Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 6251219, 15 pages
https://doi.org/10.1155/2018/6251219

Research Article

An Anonymous Handover Authentication Scheme Based on LTE-A for Vehicular Networks

Cheng Xu[1,2] **Xiaohong Huang**[1] **Maode Ma**[3] **and Hong Bao**[2]

[1]*Institute of Network Technology, Beijing University of Posts and Telecommunications, China*
[2]*Beijing Key Laboratory of Information Service Engineering, Beijing Union University, China*
[3]*School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore*

Correspondence should be addressed to Xiaohong Huang; huangxh@bupt.edu.cn

Received 22 October 2017; Accepted 28 May 2018; Published 3 July 2018

Academic Editor: Jaime Lloret

Vehicular networks play an important role in the intelligent transportation systems which have gained technical supports from car industry. Due to the mobility and the broadcast nature of wireless communication, security of the vehicular networks is a critical issue for the academia and industry. Many solutions have been proposed to target the security provisioning. However, most of them have various shortcomings. Based on the elliptic curve public key cryptography algorithm, in this paper, we propose a new anonymous roaming authentication protocol for the Long Term Evolution-Advanced (LTE-A) supported vehicular networks. For a vehicular LTE-A network, an authentication protocol should be able to fulfill a variety of security requirements, which can be met by our proposal and proved by using Burrows–Abadi–Needham (BAN) logic. Compared with some existing solutions, our scheme has lower communication costs with stronger security functionality. The analyses on the security functions and the performance of the proposed solution show that our scheme is secure and efficient with ability against various types of malicious attacks.

1. Introduction

A vehicular ad hoc network (VANET) is a mobile self-organized network in the intelligent transportation system (ITS). It has basic characteristics of a large delay-tolerant network, including long communication delays and multiple asynchronous transmission capabilities. A vehicular network is a variety of a mobile ad hoc network (MANET) used in ITS. [1]. It is comprised of vehicle on-board units (OBUs), roadside units (RSUs), which are the fixed units deployed at sides of the road, the control center, etc. An OBU at a vehicle can equip a GPS device, 3G/4G communication modules, radar, and the car-body-mounted sensory for identification of its own state, road conditions, traffic on road status with the ability to exchange information of the communications environment, which includes the body position, movement speed, driving direction, states of communications link, etc. A RSU is a bridge of the vehicle and the Internet. The vehicular network not only needs to provide navigation and traditional services such as entertainment but also involves the collection and distribution the traffic safety related information such as collision warning alarm [2].

Recent research on vehicular network has focused on major five areas: (1) the collaborative security applications on the road safety for the vehicles involved [3], (2) data transmission, information distribution, and data collation methods, (3) traffic and vehicle movement modeling, (4) the physical layer and medium access control (MAC) layer communications, and (5) privacy and identity authentication. These studies, which are aimed at improving traffic and network security, the efficiency of traffic, and the data communication, can promote the development of the ITS [4]. The Long Term Evolution-Advanced (LTE-A) wireless systems have been suggested to be used in the vehicular environments to improve the efficiency of the wireless communication in vehicular networks. With the application of the systems, the design and deployment of the vehicular networks will need less network components to obtain a higher system capacity and a larger coverage of the wireless communication. In addition, higher data rates, low access latency, flexible bandwidth, and seamless integration with other existing wireless communication systems could also be achieved [5].

1.1. Related Work. To provide LTE-A security functionality, a strong user authentication scheme in a mobile network should conform to the following requirements including the ability of resistance to impersonation attacks, foreign agent impersonation attacks, home agent impersonation attacks, offline password guessing attacks, and insider attacks. It also needs to be user-friendly and ensure user anonymity, proper mutual authentication, local verification, etc. [6]. In [7], a security scheme has been proposed, which is more suitable for the resource-limited mobile devices with low-power and it holds the ability against various malicious attacks with many outstanding features. In the LTE-A networks, the Evolved Packet System Authentication and Key Agreement (EPS-AKA) has been specified in the 3GPP standard to provide mutual authentication, key management, and key materials refresh between an eNodeB, which can be used as RSU in the vehicle environment, and a mobile node, which is supposed to be an OBU in the vehicular networks. Although the EPS-AKA scheme in the LTE-A networks and some other similar proposals can ensure the mutual authentication and key management in general, there are still some vulnerabilities existing in the mobility management in the LTE-A based vehicular networks. Particularly, three critical shortcomings exist in the handover procedures. (1) First is lack of backward security [8]. In the LTE-A systems, the standard inevitably inherits the defects of its predecessor UMTS-AKA protocol without backward-compatibility support and it cannot resist some popular types of malicious attacks, such as the redirection and man-in-the-middle attacks. At the same time, it has other security weakness as any other EPS-AKA schemes, such as the lack of privacy protection and key forward/backward secrecy (KFS/KBS) with the emergent new challenges in validation of group communication. (2) Second is vulnerability to desynchronization attacks [9]. In the LTE-A systems, the key management can prevent any compromise of the key(s) or any one piece of isolated network equipment. However, by the design, there exists a loophole in the handover key management phase, which is so-called the synchronization attack, which is an attack that threatens secure communication between the mobile node and the network. (3) Third is vulnerability to replay attacks [10]. The purpose of these types of attacks is to destroy the relationship between the OBU and the target eNodeB. Generally, the mobility management entity (MME) generates and sends an initial key to the service eNodeB. In fact, the service eNodeB always derives a new eNodeB key and sends it to the target eNodeB during any inter-eNodeB handover. Therefore, the connection between the OBU and the service eNodeB will not be kept and a new handover procedure will start.

