Efficient Group Handover Authentication for Secure 5G-based Communications in Platoons

Xiaobei Yan, Maode Ma, and Rong Su

***Abstract*—In recent years, the world of vehicular communication is in full progress. With the emergence of the fifth-generation (5G) technology, the high bandwidth and low latency features in the 5G vehicle to everything (5G-V2X) network become possible. However, the current 5G mechanism specified by the Third Generation Partnership Project (3GPP) Release 16 incurs high signaling overhead over the radio access network and the core network when a vehicle platoon moves from a source base station to the target base station. Moreover, it also has several security problems in terms of the failure of key forward secrecy (KFS) and lack of mutual authentication. In this paper, we propose an efficient authentication protocol for vehicle platoons in all handover scenarios. By the proposal, the identities of base stations and vehicles are mutually authenticated by certificateless aggregated signatures, which can also reduce signaling overhead and is free from key escrow problems. The proposed protocol has been formally evaluated by BAN-logic and the Scyther tool to show its ability to resist major typical malicious attacks. It has also been analyzed on its security functionality. The performance evaluation demonstrates that the proposed protocol is efficient in terms of signaling, computational and communication cost.**

***Index Terms*—secure handover, vehicle platoon, 5G-V2X, certificateless aggregate signature**

I. Introduction

In recent years, vehicular communications technologies are evolving fast. The interconnection between vehicles promises a safer and more enjoyable driving experience by information exchanges, such as notifying bad weather conditions or traffic jams [1]. As the 5th Generation mobile networks (5G) have been deployed commercially around the world, the cellular vehicle-to-everything (C-V2X) communication, which is specified by 3GPP for communications assisted by the gNodeB (gNB), has been considered as a promising communication method for vehicles due to its low latency. [2] With the large-scale device connectivity in 5G and the rapid growth in the number of vehicles, grouping vehicles into platoons has been investigated as a promising strategy of traffic management for road transportation. For example, the authors in [3] have proposed a resource allocation strategy to support larger platoon size in a multi-lane platoon system. And authors in [4] have investigated security solutions in the group-oriented vehicular environment.

Due to the openness of wireless channels, the security of the vehicle network has become a major concern. However, the group handover authentication has not been carefully considered by the current standard. Security requirements in 5G mainly includes confidentiality, integrity, authenticity, privacy, and availability. [5] However, it has been pointed out in [6] and [7] that there are security vulnerabilities in the handover authentication process including lack of mutual authentication, failed Key Forward Secrecy (KFS), and vulnerability to Denial of Service (DoS) attacks, etc. Also, the current standard is incapable to protect users' privacy (vehicle's identity, moving pattern, etc.). And it incurs severe signaling overloads to a vehicle platoon. As a large number of vehicles in a platoon may hand over from the source gNB (s-gNB) to the target gNB (t-gNB) in a short period, which may cause high signaling overhead. The handover can happen even more frequently in the 5G network, as the 5G has employed smaller cells than the Long Term Evolution (LTE). [8]

To mitigate the shortcomings, we propose our Efficient Group Handover Authentication protocol, which is named as EGHA. It contains the following outstanding features: 1) The protocol can achieve major security properties through cryptography methods while preserving the architecture of the 3GPP standard R16. And the protocol is suitable for all handover scenarios defined by 3GPP. 2) The scheme contains a novel method against DoS attacks caused by aggregating MAC or signature. 3) The privacy information (route, identity, etc) of each vehicle in the platoon is protected by using a temporary ID (TID), which is trackable to the core network and does not require the public key encryption. 4) The protocol utilizes the time slot induced by the gap between the first and second vehicles entering the new coverage area to mitigate the latency.

The remaining paper is organized as follows: Section 2 presents the literature survey. Section 3 explains the background knowledge. Section 4 shows the system model. Section 5 shows the proposed protocol. Section 6 presents the security analysis. Section 7 shows the results of the performance evaluation. Section 8 is the conclusion.

II. Related Work

Related studies are compared in this section. Unfortunately, there are few research focusing on vehicle platoon handover authentication based on 5G. Also, existing research work has weaknesses in terms of security or efficiency. An overview of each scheme is compared in Table I.

Authors in [9] have proposed a platoon authentication handover protocol in the 5G-V2X network. The signaling overhead has been reduced by Aggregated Message Authentication Codes (AMACs) techniques. However, this scheme

Xiaobei Yan and Rong Su (corresponding author) are with School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. E-mail: Xiaobei Yan: xiaobei001@e.ntu.edu.sg, Rong Su: rsu@ntu.edu.sg.

Maode Ma is with College of Engineering, Qatar University, Qatar. Email: mamaode@qu.edu.qa

TABLE I
COMPARISON OF RELATED WORKS

Scheme	Year	Network	Entity	Group authentication technique	Crypto-system	Authentication type	Security proof techniques
[9]	2020	5G-V2X	Vehicle	AMAC	A	HO auth	No Proof
[1]	2019	5G	Vehicle	Request aggregation	S	auth and re-auth	AVISPA [10] and SPAN [11]
[12]	2020	5G V2V/V2P	Vehicle	None	A	HO auth	No Proof
[13]	2016	LTE-A	UE	None	S	HO auth	No Proof
[14]	2022	5G	MTCD	AMAC and SCT	S	HO auth	Scyther [15]
[16]	2015	LTE-A	MTCD	SCT	S	HO auth	No Proof
[17]	2013	IEEE 802.16m	MTCD	SCT	A	HO auth	AVISPA
[18]	2015	LTE-A	MTCD	Multi-signature and AMAC	A	HO auth	No Proof
[19]	2017	LTE-A	MTCD	AMAC	S	IN and HO auth	BAN-logic [20] and Scyther
[21]	2019	LTE-A	MTCD	Message aggregation	A	HO auth	AVISPA
[22]	2019	5G	MTCD	AMAC	A+S	HO auth	Tamarin [23]
[24]	2017	LTE-A	MTCD	AMAC	A	HO auth	No Proof
[25]	2017	5G-WLAN	MTCD	AMAC	A	HO and re-auth	AVISPA, SPAN, BAN logic
[26]	2020	5G	ECN	AMAC	A	HO auth	No Proof
[27]	2019	LTE	MTCD	AMAC	S	HO auth	AVISPA

Abbreviations: user equipment (UE), machine-type communication devices (MTCDs), asymmetric cryptosystem (A), symmetric cryptosystem (S), handover (HO), initial (IN), authentication (auth), security context transmission (SCT), aggregated message authentication code (AMAC), edge computing nodes (ECN)

requires several point multiplication operations during handover authentication, which is very time-consuming. Also, this protocol cannot preserve vehicles' privacy as identities have been transmitted in plaintext from each vehicle to the group leader over an insecure channel. Moreover, the protocol suffers from DoS attacks as the AMAC can be successfully verified only if all members are legal. An attacker can send false MACs to the group leader and make entire group verification fail deliberately. This problem appears in all protocols which adopt the aggregation technique. Authors in [1] have proposed an authentication and reauthentication protocol for vehicle platoons in 5G networks. It has only utilized simple cryptographic operations and thus is efficient in computational overhead. However, it has a high communicational cost as the length of the message is proportional to the square of the group size. Also, this protocol cannot protect a vehicle's privacy. Authors in [12] proposed an efficient handover authentication protocol for 5G V2V or Vehicle to Pedestrian (V2P) systems. Elliptic Curve Diffie–Hellman (ECDH) algorithm is introduced for secure exchange of secret keys between vehicles and their control function, however, this may introduce high overhead. They also evaluate the protocol's performance with respect to varying levels of vehicle density and transmission distances.

Also, besides vehicle platoons, many authors have proposed solutions for handover authentication for a group of UEs or Machine-Type Communication Devices (MTCDs). Authors in [13] have proposed a secure authentication protocol for group handover with the mobile relay. Authors in [14] have proposed an efficient authentication protocol for a group of MTCDs in all handover scenarios specified by 3GPP. The scheme has adopted the symmetric-based cryptosystem and therefore is efficient in terms of overhead. The authors in [16] [17] have presented a Security Context Transmission (SCT)-based protocol, by which the s-gNB transmits the security contexts of all the group members when the first MTCD enters the communication coverage of the t-gNB. The SCT-based protocol may cause key leakage problems. Because if some group members suddenly leave the group after the security context has been transmitted to the t-gNB, the session keys of these members will be known by t-gNB. Moreover, the protocol in [16] cannot achieve Key Forward Secrecy (KFS) and is lack of mutual authentication. The SCT protocol in [17] has used the Elliptic Curve Cryptography (ECC) which can incur high computational overheads. The authors in [17] [18] [19] [21] [22] [24] [25] have used AMACs or aggregated signatures and send the aggregated information to the network. As mentioned before, the aggregation-based solutions usually are vulnerable to DoS attacks. Moreover, the solution in [18] suffers from the key escrow problem and has a high computational cost because of the modular exponentiation algorithm used. The solution in [19] has a lower computation overhead, while it cannot support a dynamic change of group members. And it also has some security problems such as lack of authentication for the control mobile relay nodes, failed KFS/Key backward secrecy (KBS), and failure to preserve the privacy of the MTCDs. The solution in [21] has proposed a universal protocol for N2 and Xn handovers. But it also has a high computation overhead because of the ECC and the proxy signature used. The authors in [22] have proposed 2 protocols for different security requirements. However, it is only suitable for fixed-trajectory movements. The solution in [24] has a high computation overhead due to the use of the modular exponentiation algorithm. Authors in [26] proposed an anonymous handover authentication scheme which supports multi-user access. They used AMAC with detection function (AMAD) technique to simultaneously authenticated multiple entities. However, this scheme still requires several point multiplication operations during handover authentication, which may increase overhead. Authors in [27] have proposed a group-based secure lightweight handover authentication (GSLHA) protocol for M2M communication. They only use symmetric cryptography in their scheme and therefore is efficient in terms of computational overhead. However, it has failed key forward secrecy as the secret keys are transferred to the target base station from the source base station. Therefore, the protocol may lead to the impersonation and eavesdropping attacks.

