)_{SK_{gNB_2}}$.

Step-4: $ECN_h \rightarrow ECN_i$: $(\delta'||ID_{gNB_2}||TS_2||C'||\Omega)$

ECN_h broadcasts this message to G, and each ECN_i verifies the correctness of the signature. If the verification is passed, the mutual authentication is completed. Finally, ECN_i uses its d_i to extract the session key $\xi' = e(\sigma_{0,i}, c_1')e(h_i, c_2')$.

4.3.3 Inter-domain Handover

When the source gNB_2 and the target gNB_3 are not in the same AMF, an inter-domain handover occurs. At this time, the group G needs to perform mutual authentication and negotiate a session key with gNB_3. As with intra-domain handover, when G reaches the handover threshold, SDN predicts the handover path, and informs G and AMF_1 to initiate inter-domain handover authentication.

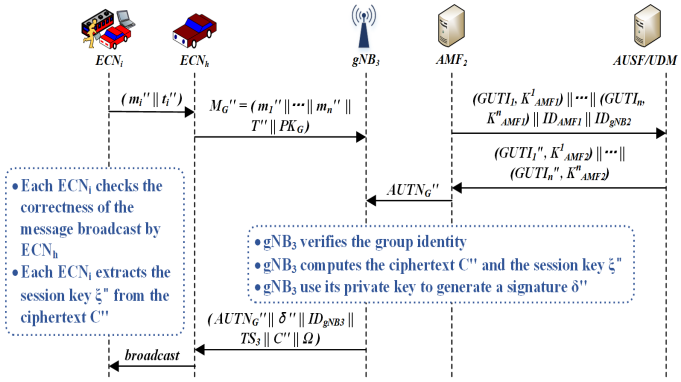


Fig. 4. Inter-domain handover

Step-1: $AMF_1 \rightarrow AMF_2$: $((GUTI_1, K^1_{AMF_1})||...||(GUTI_n, K^n_{AMF_1})||ID_{AMF_1}||ID_{gNB_2})$

Before G access, AMF_1 sends group message to AMF_2 in advance.

Step-2: $AMF_2 \rightarrow AUSF/UDM$: AMF_2 forwards the received message from AMF_1 to $AUSF/UDM$.

Step-3: $AUSF/UDM \rightarrow AMF_2$: $((K^1_{AMF_2}, GUTI_1'')||...||(K^n_{AMF_2}||GUTI_n''))$

Once the handover request message is received, $AUSF$ pre-computes a new anonymous identity $GUTI_i'' = H(SUPI_i, ID_{AMF_2}, K^i_{AMF_1})$ for ECN_i, and generates a security key $K^i_{AMF_2} = KDF(K^i_{AUSF}, ID_{AMF_2})$ shared by AMF_2 and ECN_i. Finally, AMF_2 stores $GUTI_i''$ and $K^i_{AMF_2}$.

Step-4: $AMF_2 \rightarrow gNB_3$: $(AUTH_G'' = (AUTH_1''||...||AUTH_n''||r_{AMF_2}))$

AMF_2 chooses a random number r_{AMF_2}, calculates $MAC^i_{AMF_2} = f_1(K^i_{AMF_2}, r_{AMF_2}, GUTI_i'')$ and $AUTH_i'' = (MAC^i_{AMF_2}, GUTI_i'', K^i_{AMF_1})$ for each $GUCI_i''$. Finally, AMF_2 sends its authentication token $AUTH_G''$ to gNB_3.

Step-5: $ECN_h \rightarrow gNB_3$: $(M_G'' = (m_1''||...||m_n''||T''||PK_G))$.

Members in G pre-select a random number r_i'', calculate $m_i'' = (GUTI_i''||PK_i||r_i'')$ and $t_i'' = F(K^i_{AMF_1}, m_i'')$. Then ECN_h generates $T'' = (T_1'', T_2'')$ as in Section 4.3.1.

Step-6: $gNB_3 \rightarrow ECN_h$: $(AUTH_G''||\delta''||ID_{gNB_3}||TS_3||C''||\Omega)$

If $s = T'' - t''\mathbf{S}^T = 0$, it proves that gNB_3 successfully authenticated G. Subsequently, gNB_3 computes the ciphertext $C'' = (c_1'', c_2'')$ and the session key ξ'' as in Section 4.3.1. Ultimately, gNB_3 generates a signature $\delta'' = (AUTH_G''||ID_{gNB_3}||TS_3||C''||\Omega)_{SK_{gNB_3}}$ and returns the necessary response message to ECN_h.

Step-7: $ECN_h \rightarrow ECN_i$: $(AUTH_G''||\delta''||ID_{gNB_3}||TS_3||C''||\Omega)$

ECN_h broadcasts this message to G. Each ECN_i verifies the signature δ'' to confirm whether the source of the message is legal. If the verification passes, it means that G has successfully authenticated gNB_3 and AMF_2. Finally, each ECN_i use their decryption key d_i to extract the session key $\xi'' = e(\sigma_{0,i}, c_1'')e(h_i, c_2'')$.

5 Security Analysis

In this section, we formally verify the proposed scheme by using BAN logic and the formal verification tool Scyther. Then, we analyze other security properties that the proposed scheme can achieve.

5.1 Logic Proof by BAN Logic

BAN logic is a logic for formal analysis of authentication protocols [46]. This logic deduces the final belief from the existing belief rules, and can judge whether the expected identity authentication can be achieved between the entities in the authentication protocol. Due to space limitations, this section uses the BAN logic to analyze the initial authentication protocol and intra-domain handover authentication protocol in Section 4.2. The notations of the BAN logic are given in TABLE 2, and the BAN logic rules we used are as follows:

R1. *The message-meaning rule:*

R1.1: $\frac{P|\equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}_K}{P|\equiv Q|\sim X}$, if P believes the shared key K between it and Q, and P receives the ciphertext $\{X\}_k$ encrypted by K, then P believes that Q has sent X.

R1.2: $\frac{P|\equiv \overset{K}{\rightarrow} Q, P \lhd \{X\}_{K^{-1}}}{P|\equiv Q|\sim X}$, if P believes that K is Q's public key, and P receives the ciphertext $\{X\}_{k^{-1}}$ encrypted by Q's private key k^{-1}, then P believes that Q has sent X.

R2. *The nonce-verification rule:*
$\frac{P|\equiv \sharp(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$, if P believes that X is fresh, and P believes that Q has sent X, then P believes that Q also believes X.

R3. *The decomposition rules:*
$\frac{P|\equiv (X,Y)}{P|\equiv X}$, if P believes both X and Y, then P also believes X.

R4. *The message-sending rule:*
$\frac{P|\equiv Q|\sim (X,Y)}{P|\equiv Q|\sim X}$, if P believes that Q has sent X and Y, then P believes that Q has also sent X.

R5. *The message-receiving rule:*
$\frac{P \lhd (X,Y)}{P \lhd X}$, if P receives (X, Y), then P also receives X.

R6. *The fresh-promotion rule:*
$\frac{P|\equiv \sharp(X)}{P|\equiv \sharp(X,Y)}$, if P believes that X is fresh, then P believes that Y sent at the same time as X is also fresh.