For the secure handover in the LTE-A networks, it is found that some earlier security schemes are unlikely to provide user anonymity due to the inherent design flaws, which are also susceptible to playback and simulated attacks [11, 12]. Then, a powerful user authentication scheme for a wireless smart card has been designed. However, it is shown that the scheme in [11, 12] lacks user friendliness and cannot provide user anonymity and unfairness in key agreement [13]. And further an enhanced anonymous authentication scheme has been proposed to achieve the anonymity for a roaming service in the global mobile networks [14]. To remedy some of the weaknesses, [9] proposed a novel anonymous authentication scheme in the LTE networks. It is shown in [15] that a recently proposed protocol named PairHand can outperform other protocols in terms of security and efficiency, which could be a potential candidate for the deployment in the vehicular networks. However, these schemes still need to independently send authentication request messages to the network. Secure and efficient handover authentication should possess the following functional attributes [16]: subscription validation, server authentication, key establishment, user anonymity and untraceability, conditional privacy preservation, provision of user revocation, attack resistance, periodic session key updating, low communication cost, and low computational complexity.

By the previous work, we have explored that some security schemes are vulnerable to impersonation. For LTE-A, it needs to provide user friendliness and user anonymity, lacking backward security and local verification. To remedy the weaknesses, we propose a novel anonymous roaming authentication scheme (ARHAP) for the LTE-A based VANETs.

1.2. Our Contributions. The ARHAP scheme works based on the elliptic curve public key cryptography to implement the secure and efficient handovers between the service and target eNodeBs in a LTE-A network. The outstanding features of the ARHAP scheme can be summarized as follows: (1) simplification of the generation of session keys to realize secure and efficient handovers in the LTE-A based VANET systems, (2) the ability to conform to the demand of basic security and privacy protection, (3) efficient reduction of the computational and communication costs resulting in a better performance to be applicable into the VANET systems.

The rest of the paper is organized as follows. In Section 2, we provide a brief introduction on the network architecture and the security requirements. In Section 3, we describe the proposed the ARHAP scheme in detail. In Section 4, we prove the correctness of the ARHAP scheme by using BAN logic and formally verify the security function of the ARHAP scheme under intruder attacks by using AVISPA. In Section 5, we compare the performance of the proposed ARHAP scheme with those of other authentication schemes by simulation experiments. We have the conclusion of the paper in Section 6.

2. Network Environment and Security Goals

The LTE-A network has its outstanding feature of flexibility to be deployed. It is open, secure, reliable, and easy to operate [2]. Figure 1 shows a VANET working over a LTE-A network infrastructure. A LTE-A system consists of a core network, named as an evolved packet core (EPC), and a wireless access network, named as the evolved-universal terrestrial radio access network (E-UTRAN). E-UTRAN has many evolved NodeB, each of which can communicate with a mobile node [17]. The EPC core network is the native, all-IP-based and multiaccess network that enables the deployment and operation of a common network for each kind of 3GPP

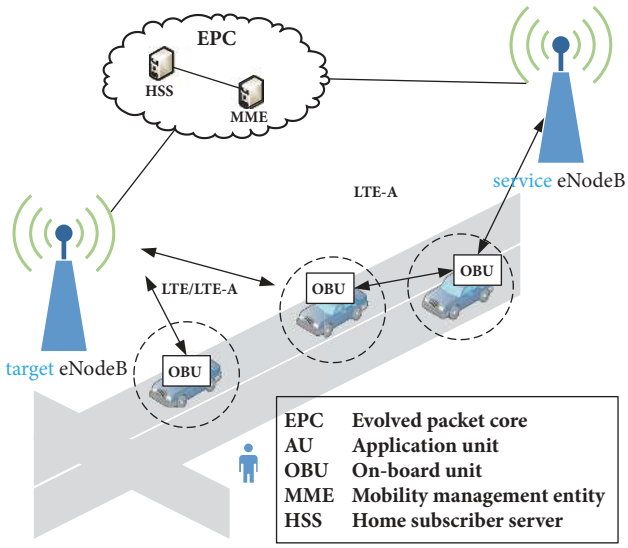

Figure 1: LTE-A Infrastructure for vehicular network environment.

access networks including 2G, 3G, and LTE. The E-UTRAN is connected to the EPC core network as the wireless access points, which have various layers of the protocol stack to support high-bandwidth applications together with real-time constraints, QoS, and high availability to the wireless mobile devices [18].

The LTE-A system can be deployed as the infrastructure for vehicular networks to make them work in a more cost-effective way [19]. By using the LTE-A systems, it is possible to reduce the latency to a few milliseconds required for real-time applications [20]. It has been envisioned to exploit the existing LTE-A infrastructure to support vehicular networking applications through an advanced LTE-enabled OBU or by using smart phones with LTE-A wireless access connectivity [21]. In terms of mobility, the E-UTRAN supports handovers across the distinct cells controlled by different eNodeBs in the LTE-A networks when a vehicle travels at a low mobile speed, from 0 to 15 km/h or a higher speed. The LTE-A systems have been qualified as a suitable candidate to be used in the VANETs due to many other features of the technology such as its extraordinary performance in terms of a higher data transmission rate, a lower latency, ease of deployment, and its infrastructure [22].

When an OBU accesses the EPC, the MME needs to connect with home subscriber server (HSS) to obtain the corresponding authentication information. Then, the mutual authentication between the OBU and the HSS controlled by security protocols [1, 23] can be realized.

2.1. Elliptic Curve Cryptography. The elliptic curve cryptography (ECC) and some relevant mathematical assumptions have been widely used for the authentication purpose. Compared with other public key cryptographies, elliptic curve cryptosystem has significant advantages of the small-size keys with fast calculations [15]. The ECC is the system with the highest encryption intensity for each bit in the known public key system. The best algorithm to solve the discrete logarithm problem on elliptic curve is the Pollard rho method, whose time complexity is complete exponential order, where n is the binary representation of m in equation $mP=P+P+\ldots+P=Q$. When $n=234$, Q is about 2117; it will take 1.6x1023 MIPS years. The advantage of the shorter ECC key is very obvious; with the increase of encryption strength, the key length changes a little. The ECC works based on the elliptic curve discrete logarithm problem, which is a known, nondeterministic polynomial (NP) hard problem. It has been widely used in several encryption schemes in the wireless networking environment to provide the required security functionality and computational efficiency. Thus, the use of the ECC can largely reduce storage and transmission costs, which fits well with the resource limitations while achieving the goal of ensuring system security.