III. Preliminaries

In this section, we introduce the concepts and cryptographic techniques that will be used in this paper.

A. Key Management in 3GPP 5G Handover

In the 5G key hierarchy, a long-term secret key K is pre-stored in the Authentication credential Repository and Processing Function (ARPF) and the Universal Subscriber Identity Module (USIM). The network side functions and the vehicle use the key K to generate session keys and integrity keys at a lower layer step by step. The K_{AUSF} is used to secure communication between the vehicle and ARPF. Then an anchor key K_{SEAF} can be derived using K_{AUSF}. The K_{SEAF} also works as an intermediate key to derive K_{AMF}. The K_{gNB} is derived by Access and Mobility Management Function (AMF) and sent to gNB to secure communication between the gNB and the vehicle. If a vehicle moves from the s-gNB to another gNB, the s-gNB should use the Next Hop parameter (NH) or the current K_{gNB} to derive the new session key K^*_{gNB}, which will be used between the t-gNB and the vehicle. The Next-hop Chaining Counter (NCC) is the NH chaining counter, which starts from zero and increases one at a time. Upon receiving the path shift request, the AMF should increase the NCC value by one and calculate a new NH.

B. Certificateless Public Key Cryptography (CL-PKC)

The certificateless public key cryptography (CL-PKC) [28], first introduced by Al-Riyami and Paterson, is an extension of the identity-based public key cryptography (ID-PKC) proposed by Shamir in 1984. [29] In ID-PKC, the public key of each user is easily computable from a string corresponding to this user's identity, (such as a telephone number), and therefore there is no need to use the certificate to prove the identity of the public key. However, the ID-PKC has an inherent key escrow problem, i.e. the Key Generation Center (KGC) knows users' private keys. The key escrow refers to the situation where an encrypted copy of each decryption key is provided to the authorities or to some trusted intermediary. And the private key of the user is completely determined by the server. [30] However, a malicious KGC can frame an innocent user by forging the user's signature [31]. The key escrow freeness (KEF) requires that vehicles' secret keys are determined by themselves instead of the server or the KGC. [32] Therefore, CL-PKC was introduced to mitigate the shortcomings. In CL-PKC, the core network generates the partial private key for a user according to its identity. And the user chooses a random value together with the partial private key to generate its full private key. Compared to certification and ID-PKC, CL-PKC scheme does not require the use of certificates, thus, avoiding the problem of key escrow. A CL-PKE scheme is specified by seven algorithms: **Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Encrypt**, and **Decrypt**. More details can be found at [28].

C. Certificateless Aggregate Signature (CL-AS)

The concept of aggregate signature was first introduced by Boneh et al. [33] The aggregate signatures are digital signatures that combine n signatures from n users into a single short signature. The aggregate signature can convince a verifier that the n users indeed signed the n corresponding messages, which reduced the computational and communication overhead. This paper adopts the CL-AS scheme proposed in [34]. A CL-AS scheme usually consists of the following algorithms:

Setup: AMF accepts a security parameter to generate a master-key and a list of system parameters *params*.

Partial-Private-Key-Extract: AMF accepts a vehicle's identity ID_i, a parameter list *params* and a master-key to produce the vehicle's partial private key D_i.

UserKeyGen: Vehicle uses its identity ID_i and a random $x_i \in Z_q^*$ as input, and outputs the user's secret key x_i and public key P_i.

Sign: Each vehicle uses parameter list *params*, some state information Δ, a message $M_i \in \mathbf{M}$ ($\mathbf{M}$ is the message space), its identity ID_i, its public key P_i, and its signing key (x_i, D_i) to output its signature σ_i.

Aggregate: The aggregate signature generator, which is the first vehicle that enters the new coverage area, uses a state information Δ, an aggregating set $\boldsymbol{U}$ of n users, the identity ID_i of each user U_i, the corresponding public key P_i of U_i, and the signature of U_i to output an aggregate signature σ.

Aggregate Verify: The aggregate signature verifier, which is the t-gNB, use Δ, an aggregating set $\boldsymbol{U}$ of n users, the identity ID_i and the corresponding public key P_i of U_i, an aggregate signature σ on messages $M_1, ..., M_n$ as inputs. It outputs true if the aggregate signature is valid, or false $\perp$ otherwise.

IV. System Model

This section introduces the system model of the 5G-V2X architecture and the corresponding attack model.

A. System Model

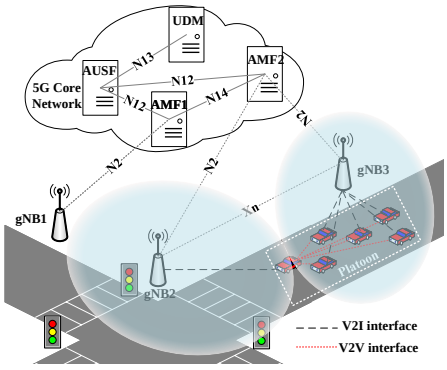

Fig. 1. System Model of 5G-V2X Network

As shown in Figure 1, in the 5G radio access network (RAN), each vehicle connects to the network over the wireless channel through gNBs. And gNBs connect to the 5G core network (CN) through the wire channel. We refer to the

communication interface between vehicles and 5G infrastructure as the vehicle-to-infrastructure (V2I) interface. And we refer to the communication interface between vehicles as the vehicle-to-vehicle (V2V) interface, which does not rely on 5G infrastructure. The system architecture of the 5G core network includes several types of functions such as AMF, Authentication Server Function (AUSF), and Unified Data Management (UDM). During handover, the AMF maintains authentication and key management with the vehicle and interacts with the AUSF. AUSF acts like an authentication server. UDM stores and generates sensitive information.

During a handover process, a vehicle may hand over within an AMF, or to a different AMF depending on the t-gNB. The handover using Xn interface between gNBs within an AMF is called Xn-based intra-AMF handover. The handover using N2 interface within the same AMF is called N2-based intra-AMF handover. The handover between different AMFs is called N2-based inter-AMF handover. The handover involves three entities, namely, the vehicle, gNB, and AMF [35].

B. Attack Model

The network attack model under the study is the Dolev-Yao model, which is commonly used to present security vulnerabilities in various wireless networks. By the Dolev-Yao intruder model, the intruder could overhear, intercept, analyze, or manipulate messages on the wireless channel, and is only limited by the constraints of the cryptographic methods used. [36] Therefore, a malicious attacker may obtain and falsify the messages sent between vehicles and gNBs, or inside the vehicle platoon. Also, by the specification [37], the N2 interface is required to implement IPsec and IKEv2 certificates-based authentication measures, which can provide integrity, confidentiality and replay attack protection. Therefore, it is assumed that the connections between the 5G core network and gNBs are secure. And it is assumed that the connections between vehicles and gNBs are not secure. Because gNBs are usually far from the core network and have limited protection measures. Also, it is assumed that all network functions in the 5G core network are trusted as they are placed in a secure location such as the hardware security module. Connections between network functions are also trusted as they have end-to-end protection which can provide integrity and confidentiality. And entities in the radio access network including the vehicle and the gNBs are not trusted [38].

V. The Proposed Scheme

In this section, the proposed EGHA is introduced in detail. We propose solutions for all handover scenarios, i.e. intra-AMF handover (Xn-based and N2-based) and inter-AMF handover.

A. Motivation

From the literature survey, it is shown that now there are very few researchers focusing on vehicle platoon handover authentication based on 5G. And all the above-mentioned protocols have weaknesses in terms of security, efficiency, or privacy. According to the papers, there are two major solutions. The first group-based solution where the protocols aggregate all vehicles' information in the group to authenticate vehicles is vulnerable to DoS attacks. It will also introduce high overheads on the leader's side. The second solution where the protocols transfer the security context of the group may cause key leakage problems. Also, the handover authentication scheme specified by the 3GPP standard TS 33.501 R16 has various shortcomings. It does not take platoon handover into consideration, and there are vulnerabilities in terms of failed KFS, lack of mutual authentication, high signaling overhead, etc. Based on the gap between the existing solutions and the security demands of the platoon handover authentications in 5G wireless networks, we have the research initiatives to design a solution for the platoon handover authentications to mitigate the above-mentioned shortcomings. Our protocol integrates the advantages of the two solutions discussed above while proposing ways to mitigate their respective shortcomings. The protocol aims to achieve various security attributes including privacy-preserving, mutual authentication, perfect KFS, and resistance to a variety of malicious attacks with low overhead.

TABLE II
Notations and Definition of the Proposed Protocol

Notation	Definition
K_{AMF}	Access key at AMF/vehicle
MAC	Message authentication code
H	Hash function
t	Timestamp
K_{gNB}	The session key of vehicle/gNB
GID	Group identity
TID	Temporary identity of vehicles
G_1/G_2	Cyclic additive/multiplicative group
P, q	generator of the group/prime order of group
$\{x\}_K$	Encrypted x with symmetric key K
SC	Security Context

The notations of the EGHA with their definitions are listed in Table II. The proposed EGHA consists of four phases: i) initial authentication, ii) group handover preparation, iii) first vehicle authentication and iv) group handover authentication phase. The first phase enables initial access mutual authentication for the vehicles with the network. The second phase happens before a handover happens. The third phase starts when the first vehicle enters the communication area of the t-gNB. And the last phase happens when the subsequent vehicles enter the communication area of the t-gNB.