Proof of initial authentication protocol using BAN logic: According to the analysis steps of the BAN logic, we first ideally describe the messages of the initial authentication protocol, omitting the messages that are not helpful for the security proof of

TABLE 2
BAN Logic notations

notions	description
$P \mid\equiv X$	Entity P believes that formula X is true
$P \lhd X$	Entity P receives X
$P \mid\sim X$	Entity P has once sent X
$P \mid\Rightarrow X$	Entity P has jurisdiction over X
$\sharp(X)$	X is fresh
$P \overset{K}{\longleftrightarrow} Q$	K is the shared key between P and Q
$\overset{K}{\longrightarrow} P$	K is the public key of P
$\{X\}_K$	encrypt X with key K

the protocol. In particular, in order to improve the security of authentication, the group member ECN_i not only authenticates the identity of the gNB_1 but also authenticates the AMF_1 according to the received authentication token $AUTH_i$, and authenticates the AUSF/UDM according to the received AU_i. In addition, it has been assumed in the security model that a security association has been established among gNB, AMF, and AUSF/UDM, so the messages involved in the initial authentication protocol can be ideally described as follows:

Message 1. $ECN_i \rightarrow AUSF/UDM$: $m_i||t_i||PK_i||ID_{AMF_1}$, where $m_i = SUCI_i||PK_i||r_i$, $t_i = F(K_i, m_i)$.

Message 2. $AUSF/UDM \rightarrow ECN_i$: $AU_G = AU_i||r_{HN}$, where $AU_i = (K^i_{AMF_1}, GUTI_i, (r_i, SUPI_i)_{K^i_{AUSF}})$.

Message 3. $AMF_1 \rightarrow ECN_i$: $AUTH_G = AUTH_i||PK_G||r_{HN}$, where $AUTH_i = (MAC_{AMF^i_1}, GUTI_i)$ and $MAC^i_{AMF_1} = f_1(K^i_{AMF_1}, r_{HN}, r_i, (r_i, SUPI_i)_{K^i_{AUSF}})$.

Message 4. $gNB_1 \rightarrow ECN_i$: $AUTH_G||ID_{gNB_1}||\delta||C||\Omega||TS_1$, where $\delta = (ID_{gNB_1}||TS_1||C||\Omega||AUTH_G)_{SK_{gNB_1}}$.

According to the protocol description, the initial authentication protocol needs to complete the identity authentication of the AUSF/UDM to the ECN_i and the ECN_i to the entities participating in the initial authentication. Therefore, the security goals that need to be achieved are:

Goal 1. $AUSF/UDM \mid\equiv ECN_i \mid\equiv m_i$.
Goal 2. $ECN_i \mid\equiv gNB_1 \mid\equiv C$.
Goal 3. $ECN_i \mid\equiv AMF_1 \mid\equiv AUTH_i$.
Goal 4. $ECN_i \mid\equiv AUSF/UDM \mid\equiv AU_i$.

It is necessary for us to make the following security assumptions before the protocol is executed:

A1. $AUSF/UDM \mid\equiv ECN_i \overset{K_i}{\longleftrightarrow} AUSF/UDM$.
A2. $ECN_i \mid\equiv \overset{PK_{gNB_1}}{\longrightarrow} gNB_1$.
A3. $AUSF/UDM \mid\equiv \sharp(r_i)$.
A4. $ECN_i \mid\equiv \sharp(TS_1)$.
A5. $ECN_i \mid\equiv \sharp(r_{HN})$.
A6. $ECN_i \mid\equiv ECN_i \overset{K^i_{AMF_1}}{\longleftrightarrow} AMF_1$.

According to **Message 1** and message-receiving rule **R5**, we have:

$$AUSF/UDM \lhd t_i \tag{1}$$

From (1), assumption **A1** and message-meaning rule **R1.1** can be obtained:

$$AUSF/UDM \mid\equiv ECN_i \mid\sim m_i \tag{2}$$

From **Message 1**, assumption **A3** and fresh-promotion rule **R6**, we get:

$$AUSF/UDM \mid\equiv \sharp(m_i) \tag{3}$$

From (2), (3) and nonce-verification rule **R2**, we obtain:

$$AUSF/UDM \mid\equiv ECN_i \mid\equiv m_i \quad \textbf{(Goal 1)} \tag{4}$$

According to **Message 4** and message-receiving rule **R5**, we have:

$$ECN_i \lhd \delta \tag{5}$$

From (5), assumption **A2** and message meaning rule **R1.2**, we get:

$$ECN_i \mid\equiv gNB_1 \mid\sim (ID_{gNB_1}, TS_1, C, \Omega, AUTH_G) \tag{6}$$

From (6) and message-sending rule **R4**, it can be known that:

$$ECN_i \mid\equiv gNB_1 \mid\sim C \tag{7}$$

From **Message 4**, assumption **A4** and fresh-promotion rule **R6**, it can be deduced:

$$ECN_i \mid\equiv \sharp(AUTH_G, ID_{gNB_1}, \delta, C, \Omega, TS_1) \tag{8}$$

From (8) and decomposition rule **R3**, we have:

$$ECN_i \mid\equiv \sharp(C) \tag{9}$$

From (7), (9) and nonce-verification rule **R2**, we can prove:

$$ECN_i \mid\equiv gNB_1 \mid\equiv C \qquad \textbf{(Goal 2)} \tag{10}$$

By (6) and message-sending rule **R4**, we have:

$$ECN_i \mid\equiv gNB_1 \mid\sim AUTH_i \tag{11}$$

From **Message 3**, we know $AMF_1 \mid\Rightarrow AUTH_G$, and it has been assumed in Section 3.2 that a security association is established among gNB_1, AMF_1 and AUSF/UDM, so (11) can be seen as:

$$ECN_i \mid\equiv AMF_1 \mid\sim AUTH_i \tag{12}$$

From (8) and decomposition rule **R3**, we have:

$$ECN_i \mid\equiv \sharp(AUTH_i) \tag{13}$$

From (12), (13) and nonce-verification rule **R2**, we can prove:

$$ECN_i \mid\equiv AMF_1 \mid\equiv AUTH_i \quad \textbf{(Goal 3)} \tag{14}$$

According to **Message 3** and message-receiving rule **R5**, we have:

$$ECN_i \lhd MAC^i_{AMF_1} \tag{15}$$

By (15), assumption **A6** and message-meaning rule **R1.1** can be obtained:

$$ECN_i \mid\equiv AMF_1 \mid\sim (K^i_{AMF_1}, GUTI_i, r_{HN}, r_i, (r_i, SUPI_i)_{K^i_{AUSF}}) \tag{16}$$

By (16) and decomposition rule **R3**, we have:

$$ECN_i \mid\equiv AMF_1 \mid\sim AU_i \tag{17}$$

From **Message 2**, we know that $AUSF/UDM \mid\Rightarrow AU_G$. And we assume in the security model of Section 3.2 that a security association has been established between AMF_1 and AUSF/UDM, so (11) can be seen as:

$$ECN_i \mid\equiv AUSF/UDM \mid\sim AU_i \tag{18}$$

From **Message 2**, assumption **A5**, fresh-promotion rule **R6** and decomposition rule **R3**, we can get:

$$ECN_i \mid\equiv \sharp(AU_i) \tag{19}$$

From (18), (19) and nonce-verification rule **R2**, we can prove:

$$ECN_i \mid\equiv AUSF/UDM \mid\equiv AU_i \quad \textbf{(Goal 4)} \quad (20)$$

Proof of handover authentication protocol using BAN logic: The messages involved in intra-domain handover authentication are idealized as follows. Likewise, we omit messages that prove invaluable to this protocol:

Message 5. $ECN_i \rightarrow gNB_2$: $m_i'||t_i'||PK_i$, where $m_i' = GUTI_i||PK_i||r_i', t_i' = F(\xi, m_i')$.