There are three elliptic curve groups that need calculations in designing secure encryption schemes. For cyclic additive group G, all elements Q in G have the form $Q=rP$, for some $P\in G$. In this case, we call P a generator of G, where $rP=P+P+\ldots+P$ (r times).

For cyclic multiplicative group G_T, all elements y in G_T have the form $y=g^k$ for some g in G_T, where g is a generator of G_T and $g^k=g\ldots g$ (k times).

For elliptic curve group, let p be a prime number and F_p denote the field of integers modulo p. An elliptic curve E over F_p is defined as $y^2=x^3+ax+b$, where $a, b\in F_p$ satisfies $4a^3+27b^2\neq 0 \bmod p$.

In order to prove our proposed security protocol, we put forward some important calculation problems using the elliptic curve group in designing secure encryption schemes.

Problem 1 (computational discrete logarithm (CDL)). Given $R=xP$, where $P, R\in G_p$, it is easy to calculate R given x and P, but it is difficult to determine x given P and R.

Problem 2 (computational Diffie-Hellman (CDH)). Given P, xP, $yP\in G_p$, it is difficult to compute $xyP\in G_p$.

Problem 3 (elliptic curve factorization (ECF)). Given two points P and $R=x\cdot P+y\cdot P$, for $x, y \in Z_q^*$, it is difficult to find $x\cdot P$ and $y\cdot P$.

2.2. Security Goals. In particular, the following security requirements should be achieved by any designed security proposals. The security requirements include the following.

(1) Anonymous handover and secure key agreement: the authentication and key agreement protocol can realize mutual authentication between the OBU and the LTE-A networks. The encryption algorithm and integrity protection is the basic requirement in the process of session key agreement. Therefore, anonymous handover can realize the confidentiality of the OBU identity to prevent attackers tracking the user location. Both the OBU at a vehicle and the target eNodeB as the RSUs must authenticate each other in a handover procedure. After mutual authentication, a fresh session key could be generated to provide data confidentiality and integrity in the communication processes between the OBU and the target eNodeB.

(2) Privacy preserving: the identities of the OBUs should be hidden from normal message receivers during the

Table 1: Notations used in the ARHAP scheme.

Notation	Description
OBU, MME, eNodeB, HSS	On-board units equip in vehicle, Mobile management entity, evolved NodeB, Home subscriber server
ID_X, PW_X	Identity and password of an entity X
P	Elliptic curve, the basis of order for n
h()	Hash function
$E_K[]/D_K[]$	Symmetrical encryption and decryption of key K
$E_K\{\}/D_K\{\}$	Unsymmetrical encryption and decryption of key K
‖	Concatenation operation
⊕	XOR operation
SK	Session key

handover authentication process. When the OBU is performing authentications, the LTE-A networks cannot reveal their true identities to the public.

(3) Attacks resistance: the designed scheme should have the ability to resist various attacks in the LTE-A networks, including replay attacks, redirection attacks, and man-in-the-middle attacks.

3. Proposed Scheme: ARHAP

In this section, we describe our proposed ARHAP scheme with the aim of achieving an anonymous handover authentication in vehicular LTE-A networks. The ARHAP scheme has been designed with 2 components: (1) mutual authentication and key agreement and (2) handover authentication. Since, in a LTE-A based VANET, an OBU at a vehicle needs first to connect the network for the registration and authentication, the first step of the actions includes initialization, registration, authentication, and the session key establishment. Once a handover happens, the control of communication changes from the current eNodeB to a target eNodeB, which needs to perform a mutual authentication between the OBU and the target eNodeB.

In a LTE-A based VANET, the proposed ARHAP scheme will simplify the session key generation using elliptic curve cryptography and can conform to the requirements of security functionality. In addition, the privacy of the vehicular can also be protected in the anonymous roaming handover authentication procedure. Table 1 lists the notations used in the proposed scheme.

3.1. Mutual Authentication and Key Agreement. The normal process of the mutual authentication and key agreement includes 3 phases: initialization, registration, and authentication and establishment of a session key. When the ARHAP scheme starts to work, the OBU at a vehicle requires initialization of the system parameters. It also needs to connect to the EPC to complete the registration to the EPC. Once it initially enters into a new LTE-A based VANET, the OBU first connects to eNodeB to perform an authentication for the establishment of a session key. After completing the mutual authentication, the OBU will execute a fast and secure handover process to change the control of communication from the service eNodeB to the target eNodeB.

3.1.1. Initialization Phase. In this phase, an OBU at a vehicle needs to access the network to obtain the system parameters, while the MME in its role as the mobility management entity selects the system parameters on behalf of the EPC to provide to the OBU and completes the initialization process.

The MME selects a secure elliptic curve on F_p and randomly selects c and y and computes $C=cP$. y and C are used as the MME key. S_{eNodeB} is used as the private key of eNodeB. S_{MME} is used as the private key of the MME.

Step 1. Choose G1, G2 as 2 loops of an additive group, whose order is of a large prime number q. P1 and P2 are the generators of G1 and G2, respectively. Ψ is the G2 and G1 isomorphism, satisfying $\Psi(P2)=P1$.

Step 2. Choose a random number $x=Z_q^*$ as a private key, and compute $Y=xP_2$ as the public key.

Step 3. Choose one-way hash functions $h()$, $F_{T1}()$, and $F_{KEY}()$.

Step 4. For each OBU and eNodeB, distribute public system parameters $\{G1, G2, q, P1, P2, \Psi, h, F_{T1}, F_{KEY}\}$.

3.1.2. Registration Phase. In this phase, the OBU needs to connect to the EPC via the HSS/authentication center (AuC) as a representative of the MME to complete the OBU-to-EPC registration. It acts in the following steps.

Step 1. An OBU chooses its identity ID_{OBU} and password PW_{OBU} and generates a random number r_{OBU}. It then computes $Z=h(r_{OBU}\|PW_{OBU})$, chooses a failure time stamp Exd through a secure channel, and submits $ID_{OBU}\|Z\|Exd$ to the MME.