B. Initial Authentication

In this phase, all vehicles, the AUSF, and the ARPF will execute the 5G authentication and key agreement protocol (5G-AKA) specified by the 3GPP standard TS 33.501 R16. After initial authentication, the gNBs and AMFs shall monitor the trace of each individual vehicle to determine if some of them could form a group. The judging criteria of forming a group can be found in [39]. In the rest of the paper, it is assumed that a group has been formed.

In the paper we have adopted the certificateless aggregate signature solution in [34]. After a platoon is established and each vehicle has passed initial authentication, the AMF chooses a cyclic additive group G_1 generated by P with order q and a cyclic multiplicative group G_2 to form a bilinear map $e : G_1 \times G_1 \rightarrow G_2$. The master key is set by a random $\lambda \in Z_q^*$. The AMF sets hash functions $H_1 \sim H_4 : \{0,1\}^* \rightarrow G_1, H_5 : \{0,1\}^* \rightarrow Z_q^*$, and generates the partial private key $\left(D_{i,0}, D_{i,1}\right) = (\lambda Q_{i,0}, \lambda Q_{i,1})$ for each vehicle in the platoon, where $Q_{i,0} = H_1\left(SUCI_i, 0\right), Q_{i,1} = H_1(SUCI_i, 1)$, and $SUCI_i$ is the SUbscription Concealed Identifier of each vehicle. Then the AMF shall publish the system parameter list $params = (G_1, G_2, e, P, P_T, H_1 \sim H_5)$ to the group and transmit the partial private key to the corresponding vehicles through secure channels, where $P_T = \lambda P$. After receiving the partial private key, the vehicle selects a nonce $x_i \in Z_q^*$ as its secret key. And it uses its secret key to generate its public key $P_i = x_i P$. The AMF also generates $(D_{gNB,0}, D_{gNB,1})$ for gNBs, using ID_{gNB} to substitute $SUCI$ in $Q_{gNB,0}, Q_{gNB,1}$, and gNBs also generate their own private keys x_{gNB} and public keys P_{gNB} following the same procedure. ID_{gNB} is the unique identity for every gNBs allocated by the AMF. Also, after the initial authentication, the SEAF shall provide the K_{AMF} to the AMF. K_{gNB} and NH will be derived by vehicles and AMF from K_{AMF}. NH will be the intermediate key used to derive K_{gNB}. K_{gNB} will be used as the session key between the vehicle and the gNB.

C. Handover Preparation

This phase happens before the next group handover, assuming the platoon has started to work in the cell. The details of this phase are shown in Figure 2. The operational details are described below:

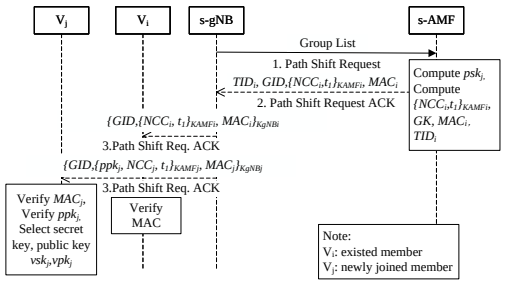

Fig. 2. Handover preparation

Step 1. s-gNB→ s-AMF: Path Shift Request (Group List)
After the previous handover, s-gNB sends all group member's temporary identities *TIDs* to s-AMF in the path shift request message.

Step 2. s-AMF→ s-gNB: Path Shift Request ACK $(TID_i, GID, \{NCC_i, t_1\}_{K_{AMF_i}}, MAC_i)$
AMF shall send an acknowledgment to the s-gNB, which includes all vehicles' temporary identities $TID_i = H(SUCI_i||NH_i||K_{AMF_i})$, group identity $GID = H(\sum_{i=1}^{n} H(TID_i))$, message authentication code $MAC_i = H(GID||NCC_i||t_1||K_{AMF_i})$, encrypted timestamp, and encrypted NCC.

Step 3. s-gNB→ Vehicle: Path Shift Request ACK $(GID, \{NCC_i, t_1\}_{K_{AMF_i}}, MAC_i)$
The s-gNB sends GID,$\{NCC_i, t_1\}_{K_{AMF_i}}, MAC_i$ to the vehicle in the platoon. The vehicle should verify the validity of NCC, timestamp and GID by determining if $MAC_i = H\left(GID||NCC_i||t_1||K_{AMF_i}\right)$. For the newly joined vehicle V_j, the AMF shall compute its partial private key $(D_{j,0}, D_{j,1})$ using the same procedures in *Initial Authentication* and send $\{GID, \left\{(D_{j,0}, D_{j,1}), NCC_j, t_1\right\}_{K_{AMF_j}}, MAC_j = H(GID||NCC_j||t_1||K_{AMF_j})\}$ to V_j. Then, V_j shall verify the MAC value and set its secret key x_j and public key P_j using the same procedures in *Initial Authentication*.

D. First Vehicle Authentication

This phase happens when the first vehicle V_1 enters the t-gNB coverage area. The details of this phase are shown in Figure 3.

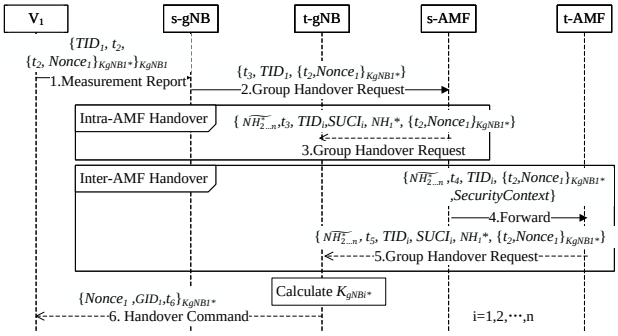

Fig. 3. First Vehicle Authentication

Step 1. Vehicle 1→s-gNB: Measurement Report $(\{TID_1, t_2, \{t_2, Nonce_1\}_{KgNB1*}\}_{KgNB1})$
When the first vehicle in the platoon enters the coverage of t-gNB, it shall send its temporary identity TID_1, a timestamp t_2, and encrypted timestamp and nonce using the new session key with t-gNB K^*_{gNB1} in the measurement report to s-gNB. The vehicle uses $K_{gNB}* = KDF(NH^*||PCI||ARFCN-DL)$ to derive the new session key K^*_{gNB1}, where KDF is the key derivation function specified by 3GPP, ARFCN-DL is the absolute radio frequency channel number-down link of gNB, and PCI is the physical cell identity of gNB. The whole message is encrypted using the session key K_{gNB1} with s-gNB.

Step 2. S-gNB→s-AMF: Group Handover Request $(t_3, TID_1, \{t_2, Nonce_1\}_{KgNB1*})$
After receiving the measurement report from the vehicle, the s-gNB informs s-AMF of the group handover by sending $\{t_3, TID_1, \{t_2, Nonce_1\}_{K_{gNB1*}}\}$. If the handover type of the group is intra-AMF handover, the process jumps to **Step 3**. If the handover type of the group is inter-AMF handover, the process jumps to **Step 4**.

Step 3. s-AMF→t-gNB: Group Handover Request $(\widetilde{NH^*_{2...n}}, t_3, TID_i, SUCI_i, NH^*_1, \{t_2, Nonce_1\}_{K_{gNB1*}})$
After receiving the group handover request message from s-gNB, s-AMF forwards $\widetilde{NH^*_{2...n}}, t_3, TID_i, SUCI_i, NH^*_1, \{t_2, Nonce_1\}_{K_{gNB1*}}$ to t-gNB for group handover authentication, where NH^*_1 is the new next-hop parameter of vehicle 1, $\widetilde{NH^*_i} = H\left(NH^*_i\right) + NH^*_i, t_3$ is the timestamp generated by s-AMF. The purpose of adopting $\widetilde{NH^*}$ is to prevent t-gNB from generating the new session keys with vehicles who do not enter the its coverage. As the vehicle may leave the group suddenly before entering the coverage of t-gNB.

Step 4. s-AMF→t-AMF: Forward Request $(\widetilde{NH^*_{2...n}}, t_4, TID_i, \{t_2, Nonce_1\}_{KgNB1*}, SC)$
When the s-AMF receives the Group Handover Request from the s-gNB, it shall forward $\widetilde{NH^*_i}, t_4, TID_i, \{t_2, Nonce_1\}_{KgNB1*}, SC$ to t-AMF. The security context SC includes the group master key λ, group parameters *params*, session keys between AMF/vehicle, identities, and related keys.

Step 5. t-AMF→t-gNB: Group Handover Request $(\widetilde{NH^*_{2...n}}, t_5, TID_1, SUCI_i, NH^*_1, \{t_2, Nonce_1\}_{K_{gNB1*}})$
After receiving the message from s-AMF, the t-AMF sends a group handover request to t-gNB with vehicle 1's credential to start the handover authentication process for vehicle 1 and other vehicles in the group.

Step 6. t-gNB→Vehicle 1: Handover Command $(\{t_6, GID_1, Nonce_1\}_{K_{gNB1*}})$
After receiving the group's keying material, the t-gNB stores the keying material and starts to process vehicle 1 V_1's authentication request. First, the t-gNB should derive the new session key K^*_{gNB1} by $K_{gNB1*} = KDF(NH^*_1||PCI||ARFCN-DL)$. And it shall use the derived key to decrypt $\{t_2, Nonce_1\}_{KgNB1*}$. If the timestamp is valid, it sends back $\{t_6, GID_1, Nonce_1\}_{KgNB1*}$ to vehicle 1 V_1, where $GID_1 = \sum_{i=2}^{n} H(TID_i)$.