Message 6. $gNB_2 \rightarrow ECN_i$: $ID_{gNB_2}||\delta'||C'||\Omega||TS_2$, where $\delta' = (ID_{gNB_2}||TS_2||C'||\Omega)_{SK_{gNB_2}}$.

According to the protocol description, the security goals that the intra-domain handover authentication protocol need to achieve are to complete the mutual authentication between the group member ECN_i and the base station gNB_2:

Goal 5. $gNB_2 \mid\equiv ECN_i \mid\equiv m_i'$.

Goal 6. $ECN_i \mid\equiv gNB_2 \mid\equiv C'$.

To analyze the intra-domain handover authentication protocol, we should have the following reasonable security assumptions:

A7. $gNB_2 \mid\equiv \sharp(r_i')$.

A8. $ECN_i \mid\equiv \sharp(TS_2)$.

A9. $gNB_2 \mid\equiv ECN_i \overset{\xi}{\longleftrightarrow} gNB_2$.

A10. $ECN_i \mid\equiv \overset{PK_{gNB_2}}{\longrightarrow} gNB_2$.

According to **Message 5** and message-receiving rule **R5**, we get:

$$gNB_2 \lhd t_i' \quad (21)$$

By (21), assumption **A9** and message-meaning rule **R1.1**, we have:

$$gNB_2 \mid\equiv ECN_i \mid\sim m_i' \quad (22)$$

From **Message 5**, assumption **A7** and fresh-promotion rule **R6**, we know:

$$gNB_2 \mid\equiv \sharp(m_i') \quad (23)$$

From (22), (23) and nonce-verification rule **R2**, we can prove:

$$gNB_2 \mid\equiv ECN_i \mid\equiv m_i' \quad \textbf{(Goal 5)} \quad (24)$$

According to **Message 6** and message-receiving rule **R5**, we have:

$$ECN_i \lhd \delta' \quad (25)$$

From (25), assumption **A10** and message meaning rule **R1.2**, we obtain:

$$ECN_i \mid\equiv gNB_2 \mid\sim (ID_{gNB_2}, TS_2, C', \Omega) \quad (26)$$

From (26) and message-sending rule **R4**, we know:

$$ECN_i \mid\equiv gNB_2 \mid\sim C' \quad (27)$$

From **Message 6**, assumption **A8** and fresh-promotion rule **R6**, it can be deduced:

$$ECN_i \mid\equiv \sharp(ID_{gNB_2}, \delta', C', \Omega, TS_2) \quad (28)$$

From (28) and decomposition rule **R3**, we have:

$$ECN_i \mid\equiv \sharp(C') \quad (29)$$

From (27), (29) and nonce-verification rule **R2**, we can prove:

$$ECN_i \mid\equiv gNB_2 \mid\equiv C' \quad \textbf{(Goal 6)} \quad (30)$$

Since the session key of the proposed scheme is extracted after the authentication protocol is executed, when using the BAN logic to analyze the authentication protocol, the mutual authentication between entities is only realized by authenticating the agreed-upon authentication token. Finally, we prove the beliefs of the goals through (4), (10), (14), (20), (24), and (30).

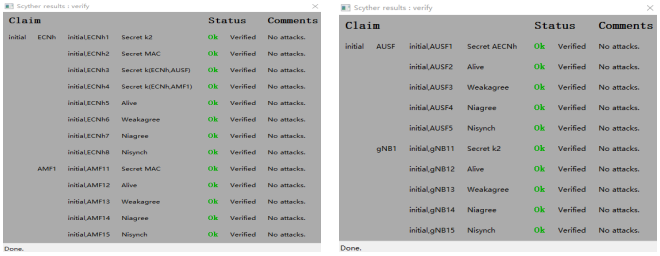
5.2 Formal Verification based on Scyther Tool

We use the Scyther tool [47] to formally verify the proposed initial authentication and intra-domain handover authentication protocol. The security properties of verified protocols mainly include *secrecy* and *authentication* [1].

```
const pk: Function;
const sk: Function;
inversekeys(pk, sk);
usertype text;
hashfunction T, KDF, f1, f2, f3;
const A, mECNh, MAC: text;
const rECNh,rHN: Nonce;

protocol initial (ECNh, gNB1, AMF1,
AUSF)
{
    role ECNh
    {
      var C,TS: Nonce;
      var k2: text;
      match(mECNh, (ECNh, pk(ECNh),
      rECNh));
      send_1(ECNh, AMF1, (mECNh,
      pk(ECNh), T));
      recv_5(gNB1, ECNh, (pk(ECNh),
      rHN, MAC, ECNh, gNB1, k2, C, A,
      TS));
      claim(ECNh, Secret, k2);
      claim(ECNh, Secret, MAC);
      claim(ECNh, Secret, k(ECNh,
      AUSF));
      claim(ECNh, Secret, k(ECNh,
      AMF1));
      claim(ECNh, Alive);
      claim(ECNh, Weakagree);
      claim(ECNh, Niagree);
      claim(ECNh, Nisynch);
    }
    role AMF1
    {
      var AECNh: text;
      send_2(AMF1, AUSF, (mECNh, T,
      pk(ECNh), AMF1));
      match(MAC, f1(k(ECNh, AMF1),
      rECNh, {rECNh, ECNh}k(ECNh,
      AUSF)));
      send_4(AMF1, gNB1, (pk(ECNh),
      rHN, MAC, ECNh));
      recv_1(ECNh, AMF1, (mECNh,
      pk(ECNh), T))
      recv_3(AUSF, AMF1, (AECNh,
      rHN));
      claim(AMF1, Secret, MAC);
      claim(AMF1, Alive);
      claim(AMF1, Weakagree);
      claim(AMF1, Niagree);
      claim(AMF1, Nisynch);
    }
    role AUSF
    {
      var AECNh: text;
      match(AECNh, (k(ECNh, AMF1),
      ECNh, {rECNh, ECNh}k(ECNh,
      AUSF)));
      send_3(AUSF, AMF1, (AECNh,
      rHN));
      recv_2(AMF1, AUSF, (mECNh, T,
      pk(ECNh), AMF1));
      claim(AUSF, Secret, AECNh);
      claim(AUSF, Alive);
      claim(AUSF, Weakagree);
      claim(AUSF, Niagree);
      claim(AUSF, Nisynch);
    }
    role gNB1
    {
      fresh C,TS: Nonce;
      fresh k2: text;
      match(k2, {gNB1, TS, C, A, rHN}
      sk(gNB1));
      send_5(gNB1, ECNh, (pk(ECNh),
      rHN, MAC, ECNh, gNB1, k2, C, A,
      TS));
      recv_4(AMF1, gNB1, (pk(ECNh),
      rHN, MAC, ECNh));
      claim(gNB1, Secret, k2);
      claim(gNB1, Alive);
      claim(gNB1, Weakagree);
      claim(gNB1, Niagree);
      claim(gNB1, Nisynch);
    }
}
```