Step 2. After the MME receives the registration request, it will test whether Exd is effective, checking if the failure has resulted in a refusal to the request of registration or if the HSS request on the user's authentication vector (AV)s is effective.

Step 3. The MME receives an authentication data request for the OBU-generated AVs, including authentication token, expected response, and the AVs as authentication data response to the MME.

Step 4. The MME receives the authentication data response and sends the AVs as a certification request to the OBU.

Step 5. The OBU receives the authentication request, verifies the validity of the Auth, and then calculates the response (RES), as the authentication response to the MME.

Step 6. The MME receives the authentication response and compares the RES and XRES Booleans for equality. Then, $Q=h(ID_{OBU}\|y)\oplus h(PW_{OBU}\|r_{OBU})$, $H=$

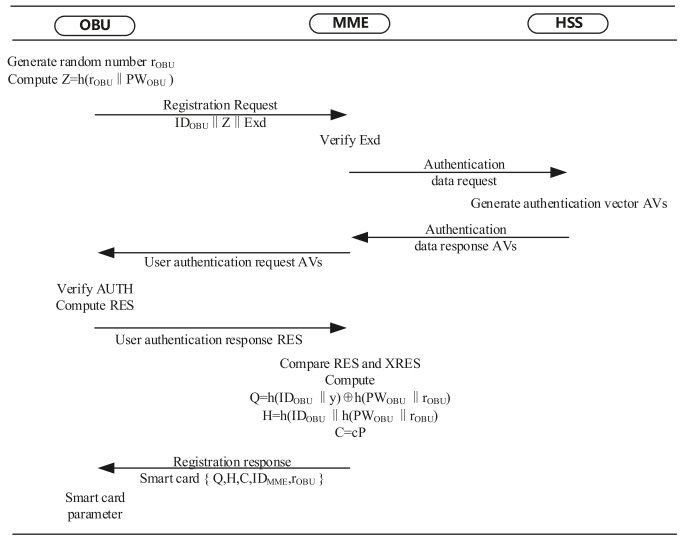

Figure 2: Registration phase.

$h(ID_{OBU} \| h(PW_{OBU} \| r_{OBU})$, and $C=cP$ are computed. The MME stores the message $\{Q, H, C, ID_{MME}, r_{OBU}\}$ in a smart card and submits the smart card data to the OBU through a secure channel. Figure 2 illustrates the registration phase.

3.1.3. Authentication and Session Key Establishment Phase. In this phase, the vehicular user OBU roams into another eNodeB to access the services from the target eNodeB. The eNodeB and the OBU first need to authenticate each other via a mutual authentication process to change some information and then negotiate to produce a session key. The authentication and establishment of session key phase of the proposed scheme proceeds as follows.

Step 1. The user at the vehicle inserts its smart card into the reader and inputs identity ID_{OBU} and password PW_{OBU}. Then, $H^*=h(ID_{OBU} \| h(PW_{OBU} \| r_{OBU})$ and $Z=h(r_{OBU} \| PW_{OBU})$ will be computed with a checking to judge whether $H=H^*$. If they are equal, it means that the OBU is a legitimate vehicular user. Otherwise, the session will be stopped. Next, a random number is generated, and $A=aP$, $R_{AC}=aC$, $N=Q \oplus h(PW_{OBU} \| r_{OBU})$, $DID_{OBU}=ID_{OBU} \oplus h(R_{AC})$, and $V_1=h(N \| R_{AC} \| ID_{MME})$ are computed, and the introductory request message $\{A, DID_{OBU}, C, V_1, ID_{MME}\}$ is sent to eNodeB though a public channel.

Step 2. The eNodeB receives the message $\{A, DID_{OBU}, C, V_1, ID_{MME}\}$ and then generates random number b and computes $B=bP$, $R_{BC}=bC$, $W_2=E_{RBC}[A, B, Cert_{eNodeB}, V_1, DID_{OBU}]$, and $V_2=E_{SeNodeB}\{h(A, B, Cert_{eNodeB}, V_1, DID_{OBU})\}$. $Cert_{eNodeB}$ is eNodeB's certificate and $E_{SeNodeB}$ is the private key of eNodeB. Then, eNodeB sent data-messages $\{B, W_2, V_2\}$ to the MME.

Step 3. The MME receives $\{B, W_2, V_2\}$ and then computes $R_{BC}=cB$ and decrypts $D_{RBC}[W_2] \longrightarrow A, B, Cert_{FA}, V_1, DID_{OBU}$. Next, signature V_2 is verified. Only if verification is successful does the MME certify eNodeB. Then, the MME computes $R_{AC}=cA$, $ID_{OBU}=DID_{OBU} \oplus h(R_{AC})$, and $V_1{}^*=h(h(ID_{OBU} \| y) \| R_{AC} \| ID_{MME})$. Next, it computes whether $V_1=V_1{}^*$ is verified. Only if the verification is successful, the MME certifies the OBU. Then, random number b is generated; $D=dP$ and $G_{OBU}=dB \oplus R_{AC}$ are computed, followed by computation of $W_1=h(h(ID_{OBU} \| y) \| dB \| A \| D \| ID_{eNodeB} \| ID_{MME})$, $W_3=E_{RBC}[ID_{eNB}, G_{OBU}, Cert_{eNodeB}, dA, A, B, D, W_1]$, and $V_3=E_{SMME}\{h(ID_{eNB}, G_{OBU}, Cert_{eNodeB}, dA, A, B, D, W_1)\}$. Then, the MME sends $\{W_3, V_3\}$ to eNodeB.

Step 4. The eNodeB decrypts $D_{RBC}[W_3] \longrightarrow ID_{eNB}, G_{OBU}, Cert_{eNodeB}, dA, A, B, D, W_1$. Then, the signature V_3 is verified. Only if the verification is successful, the eNodeB certifies the OBU and MME. $SK=h(bA)$ is computed and $W_4=E_{SK}[ID_{eNB}, D, W_1]$ is encrypted, and then eNodeB sends $\{G_{OBU}, W_4\}$ to the OBU.