E. Group Handover Authentication

This phase happens after the first vehicle V_1 finishes its handover authentication. It is the AKA process for the rest of the group members. The details are shown in Figure 4. This phase aims to utilize the handover time gap between the first and the subsequent vehicles to pre-establish the mutual authentication between vehicles and the network. The new session keys between subsequent vehicles and t-gNB are not derived until the vehicle actually enters the new coverage.

Step 1. Vehicle 1→Vehicle i: Signature Request $(info_{t_{gNB}}, TID_1, GID_1)$
The first vehicle broadcasts the t-gNB information, such as PCI, ID_{t-gNB}, and t-gNB's public key, through V2V interface. Partial group identity GID_1 is also broadcasted for verification. Each vehicle may verify the authenticity of the first vehicle easily by determining if $H(GID_1 + H(TID_1)) = GID$.

Step 2. Vehicle i→Vehicle 1: Group Signature Respond(Sig_i)

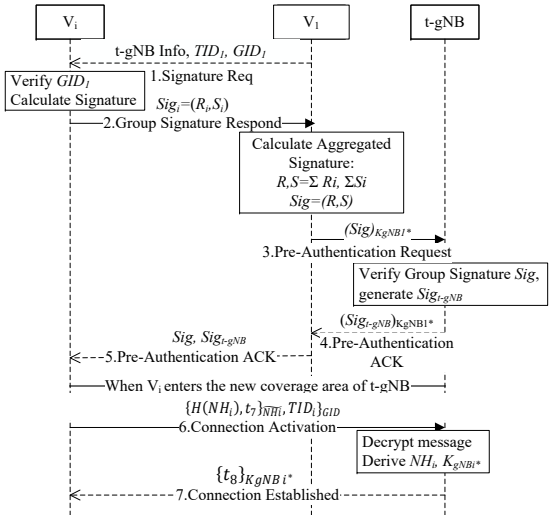

Fig. 4. Group Handover Authentication

When the vehicle receives the signature request, each vehicle shall choose a random value $r_i \in Z^*_q$ and compute $R_i = r_i P$, $h_i = H_5(TID_i||GID_1||SUPI_i||P_i), T = H_2(GID_1), V = H_3(GID_1), W = H_4(GID_1)$. Then, it computes $S_i = D_{i,0} + x_i V + h_i \left(D_{i,1} + x_i W\right) + r_i T$. Finally, each vehicle uses $Sig_i = (R_i, S_i)$ as its signature. Then, the vehicle sends its signature to vehicle 1.

Step 3. Vehicle 1→t-gNB: Pre-authentication Request $(\{Sig\}_{K_{gNB1*}})$
The first vehicle aggregates all signatures by $R = \Sigma^n_{i=2} R_i$, $S = \Sigma^n_{i=2} S_i$. Then, it sends the aggregate signature $Sig = (R, S)$ to the t-gNB.

Step 4. t-gNB→Vehicle 1: Pre-authentication ACK $(\{Sig_{t-gNB}\}_{KgNB1*})$
When the t-gNB receives the group signature Sig_{t-gNB} from vehicle 1, it uses the same procedures in Step. 2 to calculate $T, V, W, h_i, Q_{i,0}, Q_{i,1}$. Then, it verifies the signature by determining if $e(S, P) = e\left(P_T, \Sigma^n_{i=2} Q_{i,0} + \Sigma^n_{i=2} h_i Q_{i,1}\right) e(V, \Sigma^n_{i=2} P_i) \times e\left(W, \Sigma^n_{i=2} h_i P_i\right) e(T, R)$, where e refers to bilinear maps operation. If the equation holds, the t-gNB authenticates all vehicles successfully. Otherwise, the concept of binary search has been adopted to locate the attacker: The t-gNB requests the V_1 to divide the group aggregate signature into 2 aggregate signatures. Each one only contains half of the group members' signatures. Then the t-gNB shall verify the 2 messages to find the invalid one. The t-gNB shall repeat the above process until the attacker is located. Then, t-gNB uses the following steps to calculate its own signature. t-gNB chooses a random $r_{t-gNB} \in Z^*_q$ to compute $R_{t-gNB} = r_{t-gNB} P, h_{t-gNB} = H_5(Sig||GID||ID_{t-gNB}||P_{t-gNB}), T = H_2(GID), V = H_3(GID), W = H_4(GID)$. Then, it computes $S_{t-gNB} = D_{t-gNB,0} + x_{t-gNB} V + h_{t-gNB}\left(D_{t-gNB,1} + x_{t-gNB} W\right) + r_{t-gNB} T$. T-gNB uses $Sig_{t-gNB} = (R_{t-gNB}, S_{t-gNB})$ as its signature.

Then it sends its signature to vehicle 1.

Step 5. Vehicle 1→Vehicle i: Pre-authentication ACK (Sig_{t-gNB}, Sig)
Vehicle 1 broadcasts t-gNB's signature Sig_{t-gNB} and Sig to the platoon. Each vehicle shall use the same procedures in Step.5 with ID_{t-gNB} to compute $R, T, V, W, h_{t-gNB}, Q_{t-gNB,0}, Q_{t-gNB,1}$. Then it verifies the signature by determining if $e(S,P) = e\left(P_T, Q_{t-gNB,0} + h_{t-gNB}Q_{t-gNB,1}\right) e(V, P_{t-gNB}) \times e\left(W, h_{t-gNB}P_{t-gNB}\right) e(T,R)$. If the equation holds, the pre-authentication success.

Step 6. Vehicle i→t-gNB: Connection Activation $(\{\{H(NH_i^*), t_7\}_{\widetilde{NH_{i*}}}, TID_i\}_{GID})$
This step happens when the vehicle enters the coverage area of t-gNB. The vehicle shall send a connection activation message $(\{\{H(NH_i^*), t_7\}_{\widetilde{NH_{i*}}}, TID_i\}_{GID})$ to t-gNB. When the t-gNB receives the message, it should use the GID to decrypt the message and get the TID_i. Then, it finds the encrypted NH value $\widetilde{NH_i^*}$ to decrypt the $\left\{H\left(NH_i^*\right), t_7\right\}_{\widetilde{NH_{i*}}}$. Then, it checks the timestamp to see if the message is fresh. If so, it derives the new NH value to be used with the vehicle by $NH_i^* = H\left(NH_i^*\right) + \widetilde{NH_i^*}$. Then, it derives the session key with the vehicle by $K_{gNBi*} = KDF(NH_i^*||PCI||ARFCN-DL)$. So far, the group handover authentication process has succeeded. Each vehicle and the t-gNB share the session key K_{gNBi*}.

Step 7. t-gNB→Vehicle i: Connection Established $\{t_8\}_{KgNBi*}$
The t-gNB should use the new session key K_{gNBi*} to encrypt the timestamp t_8 and send it to the vehicle. The vehicle should decrypt the timestamp. It accepts the connection if it is fresh.

VI. Security Evaluation

In this section, we evaluate the security functionality of the protocol by Scyther tool. The security analysis of the protocol is also presented.

A. Formal Proof by Scyther Tool

Scyther was first introduced and used by Cremers in [15]. After that, a lot of researchers have used Scyther for security protocols verification. Scyther is an effective formal verification tool for falsification, verification, and detecting potential attacks. It can analyze the security functions following the Dolev-Yao model and the other 9 adversary models. It can analyze the claims declared in Scyther by an unbounded model checking approach and a backward symbolic state search technique. There are many different claims in Scyther, which are synchronization (Nisynch), agreement (Niagree), aliveness (Alive), weak agreement (Weakagree), secrecy, etc. [15]

In the model of the proposed protocol, there are 5 roles, which are s-gNB, t-gNB, Vi , V1, and the AMF. V1 refers to the first vehicle that enters the coverage of t-gNB and Vi refers to all subsequent vehicles. The authentication of the first vehicle V1 and the following vehicles Vi are modeled and verified separately in Figure 5 and Figure 6, respectively. Because in our protocol the first vehicle has a different authentication procedure from the subsequent vehicles. All roles are required to achieve all four claims including Nisynch, Niagree, Alive, Weakagree. Since the initial handover phase has been assumed secure, we only present the formal verification on the group handover authentication in the proposed protocol here.

AMF	Vehicle1auth,A1	Secret theta	Ok	Verified	No attacks.
	Vehicle1auth,A2	Secret NCC	Ok	Verified	No attacks.
	Vehicle1auth,A3	Nisynch	Ok	Verified	No attacks.
	Vehicle1auth,A4	Niagree	Ok	Verified	No attacks.
	Vehicle1auth,A5	Alive	Ok	Verified	No attacks.
	Vehicle1auth,A6	Weakagree	Ok	Verified	No attacks.
V1	Vehicle1auth,U1	Secret Nonce	Ok		No attacks within bounds.
	Vehicle1auth,U2	Nisynch	Ok		No attacks within bounds.
	Vehicle1auth,U3	Niagree	Ok		No attacks within bounds.
	Vehicle1auth,U4	Alive	Ok		No attacks within bounds.
	Vehicle1auth,U5	Weakagree	Ok		No attacks within bounds.
sgNB	Vehicle1auth,S1	Nisynch	Ok	Verified	No attacks.
	Vehicle1auth,S2	Niagree	Ok	Verified	No attacks.
	Vehicle1auth,S3	Alive	Ok	Verified	No attacks.
	Vehicle1auth,S4	Weakagree	Ok	Verified	No attacks.
tgNB	Vehicle1auth,T1	Nisynch	Ok	Verified	No attacks.
	Vehicle1auth,T2	Niagree	Ok	Verified	No attacks.
	Vehicle1auth,T3	Alive	Ok	Verified	No attacks.
	Vehicle1auth,T4	Weakagree	Ok	Verified	No attacks.