(a) The initial authentication protocol is written in SPDL



(b) Formal verification results

Fig. 5. Verification result of initial authentication and key agreement under Scyther tool

The Scyther tool uses the Security Protocol Description Language (SPDL) to express different types of security protocol elements, such as protocol definitions, roles, and data types. The tool supports strong security models such as Dolev-Yao and eCK and provides several claims including $Secret$, $Alive$, $Weakagree$, $Niagree$, and $Nisynch$. These claims have strong security properties such as protecting the confidentiality of messages, detecting man-in-the-middle attacks, replay attacks, guaranteeing the forward and backward security of the protocol, and detecting key leakage. Scyther adopts the idea of black-box verification. Each role verifies whether it can meet the security goal or security

1. The main building blocks of the proposed scheme, i.e., aggregated message authentication codes with detecting functionality (AMAD) and contributory broadcast encryption, their security has been proved and they can be considered as abstract terms in formal verification. Therefore, we focus on the security of proposed protocol.

```
const pk: Function;
const sk: Function;
inversekeys(pk, sk);
usertype text;
usertype Sessionkey;
hashfunction T;
const A: text;

protocol intra(ECNh, gNB1, gNB2)
{
    role gNB1
    {
      fresh k1: Sessionkey;
      send_1(gNB1, gNB2, (gNB1, k1,
      ECNh));
    }
    role ECNh
    {
      fresh rECNh: Nonce;
      var k2: text;
      var C,TS: Nonce;
      var mECNh: text;
      match(mECNh, (ECNh, pk(ECNh),
      rECNh));
      send_2(ECNh, gNB2, (mECNh,
      pk(ECNh), T));
      recv_3(gNB2, ECNh, (k2, gNB2,
      TS, C, A));
      claim(ECNh, Secret, k2);
      claim(ECNh, Alive);
      claim(ECNh, Weakagree);
      claim(ECNh, Niagree);
      claim(ECNh, Nisynch);
    }
    role gNB2
    {
      fresh C, TS: Nonce;
      fresh k2: text;
      var k1: Sessionkey;
      var mECNh: text;
      match(k2, {gNB2, TS, C,
      A}sk(gNB2));
      recv_1(gNB1, gNB2, (gNB1, k1,
      ECNh));
      recv_2(ECNh, gNB2, (mECNh,
      pk(ECNh), T));
      send_3(gNB2, ECNh, (k2, gNB2,
      TS, C, A));
      claim(gNB2, Secret, k2);
      claim(gNB2, Alive);
      claim(gNB2, Weakagree);
      claim(gNB2, Niagree);
      claim(gNB2, Nisynch);
    }
}
```

(a) The handover authentication protocol is written in SPDL

Scyther results : verify

Claim				Status		Comments
intra	ECNh	intra,ECNh1	Secret k2	Ok	Verified	No attacks.
		intra,ECNh2	Alive	Ok	Verified	No attacks.
		intra,ECNh3	Weakagree	Ok	Verified	No attacks.
		intra,ECNh4	Niagree	Ok	Verified	No attacks.
		intra,ECNh5	Nisynch	Ok	Verified	No attacks.
	gNB2	intra,gNB21	Secret k2	Ok	Verified	No attacks.
		intra,gNB22	Alive	Ok	Verified	No attacks.
		intra,gNB23	Weakagree	Ok	Verified	No attacks.
		intra,gNB24	Niagree	Ok	Verified	No attacks.
		intra,gNB25	Nisynch	Ok	Verified	No attacks.

Done.

(b) Formal verification results

Fig. 6. Verification result of handover authentication and key agreement under Scyther tool

attribute from its perspective. If the declared security attribute cannot be satisfied, the attack output graph will show Failed, otherwise OK.

TABLE 3
Symbol correspondence table

Symbols in the SPDL model	Symbols in our proposed protocol
k_1	ξ
k_2	δ
$AECN_h$	A_i
$mECN_h$	m_i
A	Ω
MAC	MAC^i_{AMF}

In the model described with SPDL, ECN_h aggregates the authentication information of all group members, after receiving the message from the communicator, all ECN_i authenticate the communicator in the same way. Therefore, we let ECN_h represent the identity of the group. As long as ECN_h does not have vulnerabilities after verification in Scyther, it means that the whole group is safe. TABLE 3 shows the correspondence between the symbols in the SPDL model and the symbols in the protocol. Fig. 5 (a) illustrates the implementation of the initial authentication protocol in SPDL language, involving four roles ECN_h, gNB_1, AMF_1, and $AUSF$, ECN_h represents the user group, and the remaining three roles correspond to entities in the protocol. Fig. 6 (a) illustrates the implementation of the intra-domain handover authentication protocol, where gNB_1 represents the source BS, and gNB_2 represents the target BS. Finally, the output result of the model attacks are shown in Fig. 5 (b) and Fig. 6 (b). Obviously, the proposed scheme does not find any attack under the test of the Scyther tool and can satisfy the security attributes that the tool can detect, which proves the security of initial authentication and handover authentication protocols.

5.3 Other Security Properties

The formal verification in Sections 5.1 and 5.2 has proved that our scheme can achieve **mutual authentication**, and the Scyther tool has been used to verify that the signature δ will not be attacked and its confidentiality can be guaranteed. Therefore, after the initial authentication and handover authentication protocols are executed, the group member ECN_i can receive the ciphertext C from δ, and use its decryption key d_i to extract the session key ξ from C to implement **session key agreement**.

In addition, other security properties achieved by this scheme are as follows:

Anonymity and Traceability: ECN uses the anonymous identity $SUCI$ to initiate initial authentication. After the group passes the authentication, AUSF/UDM uses a hash function to generate a new temporary identity $GUTI$ for each member for intra-domain handover. When SDN predicts that the next handover is between different domains, ECN updates the $GUTI$, and AUSF/UDM also forwards the new $GUTI$ to the target AMF. In case of dispute, the one-way and collision resistance of the hash function can be used to prove that only the legitimate AUSF/UDM knows the true identity of ECN and traces its trajectory according to the way $GUTI$ is generated.

KEF: The decryption key and public key of each ECN_j ($j \in \mathbf{A}$) are generated from key materials provides by n group members, For ECN_j's decryption key:

$$d_j = (\sigma_{0,j}, ..., \sigma_{j-1,j}, \sigma_{j+1,j}, ..., \sigma_{n,j})$$

$$\sigma_{i,j} = \prod_{k=1}^{n} X_{i,k} h_j^{r_{i,k}}$$

where $X_{i,k}$ and $r_{i,k}$ are randomly selected by the remaining $n-1$ members except ECN_j. Since the group changes dynamically, once a member joins or leaves, this member performs the steps of ECN_k, as show in Section 4.2. And the group public key is calculated publicly.

$$PK_G = PK_0 \circledast ... \circledast PK_n = ((R_0, A_0), ..., (R_n, A_n))$$

Therefore, the proposed scheme does not require key escrow.