Step 5. Upon receiving the message $\{G_{OBU}, W_4\}$, the OBU computes $dB=G_{OBU} \oplus R_{AC}$ and $SK=h(bA)$, and decrypts $D_{SK}[W_4] \longrightarrow ID_{eNodeB}, D, W_1$. Then, $W_1{}^*=h(N \| dB \| A \| D \| ID_{eNodeB} \| ID_{MME})$ is computed. Next, $W_1{}^*=W_1$ is verified. Only if the verification is successful, the OBU certifies the eNodeB and the MME. Then, $SK=h(aB)$ and $Auth=h(W_1 \| aB)$ are computed, and the OBU sends $Auth$ to the eNodeB.

Step 6. After the eNodeB receives $\{Auth\}$, it computes $Auth^*=h(W_1 \| bA)$ and then verifies whether $Auth^*=Auth$. Only if the verification is successful, the eNodeB establishes a session key $SK=h(bA)$.

Figure 3 illustrates the authentication and establishment of session key phase.

3.2. Handover Authentication. An OBU in the process of roaming must perform a handover authentication from the current eNodeB to the target eNodeB. The handover needs to

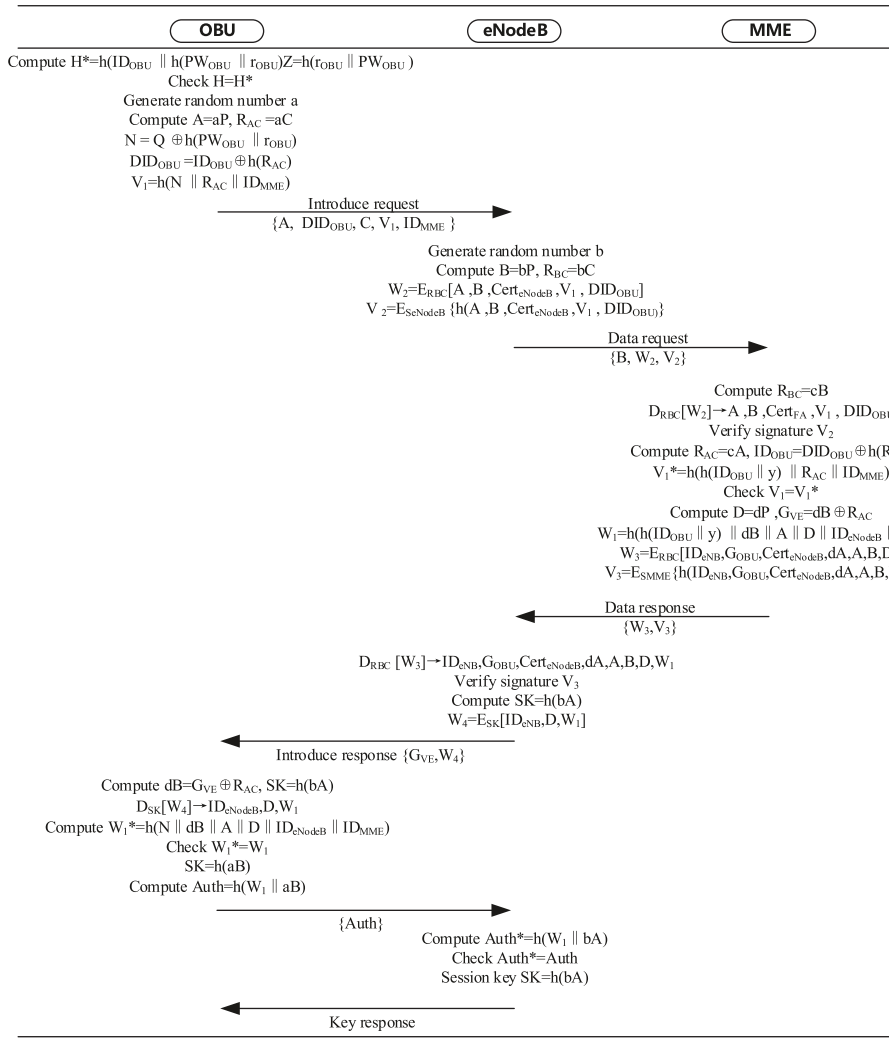

Figure 3: Authentication and session key establishment phase.

perform an authentication between the OBU and the target eNodeB after exchanges of control information to negotiate a new session key. When the connected users disconnect and reconnect to target eNodeB, the delay include transmission delay, propagation delay, and authentication processing delay. The handover authentication phase proceeds as follows.

Step 1. The OBU sends a handover request to the service eNodeB_1.

Step 2. The eNodeB_1 receives the handover request, then computes $SK_2=h(SK_1,\alpha)$, sends SK_2 to eNodeB_2, and sends the handover response to the OBU.

Step 3. The OBU receives the handover response, computes $SK_2=h(SK_1,\alpha)$, and then selects a random number a_i and computes a_iD. The OBU sends $\{a_iD\}$ to eNodeB_2 as the key request.

Step 4. The eNodeB_2 receives $\{a_iD\}$ and then selects a random number b_i and computes b_iD. Next, the new session key $Sk_i=h(b_ia_iD)$ is generated, and $S_i=h(b_ia_iD\|Sk_{i-1})$ is computed. eNodeB_2 sends $\{b_iD, S_i\}$ to the OBU.

Step 5. The OBU receives $\{b_iD, S_i\}$, then computes $S_i^*=h(a_ib_iD\|Sk_{i-1})$, and verifies whether $S_i^*=S_i$. Only if the verification is successful, the new session key $SK_i=h(a_ib_id_iP)$ is rendered valid.

Figure 4 illustrates the handover authentication phase.

After completing the above interactions, the OBU and eNodeB_2 share the new session key SK_i.