Fig. 5. Results of Formal Verification (V_1)

Claim				Status	Comments
vehicleauth	Vi	vehicleauth,i1	Nisynch	Ok	No attacks within bounds.
		vehicleauth,i2	Niagree	Ok	No attacks within bounds.
		vehicleauth,i3	Alive	Ok	No attacks within bounds.
		vehicleauth,i4	Weakagree	Ok	No attacks within bounds.
		vehicleauth,i5	Secret hnhi	Ok	No attacks within bounds.
		vehicleauth,i6	Secret H(NH,Vi,k(AMF,Vi))	Ok	No attacks within bounds.
	tgnb	vehicleauth,T1	Nisynch	Ok	No attacks within bounds.
		vehicleauth,T2	Niagree	Ok	No attacks within bounds.
		vehicleauth,T3	Alive	Ok	No attacks within bounds.
		vehicleauth,T4	Weakagree	Ok	No attacks within bounds.
		vehicleauth,T5	Secret hnhi	Ok	No attacks within bounds.
		vehicleauth,T6	Secret H(NH,Vi,k(AMF,Vi))	Ok	No attacks within bounds.

Fig. 6. Results of Formal Verification (V_i)

The verification results are shown in Figure 5 and Figure 6, from which it is shown that all the four roles can achieve synchronization (Nisynch), agreement (Niagree), aliveness (Alive), and weak agreement (Weakagree). This means mutual authentication is achieved. And false base-station attacks cannot succeed. And all intermediate keys are also confidential. Also vehicles' temporary identities are confidential, which can be seen from claims i6 and T6 in Figure 6. In conclusion, the results of the formal verification have shown that the proposed group handover authentication protocol is secure. We didn't further prove the logic correctness of the scheme due to the length restrictions.

B. Formal Proof by BAN-Logic

Burrows-Abadi-Needham logic (BAN Logic) was first introduced by Burrows et al. [20] It has been used to derive

logic correctness of security protocols formally. BAN-logic provides a logic way to describe the beliefs of trustworthy parties involved in authentication protocols and the evolution of these beliefs. In order to be verified, a protocol first needs to be translated into an idealization version. And assumptions and goals need to be proposed. Then, derivation rules are applied manually to reach the goals. The notations of BAN-logic are listed in Table III.

TABLE III
NOTATIONS OF BAN-LOGIC

Notation	Meaning
$P \mid\equiv X$	P believes the message X
$P \triangleleft X$	P sees the message X
$P \mid\sim X$	P said the message X
$P \Rightarrow X$	P has authority on X
$\#(X)$	X is fresh
$\langle X \rangle_K$	X is combined with a secret K
$\{X\}_K$	X is encrypted under the key K
$P \overset{K}{\leftrightarrow} Q$	K is a secret key shared between P and Q
$P \overset{K}{=\!=} Q$	K is a shared secret between P and Q
$\overset{K}{\rightarrowtail} P$	P has a public key K corresponding to a private key K^{-1}.

The rules of BAN-logic for derivation can be described as follows:

The first rule is Message Meaning Rule (MM). It can be described as $\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$, $\frac{P \mid\equiv P \overset{K}{=\!=} Q,\ P \triangleleft \langle X \rangle_K}{P \mid\equiv Q \mid\sim X}$, and $\frac{P \mid\equiv P \overset{K}{\rightarrowtail} Q, P \triangleleft \{X\}_K^{-1}}{P \mid\equiv Q \mid\sim X}$. The first one is for the shared secret key, and the second one describes the shared secret. The third one means that if P believes that the public key for user Q is K, and P can see the message X signed by the private key of Q is K^{-1}, then P believes the message X is sent by Q.

The second rule is Freshness Rule (FR). It can be described as $\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$.This rule means if one part of the message is fresh, then the entire message is fresh.

The third rule is Nonce Verification Rule (NV). It can be described as $\frac{P \mid\equiv \#(X),\ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$. This rule means if P believes X is fresh and P believes Q sent X, then P believes Q believes X.

The fourth rule is Jurisdiction Rule (JR), which is described as $\frac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$. This rule means if P believes Q has jurisdiction on message X, and P believes Q believes X, then P believes X.

The fifth rule is Composition Rule (CR), which is $\frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X,Y)}$. This rule means if P believes X and P believes Y then P believes (X,Y).

The sixth rule is Decomposition Rule (DR). It can be described as $\frac{P \triangleleft (X,Y)}{P \triangleleft X}$ and $\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \triangleleft X}$. This means if a P sees a message and he knows the key to the message, then he also sees its components.

The last rule is Belief Conjunction Rule (BC). It can be described as $\frac{P \mid\equiv Q \mid\equiv \{X,Y\}}{P \mid\equiv Q \mid\equiv X}$, $\frac{P \mid\equiv \{X,Y\}}{P \mid\equiv X}$ and $\frac{P \mid\equiv Q \mid\sim \{X,Y\}}{P \mid\equiv Q \mid\sim X}$.

1) The Goals of EGHA: The goals of BAN-logic are the key agreement between the vehicle and t-gNB in our scheme. As the first vehicle V_1 and the sebsequent vehicles V_i has different authentication procedure, they have been proved seperately. We refer to all vehicles including V_1 and V_i as V. The goals can be described as follows:

G1-G8 is the session key agreement between the vehicle and t-gNB. A session key K_{gNB*} , which is only known to the vehicle (V) and t-gNB, will be shared by the vehicle and t-gNB if the eight goals are achieved.

(G1) $V_i \mid\equiv V_i \overset{K_{gNBi*}}{\leftrightarrow} t-gNB$

(G2) $t-gNB \mid\equiv t-gNB \overset{K_{gNBi*}}{\leftrightarrow} V_i$

(G3) $t-gNB \mid\equiv V_i \mid\equiv V_i \overset{K_{gNBi*}}{\leftrightarrow} t-gNB$

(G4) $V_i \mid\equiv t-gNB \mid\equiv t-gNB \overset{K_{gNBi*}}{\leftrightarrow} V_i$

(G5) $V_1 \mid\equiv V_1 \overset{K_{gNB1*}}{\leftrightarrow} t-gNB$

(G6) $t-gNB \mid\equiv t-gNB \overset{K_{gNB1*}}{\leftrightarrow} V_1$

(G7) $t-gNB \mid\equiv V_1 \mid\equiv V_1 \overset{K_{gNB1*}}{\leftrightarrow} t-gNB$

(G8) $V_1 \mid\equiv t-gNB \mid\equiv t-gNB \overset{K_{gNB1*}}{\leftrightarrow} V_1$

2) The Assumptions of EGHA: To analyze the protocol, initial assumptions are described as follows: As K_{AMF} has been established since the initial authentication, therefore:

(A1) $V \mid\equiv V \overset{K_{AMF}}{\leftrightarrow} AMF$

As NCC is encrypted with K_{AMF} and can be verified with MAC, therefore:

(A2) $V \mid\equiv AMF \Rightarrow NCC$

As NH is generated by AMF and sent to t-gNB, and NH will be used to derive K_{gNB*}, therefore:

(A3) $t-gNB \mid\equiv AMF \Rightarrow K_{gNB*}$

As the t-gNB shares the group ID *GID* with all vehicles in the group, therefore:

(A4) $t-gNB \mid\equiv t-gNB \overset{GID}{\leftrightarrow} V$

As the t-gNB and the AMF communicates through the secure channel, therefore:

(A5) $t-gNB \mid\equiv t-gNB \overset{K_{\{AMF,t-gNB\}}}{\leftrightarrow} AMF$

3) Security Result: To idealize the protocol, we describe the messages in the proposed protocol as follows:

Message 1: The s-AMF sends $\{TID_i, GID, \{NCC_i, t_1\}_{K_{AMF_i}}, MAC_i\}$ to s-gNB:

(M1) $s-gNB \triangleleft \{TID_i, GID, \{NCC_i, t_1\}_{K_{AMF_i}}, MAC_i\}$

Message 2: The s-gNB sends $\{GID, \{NCC_i, t_1\}_{K_{AMF_i}}, MAC_i\}$ to the vehicle:

(M2)$V \triangleleft \{GID, \{NCC_i, t_1\}_{K_{AMF_i}}, MAC_i\}$

For the newly joined vehicle V_j as stated in Figure 2, as the only difference between the messages that s-AMF sends to V_i and V_j is the partial private key ppk_j, which has no role in derivation process. These two messages are treated as one message as M2.