PFS/PBS: In Step 6 of Section 4.3.1, gNB will randomly select $\beta \in Z_p^*$ to generate different ciphertexts and different session keys each time. The process of extracting the session key from the ciphertext C using ECN_j's decryption key d_j is as follows:

$$\xi = e(\sigma_{0,j}, c_1) e(h_j, c_2)$$

$$= e(\prod_{k=1}^{n} X_{0,k} h_j^{r_{0,k}}, g^{\beta}) e(h_j, \prod_{k=1}^{n} R_{0,k}{}^{\beta})$$

$$= \prod_{k=1}^{n} e(X_{0,k}, g) = (A_0)^{\beta} = \xi$$

Assuming that the decryption key d_j of a current ECN_j is leaked, if the adversary wants to extract the session key from the previous/future ciphertext, it must extract $\sigma_{0,j} = \prod_{k=1}^{n} X_{0,k} h_j^{r_{0,k}}$ from d_j. Except for the secret parameter $r_{0,j}$ of ECN_j is known to the adversary, the rest of $r_{0,k}$ ($k \in \mathbf{A}$) are secretly generated and saved by the remaining n-1 members.

However, our scheme has established a secure authentication channel, and it is impractical to leak all the secret parameters $r_{0,k}$ of all members of the group. Therefore, the adversary cannot rely on the leaked d_j to extract $\sigma_{0,j}$, and thus cannot extract the session key from the previous/future ciphertext using only the d_j. In conclusion, our scheme can satisfy **PFS** and **PBS**.

Protocol Attack Resistance: Group members use random numbers r_i to generate message authentication codes and ensure the freshness of message authentication codes. The gNB also uses a timestamp TS to ensure the freshness of messages during authentication, which can prevent ***replay attacks***. All authentication messages are protected by shared keys, group public keys, session keys, hash functions or digital signatures, which are confidential and integral, and can resist ***impersonation attacks*** and ***man-in-the-middle attacks***. The security of the group key protocol used is based on the n-BDHE assumption, which has been proved in [10] to be fully collusion-resistant ***against semi-adaptively attacks***. In addition, our scheme supports multi-user authentication, which can alleviate ***DDoS attacks***.

Malicious User Identity Detection: In the most of handover authentication schemes, the whole group is rejected to access the network upon group authentication fails, but our scheme can output a list of malicious members through AMAD. If $\mathbf{s} \neq 0$, it means that there are malicious messages sent by some group members in the M_G. Subsequently, the receiver can call **Algorithm** 1 to detect and output a list of malicious identities, which effectively help the group to troubleshoot and improve the robustness of the group. For the detailed detection process of this algorithm, refer to Construction II in [9].

According to the proof results of construct II in [9], the proposed scheme equipped with AMAD has a good message compression rate and a malicious user detection rate. When $l = 10$, the message compression rate is about 1%, and the probability of detecting malicious users is about 91%.

6 Performance Evaluation

In this section, we briefly analyze the performance of the initial authentication and then analyze the performance of the handover authentication in detail[2].

To ensure the fairness of comparison, the entities involved in the initial authentication and handover authentication are abstracted into user equipment (UE), the serving network (SN: gNB/AMF/MME) and the home network (HN: AUSF/UDM/HSS). In all comparison schemes, we only consider the computational cost of cryptographic operations listed in TABLE 4 [48], where T_P, T_{ME}, T_{SM}, T_{RV} and T_H are the computational overhead of a pairing operation, a modular exponentiation, an elliptic curve scalar multiplication, an RSA signature verification, a one-hash or MAC operation, respectively.

TABLE 4
Computational cost of cryptography operations

(ms)	$\mathbf{T_P}$	$\mathbf{T_{ME}}$	$\mathbf{T_{SM}}$	$\mathbf{T_{RV}}$	$\mathbf{T_H}$
UE	2.87	0.225	0.2025	0.127	0.0013
BS	0.7616	0.0337	0.030	0.019	0.00079

In initial authentication stage, we compare with 5G-AKA and EAP-AKA' protocols [7]. We assume that *m* is the number of authentication vectors delivered by AUSF each time in 5G-AKA or EAP-AKA'. The 5G-AKA and EAP-AKA' protocols typically require public key encryption operations to protect identities, which may result in higher computational and communication overhead. Moreover, for the case of *n* users accessing, 5G-AKA' and EAP-AKA' need to perform *n* rounds of complete initial authentication, which increase the transmission overhead. From the comparison results in TABLE 5, the initial authentication protocol consumes less computational, communication and transmission overhead, which can effectively reduces the authentication delay and the probability of channel congestion.

TABLE 5
Comparison of overhead in initial authentication

schemes	Computational overhead	Communication overhead	Transmission overhead
5G-AKA [7]	$18nT_H$	(1920+768m)n	3na+4nb
EAP-AKA' [7]	$14nT_H$	(2048+768m)n	3na+4nb
ours	$11nT_H$	1666n+1152	2a+2b

In handover authentication stage, we compare with schemes [11], [15], [16], [18], [25], [28], [31], [32].

6.1 Computational Overhead

TABLE 6 shows the comparison of the computational overhead of the handover authentication schemes. In the proposed scheme, each ECN_i ectracts the session key after handover authentication is completed. In addition, since most of the schemes do not involve inter-domain handover, we only compare the UE side, BS side, and total overhead during intra-domain handover. The first five schemes are single-user access schemes with excellent handover performance, we multiply its computational overhead by n to compare with multi-user access schemes. The rest are multi-user schemes similar to us. To be more intuitive, (a)(b)(c) in Fig.7 are the results of comparison with single-user schemes. It can be seen that our computational overhead is slightly higher than that of CPPHA, SD-SIN and Rehand. However, ReHand needs to interact with HN far away, which will consume more transmission overhead. And (d)(e)(f) in Fig.7 are the comparison results with multi-user schemes. We find that with the increase of group members, the proposed handover authentication protocol is slightly higher than FTGPHA1 and superior to the other three schemes in terms of UE side, BS side and total computational overhead. For inter-domain handover, our computational overhead is $3nT_H+(n+1)T_{RV}+2T_{ME}$, which is slightly larger than intra-domain handover. This is because we authenticate AMF during the inter-domain handover, thereby enhancing the security.