4. Security Evaluation

In this section, the security objectives of the ARHAP scheme are analyzed. The Burrows–Abadi–Needham (BAN) logic, along with the results of analysis by using the formal verification tool of automated validation of Internet security protocols and applications (AVISPA), is used to confirm that the security objectives can be met. Analysis shows that the ARHAP scheme can work correctly to achieve the security objectives. In addition, a comparative analysis of security

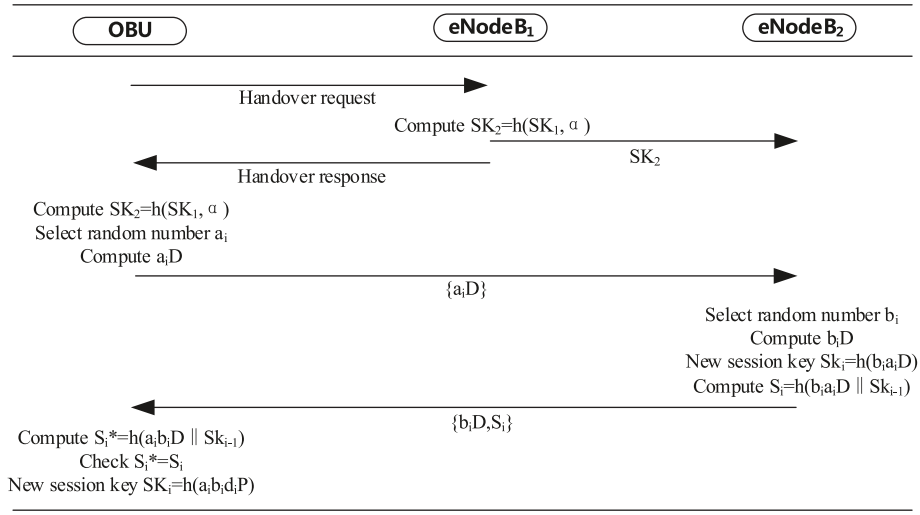

Figure 4: Handover authentication phase.

functionality is done against other relevant schemes with the results to show that the ARHAP scheme is secure and efficient in the vehicular networks.

4.1. Proof of Security Objectives. At present, the most widely used method of formal analysis of security protocol is the formal logic analysis method. It plays an important role to verify security protocols, especially the analysis of the authentication protocol. Cohen et al. [24] proposed a kind of logic expression based on the BAN logic of belief. By BAN logic, lots of protocols can be verified. Furthermore, BAN logic has played a significant role for the security protocol development.

The logical symbols and inference rules of BAN logic [25] are described as follows.

(1) P,Q: subjects, that is, the principal participants in the protocol.

(2) X: message.

(3) K: secret key.

(4) $\{X\}_K$: message X is encrypted with K.

(5) P|≡Q: P believes Q.

(6) P◁X: P has received message X.

(7) $P|\sim X$: P said X.

(8) Q⟹X: Q has the jurisdiction to X.

(9) #(X): X is fresh.

(10) $P \overset{K}{\longleftrightarrow} Q$: K is the common preshared key of P and Q.

BAN logic specifies the message-meaning rules, nonce-verification rules, jurisdiction rules, etc. The messages above the horizontal line are known as the conditions, while those below it are the results deduced from the known conditions.

(1) Message-meaning rules: P shares the secret key K with Q. If P receives a message that X encrypted with K, then P believes that Q has sent X.

(2) Nonce-verification rule: if P believes that message X is fresh and believes that Q has sent X, then P believes that Q believes X.

(3) Jurisdiction rules: if P believes Q has sent message X, and P believes that Q believes X, then P believes X.

(4) Belief-joint rules: if P believes X and Y, then P believes messages of a cascade of X and Y. If P believes that Q believes messages of a cascade of X and Y, then P believes that Q believes X or Y. If P believes that Q has said X and Y, then P believes that Q has said X or Y; if P believes the message of a cascade of X and Y, then P believes X or Y.

(5) Freshness-joint rule: if P believes that X is fresh, P believes the entire message of a cascade with X is fresh.

(6) Reception rules: if P receives messages of a cascade of X and Y, we consider that P receives X or Y; if P receives the connection of the formula of X and Y, we consider that P receives X or Y; P shares secret key K with Q. If P receives message X encrypted with K, we can infer that P receives X.

(7) Additional rules: secret key K is fresh. If P receives message X encrypted with K and P believes that P shares secret key K with Q, we can infer that P believes Q has sent message X and that P believes that Q believes P shares secret key K with Q.

In the following, based on the BAN logic model, we will express that the mutual authentication and key agreement between the OBU and the LTE-A network can be correctly realized. The proof process is as follows.

(1) Protocol Idealization. To facilitate the derivation, by using BAN logic analysis, the first step is to convert every step of the authentication into the idealized form.

$$m_1 : OBU \longrightarrow MME : \langle A, ID_{MME} \rangle_{h(ID_{OBU} \| y)};$$

$m_2 : eNodeB \longrightarrow MME : \langle B \rangle_{S_{eNodeB}}$;

$m_3 : MME \longrightarrow OBU : \langle A, B, ID_{eNodeB}, OBU \overset{dB}{\longleftrightarrow} eNodeB \rangle_{h(ID_{OBU} \| y)}$;

$m_4 : MME \longrightarrow eNodeB : \langle A, B, OBU \overset{dA}{\longleftrightarrow} eNodeB \rangle_{S_{MME}}$;

$m_5 : eNodeB \longrightarrow OBU : \langle A, B, OBU \overset{SK}{\longleftrightarrow} eNodeB \rangle_{SK}$;

$m_6 : OBU \longrightarrow eNodeB : \langle A, B, OBU \overset{SK}{\longleftrightarrow} eNodeB \rangle_{SK}$.

(2) Initial Assumption. The initial assumption is the important guarantee for the logic analysis on the proposed scheme to be successfully conducted. The assumption includes which key is the initial shared, which key in some situations to be trusted, and which key generates a new value. Initial assumptions for the proposed agreement are the following.