Message 3: The first vehicle V_1 sends $\{TID_1, t_2, \{t_2, Nonce_1\}_{KgNB1*}\}_{KgNB1}$ to s-gNB:

(M3)$s-gNB \triangleleft \{TID_1, t_2, \{t_2, Nonce_1\}_{KgNB1*}\}_{KgNB1}$

Message 4: The s-gNB sends $\{t_3, TID_1,\ \{t_2, Nonce_1\}_{KgNB1*}\}$ to s-AMF:

(M4)$s-AMF \triangleleft \{t_3, TID_1, \{t_2, Nonce_1\}_{KgNB1*}\}$

Message 5: The s-AMF sends $\{\widehat{NH^*_{2...n}}, t_3, TID_i, SUCI_i, NH^*_1, \{t_2, Nonce_1\}_{K_{gNB1*}}\}$ to t-gNB through the secure channel:

(M5)$t-gNB \triangleleft \{\widehat{NH^*_{2...n}}, t_3, TID_i, SUCI_i, NH^*_1,$
$\{t_2, Nonce_1, K_{gNB*}\}_{K_{gNB1*}}\}_{K(AMF,t-gNB)}$

Message 6: The s-AMF sends $\{\widehat{NH^*_{2...n}}, t_4, TID_i, \{t_2, Nonce_1\}_{K_{gNB1*}}, SC\}$ to t-AMF through the secure channel:

(M6)$t-AMF \lhd \{\widetilde{NH^*_{2...n}}, t_4, TID_i, \{t_2, Nonce_1\}_{K_{gNB1*}}, SC\}_{K(s-AMF,t-AMF)}$

Message 7: The t-AMF sends $\{\widetilde{NH^*_{2...n}}, t_5, TID_i, SUCI_i, NH^*_1, \{t_2, Nonce_1\}_{K_{gNB1*}}\}$ to t-gNB through the secure channel:

(M7)$t-gNB \lhd \{\widetilde{NH^*_{2...n}}, t_5, TID_i, SUCI_i, NH^*_1, \{t_2, Nonce_1, K_{gNB1*}\}_{K_{gNB1*}}\}_{K(AMF,t-gNB)}$

Message 8: The t-gNB sends $\{Nonce_1, GID_1, t_6,\}_{K_{gNB1*}}$ to the first vehicle V_1:

(M8) $V_1 \lhd \{Nonce_1, GID_1, t_6, K_{gNB1*}\}_{K_{gNB1*}}$

Message 9: The first vehicle V_1 sends $\{TID_1, GID_1, info_{t_{gNB}}\}$ to the other vehicle V_i:

(M9) $V_i \lhd \{TID_1, GID_1, info_{t_{gNB}}\}$

Message 10: V_i sends $\{Sig_i\}$ to the first vehicle V_1:

(M10) $V_1 \lhd \{TID_i, GID_1\}_{sk_{V_i}}$

Where sk_{V_i} is the private (signing) key of vehicle i, as the signature can be formulated as the message encrypted by the private key.

Message 11: The first vehicle V_1 sends all vehicle's aggregated signature $\{\{Sig\}_{K_{gNB1*}}\}$ to the t-gNB:

(M11) $t-gNB \lhd \{\sum_i \{TID_i, GID_1\}_{sk_{V_i}}\}_{K_{gNB1*}}$

Message 12: The t-gNB sends $\{Sig_{t-gNB}\}_{KgNB1*}$ to the first vehicle V_1:

(M12) $V_1 \lhd \{\{Sig, ID_{t-gNB}, GID\}_{sk_{gNB}}\}_{KgNB1*}$

Message 13: The first vehicle V_1 sends $\{Sig, Sig_{t-gNB}\}$ to V_i:

(M13) $V_i \lhd \{TID_i, GID_1\}_{sk_{V_i}}, \{Sig, ID_{t-gNB}, GID\}_{sk_{gNB}}$

Message 14: V_i sends $\{\{H(NH^*_i), t_7\}_{\widetilde{NH_{i*}}}, TID_i\}_{GID}$ to the t-gNB:

(M14) $t-gNB \lhd \{\{H(NH^*_i), t_7\}_{\widetilde{NH_{i*}}}, TID_i\}_{GID}$

Message 15: $t-gNB$ sends $\{t_8\}_{KgNBi*}$ to the vehicle:

(M15) $V_i \lhd \{t_8, K_{gNBi*}\}_{KgNBi*}$

We refer to all vehicles including V_1 and V_i as V. Using the rules, assumptions and messages described above, the detailed proof is given below:

According to M2 and rule DR, the vehicle sees $\{NCC, t_1\}_{K_{AMF}}$

$$V \lhd \{NCC, t_1\}_{K_{AMF}} \tag{1}$$

If the timestamp t_1 is verified to be fresh, according to rule FR, then the vehicle believes the other component in the same message (NCC) is also up to date:

$$V \mid\equiv \#NCC \tag{2}$$

Since NCC is used to derive K_{gNB*} for the vehicle, the freshness of NCC guarantees the freshness of K_{gNB*}:

$$V \mid\equiv \#K_{gNB*} \tag{3}$$

This means the vehicle believes K_{gNB*} is fresh. According to M5 (M7 for inter-AMF handover), A5, and rule DR, we have

$$t-gNB \lhd \{NH^*, t\} \tag{4}$$

Similarly, according to (4), rule FR, if the timestamp t is verified to be fresh, then the other component (NH^*) in the same message is also believed fresh:

$$t-gNB \mid\equiv \#NH^* \tag{5}$$

Since NH is used to derive K_{gNB*} for t-gNB, the freshness of NH guarantees the freshness of K_{gNB*}:

$$t-gNB \mid\equiv \#K_{gNB*} \tag{6}$$

This means t-gNB believes K_{gNB*} is fresh. According to M2, A1 and rule MM, we have

$$V \mid\equiv AMF \mid\sim \{NCC, t_1\} \tag{7}$$

According to (2) and rule FR, because a part of the message is believed fresh, the vehicle believes the whole message is fresh:

$$V \mid\equiv \#\{NCC, t_1\} \tag{8}$$

According to (7), (8) and rule NV, the vehicle believes AMF believes $\{NCC, t_1\}$:

$$V \mid\equiv AMF \mid\equiv \{NCC, t_1\} \tag{9}$$

According to (9) and rule BC, the vehicle believes AMF believes NCC:

$$V \mid\equiv AMF \mid\equiv NCC \tag{10}$$

According to (10), A2 and rule JR, consider the vehicle use NCC to derive K_{gNB*}, we have:

$$V \mid\equiv K_{gNB*} \tag{11}$$

which is $V \mid\equiv V \overset{K_{gNB*}}{\leftrightarrow} t-gNB$ (G1 and G5)

According to M5 (M7 for inter-AMF handover), A5, rule MM, and rule BC:

$$t-gNB \mid\equiv AMF \mid\sim NH^* \tag{12}$$

Since NH^* is used to derive K_{gNB*}, we have:

$$t-gNB \mid\equiv AMF \mid\sim K_{gNB*} \tag{13}$$

According to (6), (13) and rule NV, we can derive that:

$$t-gNB \mid\equiv AMF \mid\equiv K_{gNB*} \tag{14}$$

According to A3 and rule JR, we can derive that:

$$t-gNB \mid\equiv K_{gNB*} \tag{15}$$

which is (G2 and G6) $t-gNB \mid\equiv t-gNB \overset{K_{gNB*}}{\leftrightarrow} V$

According to (15), consider that $\widetilde{NH*}$ is used to derive K_{gNB*}, we have:

$$t-gNB \mid\equiv t-gNB \overset{\widetilde{NH*}}{\leftrightarrow} V \tag{16}$$

According to M14, rule DR, and A4, we have:

$$t-gNB \lhd \{H(NH^*_i), t_7\}_{\widetilde{NH_{i*}}} \tag{17}$$

According to (17), (16), and rule MM, we have:

$$t - gNB \mid\equiv V_i \mid\sim \{H(NH_i^*)\} \tag{18}$$

According to (18), (6) and rule NV, consider that $H(NH_i^*)$ is used to derive K_{gNBi*}, we can prove the goal G3:

$$t - gNB \mid\equiv V_i \mid\equiv V_i \overset{K_{gNBi*}}{\leftrightarrow} t - gNB \ (G3) \tag{19}$$

According to M15, (11) and rule MM, the vehicle believes t-gNB said K_{gNBi*}:

$$V_i \mid\equiv t - gNB \mid\sim K_{gNBi*} \tag{20}$$

According to (20), (3) and rule NV, the vehicle believes t-gNB believes K_{gNBi*}:

$$V_i \mid\equiv t - gNB \mid\equiv K_{gNBi*} \tag{21}$$

which is (G4) $V_i \mid\equiv t - gNB \mid\equiv t - gNB \overset{K_{gNBi*}}{\leftrightarrow} V_i$

According to A5, M7 and rule DR, we have:

$$t - gNB \lhd \{t_2, Nonce_1, K_{gNB1*}\}_{K_{gNB1*}} \tag{22}$$

According to (22), rule MM, rule BC, and (15), we have:

$$t - gNB \mid\equiv V_1 \mid\sim K_{gNB1*} \tag{23}$$

According to (23), (6), and rule NV, we can prove the goal G7:

$$t - gNB \mid\equiv V_1 \mid\equiv V_1 \overset{K_{gNB1*}}{\leftrightarrow} t - gNB \ (G7) \tag{24}$$

According to M8, (11), rule BC and rule MM, the first vehicle believes t-gNB said K_{gNB1*}:

$$V_1 \mid\equiv t - gNB \mid\sim K_{gNB1*} \tag{25}$$

According to (25), (3) and rule NV, the vehicle believes t-gNB believes K_{gNB1*}:

$$V_1 \mid\equiv t - gNB \mid\equiv K_{gNB1*} \tag{26}$$

which is (G8) $V_1 \mid\equiv t - gNB \mid\equiv t - gNB \overset{K_{gNB1*}}{\leftrightarrow} V_1$

In summary, all security goals are achieved. This means the assurance of key agreement and mutual authentication are achieved. The vehicle and gNB are able to establish a secure session key and use it to encrypt messages between them.