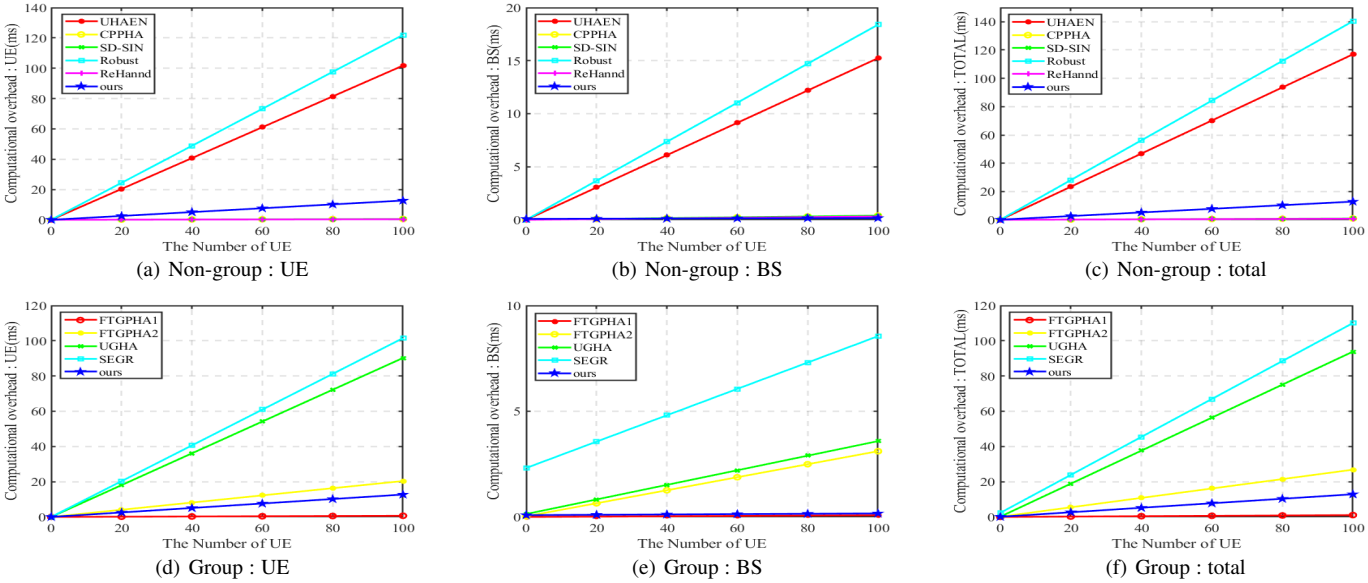
6.2 Communication Overhead

At this stage, we mainly compare the size of handover authentication messages in different schemes. In order to achieve the same security level of key strength, we assume that the encryption and decryption key length of AES is 128 bits, the key length of ECC-based algorithm is 256 bits, and the length of the RSA algorithm is 3072 bits. Moreover, the length of identity information such as $SUCI$ and $GUTI$ is defined as 128bits, the length of message output by the hash or MAC function is 128 bits, the output size of the Chebyshev chaotic map is 128 bits, the random number is 128 bits, and the timestamp is 32 bits. The size of the aggregated message authentication code T output in our scheme is 1n bits. TABLE 7 lists the communication overhead of the handover authentication schemes, and Fig.8 (a)(b) are comparisons with the single-user schemes and the multi-user

2. Here we do not consider the overhead of group key agreement since we mainly focus on the authentication overhead during handover. Although the process of group key agreement introduces some computational overhead, it is performed offline and will not influence the performance of the handover.

TABLE 6
Comparison of computational overhead

schemes	T_{UE} in HO authentication	T_{BS} in HO authentication	T_{tot}
UHAEN [11]	$(5T_{SM}+4T_H)$n =1.0177n	$(5T_{SM}+3T_H)$n =0.15237n	$(10T_{SM}+7T_H)$n =1.17007n
CPPHA [15]	$(4T_H)$n =0.0052n	$(5T_H)$n =0.00395n	$(9T_H)$n =0.00915n
SD-SIN [16]	$(4T_H)$n =0.0052n	$(5T_H)$n =0.00395n	$(9T_H)$n =0.00915n
Robust [18]	$(6T_{SM}+4T_H)$n =1.2202n	$(6T_{SM}+5T_H)$n =0.18395n	$(12T_{SM}+9T_H)$n=1.40415n
ReHend [28]	$(3T_H)$n =0.0039n	$(4T_H)$n =0.00316n	$(8T_H)$n =0.00785n
FTGPHA1 [25]	$5nT_H$ =0.0065n	nT_H =0.00079n	$10nT_H$=0.01045n
FTGPHA2 [25]	nT_{SM}+(n+1)T_H =0.2038n + 0.0013	(n+1)T_{SM}+nT_H =0.03079n+0.03	(3n+4)T_{SM}+(5n+2)T_H=0.26696n+0.12209
UGHA [31]	$4nT_{ME}$+2nT_H=0.9026n	(n+4)T_{ME}+(n+3)T_H=0.03449n+0.13717	(5n+4)T_{ME}+(3n+3)T_H=0.93709n+0.13717
SEGR [32]	$5nT_{SM}$+2nT_H = 1.0151n	(2n+1)T_{SM}+3nT_H+3T_P = 0.06237n+2.3148	(7n+1)T_{SM}+5nT_H+3T_P = 1.07747n+2.3148
ours	nT_{RV} =0.127n	nT_H+2T_{ME}+T_{RV} =0.00079n+0.0864	nT_H+(n+1)T_{RV}+2T_{ME} =0.12779n+0.0864



(a) Non-group : UE (b) Non-group : BS (c) Non-group : total

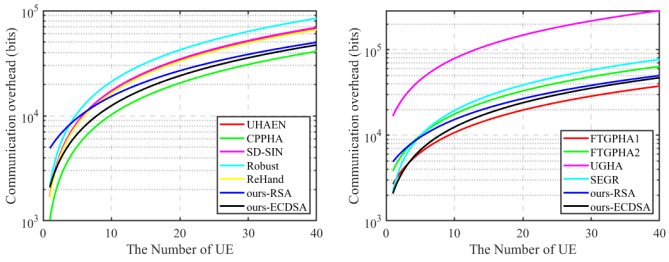
(d) Group : UE (e) Group : BS (f) Group : total

Fig. 7. Computational cost of non-group and group handover authentication

TABLE 7
Comparison of communication overhead

schemes	Comparison of communication overhead in handover authentication (bits)
UHAEN [11]	(640+896+128)n=1664n
CPPHA [15]	(512+384+128)n=1024n
SD-SIN [16]	(672+544+128+384)n=1728n
Robust [18]	(928+1056+128)n=2112n
ReHand [28]	(850+288+384+128)n=1650n
FTGPHA1 [25]	128+256n+128n+256+128n+256+256n+128+384+384+256+128n=896n+1792
FTGPHA2 [25]	512n+256+512n+256+384n +512+512+512+256+128n=1536n+2304
UGHA [31]	3584n+3200n+3456+6400+128n=6912n+9856
SEGR [32]	896n+256n+256+384n+384n=1920n+256
ours	640n+513n+256+3488+n=1154n+3744 (RSA) /640n+513n+256+672+n=1154n+928 (ECDSA)

schemes, respectively. Obviously, as n increases, our handover authentication protocol has lower communication overhead, but it is slightly higher than the CPPHA and FTGPHA1 schemes. In Fig. 8 (b), in order to achieve the same security strength as other types of cryptographic algorithms, the key length of the finite-field-based algorithm used by UGHA [31] leads to high communication overhead. In the proposed handover authentication protocol, gNB can use any signature algorithm to sign to prove the legitimacy of the sent messages, Fig.8 shows the communication overhead when gNB uses the RSA algorithm or the ECDSA algorithm. When there are few group members, the communication overhead of using ECDSA signature is significantly lower than using RSA signature. Since we provide the group G authenticates AMF in inter-domain handover, the communication will increase, which is 1537n + 3744 (RSA)/1537n + 928 (ECDSA).