$A1$: $OBU \mid\equiv \#(B)$;

$A2$: $eNodeB \mid\equiv \#(A)$;

$A3$: $MME \mid\equiv \#(A)$;

$A4$: $MME \mid\equiv \#(B)$;

$A5$: $OBU \mid\equiv \#MME \Longrightarrow OBU \overset{dB}{\longleftrightarrow} eNodeB$;

$A6$: $eNodeB \mid\equiv \#MME \Longrightarrow OBU \overset{dA}{\longleftrightarrow} eNodeB$;

$A7$: $MME \mid\equiv OBU \mid \Longrightarrow A$;

$A8$: $MME \mid\equiv eNodeB \mid \Longrightarrow B$;

$A9$: $MME \mid\equiv OBU \mid \Longrightarrow ID_{OBU}$;

$A10$: $OBU \mid\equiv OBU \overset{h(ID_{OBU} \| y)}{\longleftrightarrow} MME$;

$A11$: $MME \mid\equiv OBU \overset{h(ID_{OBU} \| y)}{\longleftrightarrow} MME$;

$A12$: $eNodeB \mid\equiv \mid \overset{P_{MME}}{\longrightarrow} MME$;

$A13$: $MME \mid\equiv \mid \overset{P_{eNodeB}}{\longrightarrow} eNodeB$.

(3) Protocol Goal. The ultimate goal of the proposed scheme is to realize the mutual authentication between the OBU and the eNodeB and establish a shared session key. The expression of the objectives can be expressed by BAN logic as follows.

$Goal1$: $OBU \mid\equiv OBU \overset{SK}{\longleftrightarrow} eNodeB$;

$Goal2$: $OBU \mid\equiv eNodeB \mid\equiv OBU \overset{SK}{\longleftrightarrow} eNodeB$;

$Goal3$: $eNodeB \mid\equiv OBU \overset{SK}{\longleftrightarrow} eNodeB$;

$Goal4$: $eNodeB \mid\equiv OBU \mid\equiv OBU \overset{SK}{\longleftrightarrow} eNodeB$.

(4) Protocol Annotations and Target Derivation. Based on m_1, we have

$Statment\ 1 : MME \triangleleft \langle A, ID_{MME} \rangle_{h(ID_{OBU} \| y)}$

Based on Statement 1 and A11, by the message-meaning rule,

$Statement\ 2 : MME \mid\equiv OBU \mid\sim \langle A, ID_{MME} \rangle$

Based on Statement 2 and A3, by the fresh value validation and freshness verification rules,

$Statement\ 3 : MME \mid\equiv OBU \mid\equiv \langle A, ID_{MME} \rangle$

Based on m_2,

$Statement\ 4 : MME \triangleleft \langle B \rangle_{S_{eNodeB}}$

Based on Statement 4 and A13, by the message-meaning rule,

$Statement\ 5 : MME \mid\equiv OBU \mid\sim \langle B \rangle$

Based on Statement 5 and A4, by the freshness verification rule,

$Statement\ 6 : MME \mid\equiv OBU \mid\equiv \langle B \rangle$

Based on m_3,

$Statement\ 7 : VE \triangleleft \langle A, B, VE \overset{dB}{\longleftrightarrow} eNodeB \rangle_{h(ID_{VE} \| y)}$

Based on Statement 7 and A10, by the message-meaning rule,

$Statement\ 8 : OBU \mid\equiv MME \mid\sim \langle A, B, OBU \overset{dB}{\longleftrightarrow} eNodeB \rangle$

Based on Statement 8 and A1, by the fresh value validation and freshness verification rules,

$Statement\ 9 : OBU \mid\equiv MME \mid\equiv \langle A, B, OBU \overset{db}{\longleftrightarrow} eNodeB \rangle$

Based on Statement 9 and A5, by the control rule,

$Statement\ 10 : OBU \mid\equiv \langle OBU \overset{dB}{\longleftrightarrow} eNodeB \rangle$

Based on SK=h(adB)=h(abdP),

$Statement\ 11 : OBU \mid\equiv \langle OBU \overset{SK}{\longleftrightarrow} eNodeB \rangle$ **(Goal 1)**

Based on m_4,

$Statement\ 12 : eNodeB \triangleleft \langle A, B, OBU \overset{dA}{\longleftrightarrow} eNodeB \rangle_{S_{MME}}$

Based on Statement 12 and A12, by the message-meaning rule,

$Statement\ 13 : eNodeB \mid\equiv MME \mid\sim \langle A, B, VE \overset{dA}{\longleftrightarrow} eNodeB \rangle$

Based on Statement 13 and A2, by the fresh value validation and freshness verification rules,

$Statement\ 14 : eNodeB \mid\equiv MME \mid\equiv \langle A, B, OBU \overset{dA}{\longleftrightarrow} eNodeB \rangle$

Based on Statement 14 and A6, by the control rule,

$Statement\ 15 : eNodeB \mid\equiv \langle OBU \overset{dA}{\longleftrightarrow} eNodeB \rangle$

Based on SK=h(bdA)=h(abdP),

$Statement\ 16 : eNodeB \mid\equiv \langle OBU \overset{SK}{\longleftrightarrow} eNodeB \rangle$ **(Goal 2)**

Based on m_5,

$$Statement\ 17: OBU \lhd \langle A, B, VE \overset{SK}{\longleftrightarrow} eNodeB\rangle_{SK}$$

Based on Statement 17, by the message-meaning rule,

$$Statement\ 18: OBU|\equiv eNodeB|\sim\langle A, B, OBU \overset{SK}{\longleftrightarrow} eNodeB\rangle$$

Based on Statement 18 and A1, by the fresh value validation and freshness verification rules,

$$Statement\ 19: OBU|\equiv eNodeB|\equiv\langle A, B, OBU \overset{SK}{\longleftrightarrow} eNodeB\rangle$$

Based on Statement 19,

$$Statement\ 20: OBU|\equiv eNodeB|\equiv\langle OBU \overset{SK}{\longleftrightarrow} eNodeB\rangle$$ **(Goal 3)**