C. Security Analysis

In this section, the security properties of our proposed protocol are discussed and analyzed.

Privacy Protection (Anonymity and Unlinkability): The privacy of vehicles is under protection by our proposal. The temporary identity instead of the real identity of a vehicle (*TID*) is transmitted through the wireless channel. As the real identity is only revealed to legal base stations and core networks. Thus, anonymity is met. Also, as this temporary identity is changed after every handover, it is hard for an adversary to determine if two *TIDs* belong to the same vehicle. Thus, the attacker cannot link the moving pattern with the vehicle, which preserves the unlinkability.

Ability against DoS Attacks: By the original 5G protocol specified by 3GPP, an attacker may impersonate a legal gNB and send lots of fake NCC values to the vehicle to sabotage the key derivation process. By the EGHA protocol, a MAC value is added to ensure the NCC's integrity. Also, by the protocols using the aggregate MAC or signature, an attacker may send false information to sabotage the verification of the group. In our paper, we have proposed a universal method for such aggregate-based solutions to quickly locate the false MAC or signature with reduced time complexity.

Ability against False Base-station Attacks: By the EGHA protocol, the vehicle and the t-gNB establish mutual authentication through certificateless signature, which can ensure the vehicle is connecting to the legal gNB. Also, only legal gNBs can receive the encrypted NH values through the secure channel with the AMF. Without the valid session key, the false gNB cannot establish communication with the vehicle. Therefore, false base-station attacks can be prevented.

Ability against Key Leakage All keys in the EGHA are able to resist key leakage. To prevent t-gNB from knowing the session keys of vehicles who have not entered the coverage of t-gNB, we use a xor operation to encrypt NH values by $\widetilde{NH_i^*} = H\left(NH_i^*\right) + NH_i^*$. The t-gNB can only derive the correct NH after it receives $\widetilde{NH_i}*$ through the secure channel with AMF and $H\left(NH_i^*\right)$ from the vehicle V_i. Therefore, the key leakage can be prevented.

Traceability For malicious vehicle tracing, with vehicle communications being anonymous and unlinkable, only the 5G core network can retrieve a vehicle's real ID using temporary ID *TID* when the message is in dispute. As each message has sender's temporary ID *TID* included, each message from the vehicle is always traceable by the 5G core network.

VII. Performance Evaluation

In this section, the performance of the proposed protocol has been evaluated with the comparison of the performance of some other protocols. Our proposed EGHA is compared with the 5G standard specified by 3GPP TS 33.501 R16 [37], the protocols in [9], and [1]. They are indicated as 5G, PHA, and NAPV. In the simulation, it is assumed that all symmetric encryption keys are 256 bits, MAC is 160 bits, *NH, H(NH), hash, nonce, TID, GID, ID, SUPI, 5G-GUTI, PW*, r'_{Vi}, PCI, and *ARFCN-DL* are 128 bits, the timestamp is 32 bits, and the sizes of the elements in the group G_1, G are 1024 bits, 320 bits, respectively. [40]

A. Signaling Cost

We evaluate the possibility of causing network congestion by evaluating the signaling cost, which has been calculated in terms of the number of signaling messages for n vehicles between vehicles and the network. The messages among vehicles inside the vehicle platoon are not included in the calculation. The results of the signaling overheads have been shown in Table IV.

From Table IV, it can be seen that our protocol has a significantly lower signaling overhead than the 5G standard specified by 3GPP R16, and it has a similar performance with

TABLE IV
SIGNALLING OVERHEAD FOR N VEHICLES

Scheme	Xn-based Handover	N2-based Intra-AMF Handover	Inter-AMF Handover
5G	5n	7n	8n
PHA	3	3	9
NAPV	2n+2	2n+2	2n+2
EGHA	2n+4	2n+4	2n+5

the NAPV. It can also be seen that our EGHA has a higher overhead than that of PHA, which has a constant overhead. However, the PHA has other security and delay problems as discussed in this paper.

B. Communication Cost

In this subsection, we evaluate the communication cost of our protocol and other compared protocol for n vehicles. The communication cost consists of transmission delay and propagation delay. For the transmission delay, according to the 3GPP specification TS 22.261 [41], the experienced data rate of the downlink of general wide-area scenario in the urban area is 50 Mbps and 25 Mbps for uplink data rate. We assume the data rate between gNBs is 50Mbps. And we ignore the transmission delay inside the core network. As for the propagation delay, the wave propagation speed is approximately equal to $3\times10^8\ m/s$ in wireless communication. It is assumed that the radius of a cell is 200 meters, and the signal sent by a vehicle will travel 200 meters at the speed of $3\times10^8\ m/s$ to arrive at a gNB. We ignore the propagation delay inside the core network. The theoretical communication cost is compared in Table V, where T_t, T_p, T_{total} represent the transmission delay, propagation delay, and total communication time, respectively. We use inside to refer to communications between gNBs. The simulation parameter lengths are introduced at the beginning of this section. And the communication overhead that appears in the handover preparation phase is not counted as it happens before the handover.

TABLE V
COMMUNICATION OVERHEAD FOR N VEHICLES

Scheme	Link	Message Size (bits)	$T_t(\mu s)$	$T_p(\mu s)$	Complexity
5G	Up	128n	5.12n	0.67n	$O(n)$
	Down	128n	2.56n	0.67n	
	Inside	640n	12.8n	1.34n	
PHA	Up	416n+192	16.64n+7.68	0.67	
	Down	160	3.2	0.67	
	Inside	384n+128	7.68n+2.56	0.67	
NAPV	Up	416n	16.64n	0.67n	$O(n^2)$
	Down	128n(n+1)	2.56n(n+1)	0.67n	
EGHA	Up	288n+2080	11.52n+83.2	0.67(n+1)	$O(n)$
	Down	355n+2304	7.1n+46.08	0.67(n+1)	

From Table V, it can be seen that our protocol has the advantage when the number of vehicles in the platoon is large. By simply solving the equations of the total time in Table V, it can be seen that our protocol outperforms the NAPV in terms of communication cost when n is larger than 7, and it outperforms PHA and 5G when n is larger than 26 and 40, respectively.

C. Computational Cost

For the computational overhead, we follow the evaluation work in [22], where C/C++ OPENSSL library has been used on an Intel(R) Core(TM) m3-6Y30 with a CPU 0.9 GHz processor as an on-board unit of a vehicle and an Intel(R) Core(TM) i7-7500U with a CPU 2.70 GHz as a gNB. According to the cryptography operations in [22], the point multiplication operation T_{PM} for a vehicle and a gNB are 960μs, 500μs respectively. The symmetric encryption/decryption operation T_A for a vehicle and a gNB are 2.26μs, 1.05μs respectively. And the hash operation T_H for a vehicle and a gNB are 2.38μs, 1.21μs respectively. The XOR, multiplication, and arithmetic operations have been ignored. The results are shown in Table VI. T_V, T_{gNB} represent the computational time for a vehicle and a gNB, respectively. Only operations during handover authentication are counted for all compared schemes. For our scheme, calculations happened in initial authentication, handover preparation, and step 1-5 in group handover authentication have been excluded from calculation. The reason for excluding these steps is that they can be optimized to happen outside the handover authentication to lower the latency.

TABLE VI
COMPUTATIONAL OVERHEAD FOR N VEHICLES (DURING HANDOVER)

Scheme	T_V	T_{gNB}
5G	$4T_H n$	$2T_H n$
PHA	$2n(T_{pm}+T_H)$	$2n(T_{pm}+T_H)$
NAPV	$2nT_A+nT_H$	$2nT_A+nT_H$
EGHA	$2nT_H+(2n+1)T_A$	$2nT_H+(2n+1)T_A$

Also, Figure 7 shows the handover authentication time cost (i.e. communication cost and computational cost) of n vehicles in the platoon. It is shown that PHA has the highest time cost, as it has 2 point multiplication operations during authentication. It is also shown that our proposed EGHA has better performance than NAPV and PHA when there are more than 7 vehicles in the platoon. And our EGHA has a similar performance with the 5G standard specified by 3GPP. However, the 5G standard specified by 3GPP has security problems which are prone to attacks, and it has high signaling overheads in all types of handover scenarios.

Then, the robustness of the protocols is evaluated. Unknown attacks have been introduced to each of the systems. When facing unknown attacks, an authentication process could be forced to stop and restart. It is assumed that at each step of the authentication, the probability of an unknown attack appearing is even. The average time for a successful handover is calculated by the following formula:

$$T=\frac{T_{success}+T_{failed}}{N_{success}}=\frac{\Sigma_{i=1}^{n}\frac{1}{n}\times t_{fail}\times p+t_{success}\times(1-p)}{1-p}$$

Where T, $T_{success}$, T_{failed} are the average time for a successful handover authentication, the total time for successful handover authentications, and the total time for failed handover authentications, respectively; $N_{success}$ is the number of

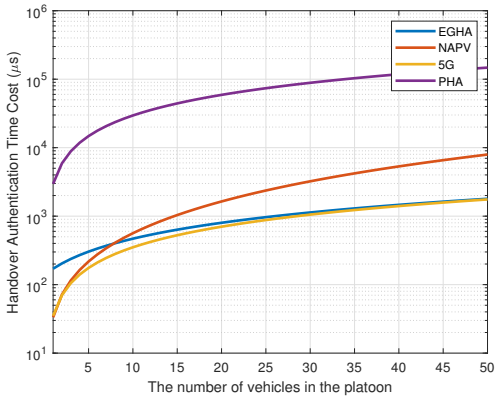

Fig. 7. The Comparison of the Authentication Time Cost

successful handover authentications; p is the percentage of unknown attacks; n is the number of steps in the protocol; t_{fail} represents the amount of time of a failed handover authentication before the attack happens; And $t_{success}$ represents the amount of time of a successful handover authentication before the attack happens.