(a) non-group (b) group

Fig. 8. Communication cost of non-group and group handover authentication

6.3 Transmission Overhead

Assumed that the transmission overhead incurred by delivering a piece of signaling between UE and SN is a unit, that between SN and HN is b unit, and that between UEs is ignored. Generally,

the distance between SN and HN is much larger than that between UE and SN, i.e., $b \gg a$. TABLE 8 lists the transmission overhead of handover authentication schemes supporting single-user and multi-user. Fig. 9 depicts the analysis results of the transmission overhead when $a = 1$ and $b = 100$. The transmission overhead of all multi-user schemes are lower than that of single-user schemes, because the multi-user schemes adopt mechanisms such as aggregated signature or batch authentication, which can effectively reduce transmission overhead and alleviate channel congestion. The ReHand, FTGPHA1 and FTGPHA2 schemes require HN to implement user authentication and key agreement, resulting in a large amount of transmission overhead. In addition, compared with the multi-user schemes in Fig.9, our scheme has the lowest transmission overhead. The first four steps in Section 4.3.3 are sent in advance when the handover threshold is reached, so the transmission overhead of the inter-domain handover authentication is still $2a$.

TABLE 8
Comparison of transmission overhead

schemes	Transmission overhead
UHAEN [11]	$3na$
CPPHA [15]	$3na$
SD-SIN [16]	$3na$
Robust [18]	$3na$
ReHand [28]	$3na + nb$
FTGPHA1 [25]	$3a + 4b$
FTGPHA2 [25]	$3a + 4b$
UGHA [31]	$3a$
SEGR [32]	$na + a$
ours	2a

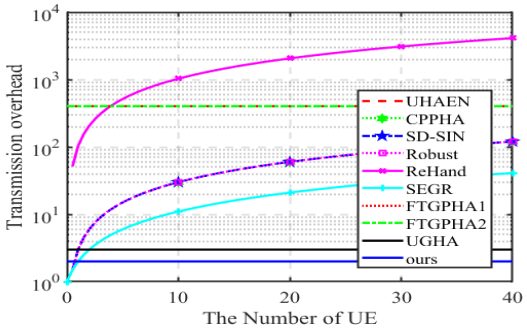


Fig. 9. Transmission overhead

6.4 Comprehensive discussion and Functionality Comparison

Judging from the analysis results of the computational, communication, and transmission overhead, our scheme is slightly inferior to CPPHA, SD-SIN, ReHand and FTGPHA1 in terms of computational overhead, and slightly inferior to CPPHA and FTGPHA1 in terms of communication overhead. However, the transmission overhead of our scheme is the lowest among these schemes, especially far less than the transmission overhead of single-user schemes. For ReHand and FTGPHA, both of them require key materials or authentication information provided by HN to achieve mutual authentication and key agreement, which will cause more time delay. In terms of realized functions, as show in TABLE 9, our scheme realizes anonymity, traceability, KEF, PFS/PBS, and can resist multiple protocol attacks. However, CPPHA, SD-SIN, ReHand and FTGPHA1 do not implement Key Escrow Freedom (KEF) and Perfect Forward/Backward Secrecy (PFS/PBS), and SD-SIN cannot guarantee user anonymity. In particular, our scheme provides the function of communicating with specified group members, the BS can negotiate a session key with the expected receiving member. For malicious messages, we use AMAD to accurately output the corresponding list of malicious identities, which helps the group's troubleshooting and improves the group's robustness. The proposed scheme also has a higher message compression rate, which can reduce communication overhead.

Furthermore, the proposed scheme fully discusses initial authentication, intra-domain handover authentication, and inter-domain handover authentication. Although some of the existing schemes consider the initial authentication, they just directly use 5G-AKA in the 3GPP standard for key material preparation and does not design authentication scheme suitable for multi user access. Except for our scheme, other schemes does not distinguish the intra and inter handover authentication and some of them does not discuss the inter-domain handover authentication in detail. Among these schemes, only part of them are suitable for inter-domain handover authentication. In conclusion, for multi user access scenario, our scheme not only has moderate computational and communication overhead, lower transmission overhead, but also provides powerful security functions.

7 Conclusions

Under the network architecture of MEC and SDN integration, we have proposed a novel authentication scheme supporting multi-user access based on AMAD and contributory broadcast encryption technique. The proposed scheme possesses initial authentication, intra-domain and inter-domain handover authentication, which can simplify the authentication process, reduce handover delay and the number of signaling interactions. Through security analysis and the use of the Scyther tool, the proposed scheme can realize a variety of security functions. In particular, it can detect malicious identities, and the gNB can communicate securely with specific group members. By comparing with existing schemes in terms of computational, communication and transmission overhead, and functions, it can be seen that our scheme has advantages over most of the existing schemes.

Acknowledgments

This work is supported by the Key Research and Development Program of Shaanxi Province under 2021ZDLGY06-02, and the National Natural Science Foundation of China Research under Grant 62072369.

References

[1] C. Lai, M. Zhang, J. Cao, and D. Zheng, "Spir: A secure and privacy-preserving incentive scheme for reliable real-time map updates," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 416–428, 2020.

[2] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5g and beyond," *IEEE Communications Surveys Tutorials*, vol. 21, no. 4, pp. 3682–3722, Fourthquarter 2019.

[3] M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. Le Moullec, "A survey on the roles of communication technologies in iot-based personalized healthcare applications," *IEEE Access*, vol. 6, pp. 36 611–36 631, 2018.

[4] J. Du, F. R. Yu, G. Lu, J. Wang, J. Jiang, and X. Chu, "Mec-assisted immersive vr video streaming over terahertz wireless networks: A deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9517–9529, 2020.

[5] H. Jayakumar, A. Raha, Y. Kim, S. Sutar, W. S. Lee, and V. Raghunathan, "Energy-efficient system design for iot devices," in *21st Asia and South Pacific Design Automation Conference, ASP-DAC 2016, Macao, Macao, January 25-28, 2016*. IEEE, 2016, pp. 298–301. [Online]. Available: https://doi.org/10.1109/ASPDAC.2016.7428027

TABLE 9
Functionality comparison

schemes	MAKA	Anonymity	Traceability	KEF	PFS	PBS	Communicating with specified group members	Malicious messages detecting	Authentication stages Initial, Intra, Inter
UHAEN [11]	√	√	×	×	√	×	-	-	Initial, Intra, Inter
CPPHA [15]	√	√	√	×	×	×	-	-	Intra, Inter
SD-SIN [16]	√	×	×	×	×	×	-	-	Initial, Intra
Robust [18]	√	√	√	√	√	×	-	-	Initial, Intra, Inter
ReHand [28]	√	√	√	×	×	×	-	-	Initial, Intra
FTGPHA1 [25]	√	√	√	×	×	×	×	×	Intra, Inter
FTGPHA2 [25]	√	√	√	×	√	√	×	×	Intra, Inter
UGHA [31]	√	×	×	×	×	×	×	×	Intra
SEGR [32]	√	×	×	√	√	√	×	×	Initial, Intra, Inter
ours	√	√	√	√	√	√	√	√	Initial, Intra, Inter

Initial, Intra, Inter: If a scheme proposes an initial authentication protocol, and can realize intra-domain handover authentication and inter-domain handover authentication, fill in Initial, Intra, Inter in the corresponding positions in the last column of TABLE 9.
√: The scheme can implement this function. **×:** The scheme cannot implement this function. **-:** The function is not suitable for single-user authentication schemes
MAKA: Mutual authentication and key agreement. **KEF:** Key Escrow Freedom. **PFS:** Perfect Forward Secrecy. **PBS:** Perfect Backward Secrecy.