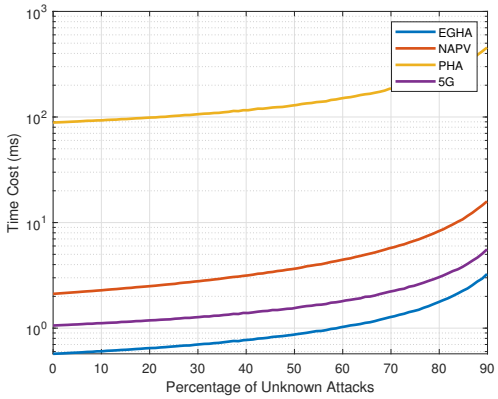

Fig. 8. The Comparison of the Time Cost for 30 Vehicles

The relationship between the time cost and the percentage of unknown attacks is simulated with the results shown in Figure 8. The number of vehicles in the group is set to 30 in the simulation. It is suggested that when the platoon has 30 vehicles, our protocol has the strongest robustness in terms of time cost in the group handover authentication.

D. Discussion

In this subsection, we present a comparison on performance and security between our EGHA and other related protocols in Table VII. We have compared our protocol with [37], [9], and [1], indicated as 5G, PHA, NAPV, respectively. We choose the re-authentication protocol in NAPV to compare with other protocols. It is shown that our EGHA has better performance in security and efficiency. By utilizing the time slot induced by the gap between first and second vehicles entering the new coverage area, it incurs less computational and communication overheads than other protocols. At the same time, our EGHA can provide major security properties including mutual authentication, KFS/KBS, and resistance to some of the protocol attacks.

TABLE VII
SECURITY ANALYSIS AND NETWORK OVERHEADS OF PROTOCOLS

	EGHA	**5G**	**PHA**	**NAPV**
Mutual Authentication	Y	N	Y	N
Follow 3GPP standard	Y	Y	Y	N
Key Agreement	Y	Y	Y	Y
KFS/KBS	Y	N	N	Y
Privacy Protection	Y	N	N	N
Resistance from DoS attack	Y	N	N	Y
Signaling Cost	L	H	L	L
Communication Cost	L	L	L	H
Computational Cost	L	L	H	L

Abbreviations: Y: Yes, N: No, H: High, M: Medium, L: Low

VIII. CONCLUSION

In this paper, we have proposed an authentication protocol for vehicle platoons in 5G-based V2X networks under different handover scenarios. The proposed protocol has been formally verified by BAN-logic and the Scyther tool to prove its security. And it has been analyzed on its security functionality to show its ability to resist major typical malicious attacks. The proposed protocol has achieved a lower overhead than other compared protocols. Our experimental results suggest that the proposed protocol can support platoon authentication securely and efficiently.

ACKNOWLEDGMENT

This research is supported by A*STAR under its RIE2020 Advanced Manufacturing and Engineering (AME) Industry Alignment Fund – Pre Positioning (IAF-PP) (Award A19D6a0053). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of A*STAR.

REFERENCES

[1] I. Gharsallah, S. Smaoui, and F. Zarai, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5g cellular networks," *IET Information Security*, vol. 14, no. 1, pp. 21–29, 2019.

[2] G. Li, C. Lai, R. Lu, and D. Zheng, "Seccdv: A security reference architecture for cybertwin-driven 6g v2x," *IEEE Transactions on Vehicular Technology*, 2021.

[3] P. Wang, B. Di, H. Zhang, K. Bian, and L. Song, "Platoon cooperation in cellular v2x networks for 5g and beyond," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 3919–3932, 2019.

[4] C. Lai, H. Zhou, N. Cheng, and X. S. Shen, "Secure group communications in vehicular networks: A software-defined network-enabled architecture and solution," *IEEE Vehicular Technology Magazine*, vol. 12, no. 4, pp. 40–49, 2017.

[5] 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.

[6] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3gpp 5g networks," *IEEE communications surveys & tutorials*, vol. 22, no. 1, pp. 170–195, 2019.

[7] A. Sharma, A. Jain, and I. Sharma, "Exposing the security weaknesses of fifth generation handover communication," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2019, pp. 1–6.

[8] X. Yan, M. Ma, and R. Su, "A certificateless efficient and secure group handover authentication protocol in 5g enabled vehicular networks," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 1678–1684.

[9] G. Li and C. Lai, "Platoon handover authentication in 5g-v2x: Ieee cns 20 poster," in *2020 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2020, pp. 1–2.

[10] *AVISPA v1.1 User Manual*.

[11] Y. Glouche, T. Genet, O. Heen, and O. Courtay, "A security protocol animator tool for avispa," in *ARTIST2 workshop on security specification and verification of embedded systems, Pisa*, 2006, pp. 1–7.

[12] V. O. Nyangaresi, A. J. Rodrigues, and S. O. Abeka, "Efficient group authentication protocol for secure 5g enabled vehicular communications," in *2020 16th International Computer Engineering Conference (ICENCO)*. IEEE, 2020, pp. 25–30.

[13] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve secure handover session key management via mobile relay in lte-advanced networks," *IEEE internet of things journal*, vol. 4, no. 1, pp. 29–39, 2016.

[14] X. Yan and M. Ma, "A privacy-preserving handover authentication protocol for a group of mtc devices in 5g networks," *Computers & Security*, p. 102601, 2022.

[15] C. J. F. Cremers, *Scyther: Semantics and verification of security protocols*. Eindhoven university of Technology Eindhoven, Netherlands, 2006.

[16] J. Cao, H. Li, and M. Ma, "Gahap: A group-based anonymity handover authentication protocol for mtc in lte-a networks," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 3020–3025.

[17] A. Fu, G. Zhang, Y. Zhang, and Z. Zhu, "Ghap: An efficient group-based handover authentication mechanism for ieee 802.16 m networks," *Wireless personal communications*, vol. 70, no. 4, pp. 1793–1810, 2013.

[18] J. Cao, H. Li, M. Ma, and F. Li, "Ugha: Uniform group-based handover authentication for mtc within e-utran in lte-a networks," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 7246–7251.

[19] J. Cao, M. Ma, and H. Li, "G2rha: Group-to-route handover authentication scheme for mobile relays in lte-a high-speed rail networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 9689–9701, 2017.

[20] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

[21] S. Gupta, B. L. Parne, and N. S. Chaudhari, "Srgh: A secure and robust group-based handover aka protocol for mtc in lte-a networks," *International Journal of Communication Systems*, vol. 32, no. 8, p. e3934, 2019.

[22] R. Ma, J. Cao, D. Feng, H. Li, and S. He, "Ftgpha: Fixed-trajectory group pre-handover authentication mechanism for mobile relays in 5g high-speed rail networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2126–2140, 2019.

[23] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The tamarin prover for the symbolic analysis of security protocols," in *International conference on computer aided verification*. Springer, 2013, pp. 696–701.

[24] Z. Haddad, A. Alsharif, A. Sherif, and M. Mahmoud, "Privacy-preserving intra-mme group handover via mrn in lte-a networks for repeated trips," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2017, pp. 1–5.

[25] J. Cao, M. Ma, H. Li, Y. Fu, and X. Liu, "Eghr: Efficient group-based handover authentication protocols for mmtc in 5g wireless networks," *Journal of Network and Computer Applications*, vol. 102, pp. 1–16, 2018.

[26] C. Lai and Y. Ma, "A novel group-oriented handover authentication scheme in mec-enabled 5g networks," in *2021 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2021, pp. 29–34.

[27] M. M. Modiri, J. Mohajeri, and M. Salmasizadeh, "Gslha: Group-based secure lightweight handover authentication protocol for m2m communication," in *2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*. IEEE, 2019, pp. 15–20.

[28] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *International conference on the theory and application of cryptology and information security*. Springer, 2003, pp. 452–473.

[29] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*. Springer, 1984, pp. 47–53.

[30] C. V. Wright and M. Varia, "Crypto crumple zones: Enabling limited access without mass surveillance," *Euro S&P*, 2018.

[31] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 219, pp. 225–235, 2013.

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

[33] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2003, pp. 416–432.

[34] L. Zhang, B. Qin, Q. Wu, and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," *Computer Networks*, vol. 54, no. 14, pp. 2482–2491, 2010.

[35] X. Yan and M. Ma, "A lightweight and secure handover authentication scheme for 5g network using neighbour base stations," *Journal of Network and Computer Applications*, vol. 193, p. 103204, 2021.

[36] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[37] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 16)*, v16.1.0 ed., 3PP Support Office, 2019.

[38] X. Yan and M. Ma, "Nseha: A neighbor-based secure and efficient handover authentication mechanism for 5g networks," in *2021 9th International Conference on Communications and Broadband Networking*, 2021, pp. 209–216.

[39] H. Lee, D. Kim, B. Chung, and H. Yoon, "Adaptive hysteresis using mobility correlation for fast handover," *IEEE Communications Letters*, vol. 12, no. 2, pp. 152–154, 2008.

[40] H. Shu, F. Chen, D. Xie, L. Sun, P. Qi, and Y. Huang, "An aggregate signature scheme based on a trapdoor hash function for the internet of things," *Sensors*, vol. 19, no. 19, p. 4239, 2019.

[41] 3GPP, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the 5g System; (Release 16)*, 3PP Support Office, Jul 2020.