[6] T. Yang, H. Feng, S. Gao, Z. Jiang, M. Qin, N. Cheng, and L. Bai, "Two-Stage Offloading Optimization for Energy-Latency Tradeoff With Mobile Edge Computing in Maritime Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5954–5963, 2020.

[7] *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System(Rel. 15), V15.3.1*, 3GPP Standard TS 33.501, Dec. 2018.

[8] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," *IEEE Network*, vol. 34, no. 2, pp. 37–45, 2020.

[9] 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)*, 2020, pp. 868–873.

[10] 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 Trans. Computers*, vol. 65, no. 2, pp. 466–479, 2016. [Online]. Available: https://doi.org/10.1109/TC.2015.2419662

[11] 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.

[12] L. Cai, S. Machiraju, and H. Chen, "Capauth: A capability-based handover scheme," in *2010 Proceedings IEEE INFOCOM*, 2010, pp. 1–5.

[13] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, 2010.

[14] X. Duan and X. Wang, "Authentication handover and privacy protection in 5g hetnets using software-defined networking," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28–35, 2015.

[15] 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*, pp. 1–1, 2019.

[16] K. Xue, W. Meng, H. Zhou, D. S. L. 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.

[17] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2019.

[18] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5g hetnets," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–1, 2019.

[19] V. Sharma, I. You, F. Palmieri, D. N. K. Jayakody, and J. Li, "Secure and energy-efficient handover in fog networks using blockchain-based dmm," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 22–31, 2018.

[20] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[21] R. Roman, J. López, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2016.11.009

[22] C. Wang, Y. Zhang, X. Chen, K. Liang, and Z. Wang, "Sdn-based handover authentication scheme for mobile edge computing in cyber-physical systems," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8692–8701, 2019.

[23] Y. Sun, S. Zhou, and J. Xu, "Emm: Energy-aware mobility management for mobile edge computing in ultra dense networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2637–2646, 2017.

[24] 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 Inf. Secur.*, vol. 14, no. 1, pp. 21–29, 2020. [Online]. Available: https://doi.org/10.1049/iet-ifs.2018.5443

[25] 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 Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2126–2140, 2020. [Online]. Available: https://doi.org/10.1109/TVT.2019.2960313

[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] 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, 2012.

[28] C. Fan, J. Huang, M. Zhong, R. Hsu, W. 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, 2020.

[29] C. Lai, Q. Li, H. Zhou, and D. Zheng, "Srsp: A secure and reliable smart parking scheme with dual privacy preservation," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[30] 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.

[31] 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)*, 2015, pp. 7246–7251.

[32] 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)*, 2014, pp. 1011–1016.

[33] X. Huang, R. Yu, J. Kang, Y. He, and Y. Zhang, "Exploring mobile edge computing for 5g-enabled software defined vehicular networks," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 55–63, 2017.

[34] 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.

[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] 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, 2017.

[37] 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, 2019.

[38] 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, 2017.
[39] 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.
[40] 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, 2016.
[41] 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)*, 2021, pp. 29–34.
[42] L. Harn, "Group authentication," *IEEE Transactions on Computers*, vol. 62, no. 9, pp. 1893–1898, 2013.
[43] "Ieee standard for wireless access in vehicular environments security services for applications and management messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, pp. 1–289, 2013.
[44] "Ieee standard for wireless access in vehicular environments (wave) – multi-channel operation," *IEEE Std 1609.4-2016 (Revision of IEEE Std 1609.4-2010)*, pp. 1–94, 2016.
[45] Y. Hou, S. Garg, L. Hui, D. N. K. Jayakody, R. Jin, and M. S. Hossain, "A data security enhanced access control mechanism in mobile edge computing," *IEEE Access*, vol. 8, pp. 136 119–136 130, 2020.
[46] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," in *Proceedings of the Twelfth ACM Symposium on Operating System Principles, SOSP 1989, The Wigwam, Litchfield Park, Arizona, USA, December 3-6, 1989*, G. R. Andrews, Ed. ACM, 1989, pp. 1–13. [Online]. Available: https://doi.org/10.1145/74850.74852
[47] C. J. F. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Computer Aided Verification, 20th International Conference, CAV 2008, Princeton, NJ, USA, July 7-14, 2008, Proceedings*, ser. Lecture Notes in Computer Science, A. Gupta and S. Malik, Eds., vol. 5123. Springer, 2008, pp. 414–418. [Online]. Available: https://doi.org/10.1007/978-3-540-70545-1_38
[48] M. J. Alam and M. Ma, "DC and CoMP Authentication in LTE-Advanced 5G HetNet," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, 2017, pp. 1–6.

Chengzhe Lai received his B.S. degree in information security from Xi'an University of Posts and Telecommunications in 2008 and a Ph.D. degree from Xidian University in 2014. He was a visiting Ph.D. student with the Broadband Communications Research (BBCR) Group, University of Waterloo from 2012 to 2014. He is a professor at School of Cyberspace Security, National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts and Telecommunications. He has published research articles in IEEE TITS, IEEE TVT, IEEE TCC, Computer Networks, Globecom, ICC, etc. He served for the program committee of several conferences and the editorial members of several international journals. His research interests include wireless network security and privacy preservation.

Yixiao Ma received the B.S. degree in information security from Xi'an University of Posts and Telecommunications in 2019. She is currently pursuing the master's degree with Cyberspace Security, Xi'an University of Posts and Telecommunications, Xian, China. Her research interests include cryptography, 5G security and privacy preservation.

Rongxing Lu received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012. He was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2013 to 2016. He has been an Associate Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Fredericton, NB, Canada, since 2016. He was a Post-Doctoral Fellow with the University of Waterloo, from 2012 to 2013. Dr. Lu was a recipient of the Governor Generals Gold Medal for his Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, the 8th IEEE Communications Society (ComSoc) AsiaPacific Outstanding Young Researcher Award in 2013, and the 2016 to 2017 Excellence in Teaching Award from FCS, UNB. He is currently serves as the ViceChair (Publication) of IEEE ComSoc CIS-TC.

Yinghui Zhang received his Ph.D degree in Cryptography from Xidian University, China, in 2013. He is a professor at School of Cyberspace Security, National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts and Telecommunications. He has published research articles in ACM ASIACCS, ACM Computing Surveys, IEEE TDSC, IEEE TSC, IEEE TCC, IEEE TII, Computer Networks, Computers & Security, etc. He served for the program committee of several conferences and the editorial members of several international journals in information security. His research interests include public key cryptography, cloud security and wireless network security.

Dong Zheng received an M.S. degree in mathematics from Shaanxi Normal University, Xi'an, China, in 1988, and a Ph.D. degree in communication engineering from Xidian University, in 1999. He was a professor in the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a professor at Xi'an University of Posts and Telecommunications and is also connected with the National Engineering Laboratory for Wireless Security, Xi'an, China. His research interests include provable security and new cryptographic technology.