Based on m_6,

$$Statement\ 21: eNodeB \lhd \langle A,B, OBU \overset{SK}{\longleftrightarrow} eNodeB\rangle_{SK}$$

Based on Statement 21, by the message-meaning rule,

$$Statement\ 22: eNodeB|\equiv OBU|\sim\langle A, B, OBU \overset{SK}{\longleftrightarrow} eNodeB\rangle$$

Based on Statement 22 and A2, by the fresh value validation and freshness verification rules,

$$Statement\ 23: eNodeB|\equiv OBU|\equiv\langle A, B, OBU \overset{SK}{\longleftrightarrow} eNodeB\rangle$$

Based on Statement 23,

$$Statement\ 24: eNodeB|\equiv OBU|\equiv\langle OBU \overset{SK}{\longleftrightarrow} eNodeB\rangle$$ **(Goal 4)**

By the logic presentation and derivation, we can obtain Goals 1–4, which show that the ARHAP scheme can realize the mutual authentication and session key agreement between the OBU and the eNodeB.

4.2. Security Analysis. In this section, we analyze the security functions of the ARHAP scheme to explain that it can resist some malicious attacks such as replay attacks, man-in-the-middle attacks, and secrecy attacks.

Proposition 4. *The ARHAP scheme can make the OBU anonymity.*

Proof. By the ARHAP scheme, the OBU sends the access request message $\{A, DID_{OBU}, C, V_1, ID_{MME}\}$ to the eNodeB, while the real identity ID_{OBU} of the OBU is protected by $DID_{OBU} = ID_{OBU} \oplus h(aC)$. Based on the computational discrete logarithm (CDL) problem, any attacker cannot obtain the random number a from A, and cannot retrieve ID_{OBU} from DID_{OBU}. In addition, due to the randomness of the parameter a, the access request, i.e., A, DID_{OBU}, V_1, sent by the OBU can be dynamically changed. It can avoid the attacker tracing the moving history and the current location of the OBU. Therefore, the ARHAP scheme can make the OBU anonymity. □

Proposition 5. *The ARHAP scheme can provide a mutual authentication and withstand attacks.*

Proof. The OBU, the eNodeB, and the MME should authenticate each other. It requires that the ARHAP scheme provides a mutual authentication mechanism between any two of them.

The ARHAP scheme is able to provide authentication of the eNodeB and the MME to the OBU. Thus, the attacker cannot impersonate the OBU to cheat the eNodeB and the MME. By the scheme, the MME authenticates the OBU by verifying $V_1{}^* = h(h(ID_{OBU}\|y)\|R_{AC}\|ID_{MME})$ with the received $V1 = h(N\|R_{AC}\|ID_{MME})$. As the attacker cannot possess the OBU's password, PW_{OBU}, it cannot compute the correct $N = Q \oplus h(PW_{OBU}\|x_{OBU})$ and cannot cheat the MME by forging a request message. Due to the one-time random number a, the request message sent by the OBU is dynamically changed in each moment. Thus, the attacker cannot cheat the MME by replaying a previous request message. Besides, when an OBU gets into the LTE-A network, the authentication of the eNodeB to the OBU is completely dependent on the authentication of the MME to the OBU. Therefore, the attacker cannot cheat MME and eNodeB by masquerading as OBU.

The ARHAP scheme can withstand the attacker impersonate eNodeB to cheat OBU and MME. In our scheme, the MME authenticates eNodeB by verifying the computed $V_2 = E_{SeNodeB}\{h(A,B,Cert_{eNodeB}, V_1, DID_{OBU})\}$, as the attacker cannot know eNodeB's private key S_{eNodeB} and compute the correct eNodeB's digital signature V_2. It cannot cheat MME by masquerading as eNodeB. Besides, the authentication of the OBU to the eNodeB is completely dependent on the authentication of the MME to the eNodeB. Thus, attacker cannot perform an authentication from the MME and the OBU. Therefore, the attacker cannot cheat the MME and the OBU by masquerading as an eNodeB.

The ARHAP scheme can withstand the attacker impersonating the MME to cheat the OBU and the eNodeB. By the proposed scheme, the eNodeB authenticates the MME by verifying the value of $V_3 = E_{SMME}\{h(ID_{eNB}, G_{OBU}, Cert_{eNodeB}, dA, A, B, D, W_1)\}$ because the attacker cannot know the private key S_{MME} of the MME to compute the correct digital signature V_3. It cannot cheat the eNodeB by masquerading as the MME. Besides, the OBU computes $W_1 = h(h(ID_{OBU}\|y)\|dB\|A\|D\|ID_{eNodeB}\|ID_{MME})$ and $W_1{}^* = h(N\|dB\|A\|D\|ID_{eNodeB}\|ID_{MME})$ to verify the eNodeB. The attacker cannot acquire ID_{OBU} and y; it cannot forge W_1 to get the authentication from the OBU. Therefore, the attacker cannot cheat the eNodeB and the OBU by masquerading as the MME. □

Proposition 6. *The ARHAP scheme is able to provide forward/backward secrecy.*

Proof. Forward/backward security means that an attacker cannot derive the current session key from the previous generated session key. By the proposed scheme, the session key SK's parameters are generated from the OBU, the eNodeB, and the HSS. They hold random parameters *a, b, d.* Due to the difficulty of the elliptic curve discrete logarithm

problem (ECDL) and the computational problem (CDH), the attacker cannot retrieve the correct values of *a, b, d,* according to $A=aP$, $B=bP$, $D=dP$, $R_{AC}= aC= cA$, and $R_{BC}= bC= cB$. In addition, since the 2 certifications before and after are not related, the proposed scheme can achieve perfect forward/backward secrecy. □

Proposition 7. *The ARHAP scheme can provide a local password authentication without a verification table.*

Proof. In the vehicles, an OBU can get *ID* and *PW* into the terminal to calculate H^*. Then it can verify whether $H^*=H$. If the validation fails, the smart card will interrupt the conversation. Therefore, the proposed scheme, by the use of a smart card to realize a local password authentication, can effectively avoid unauthorized access. By the proposed scheme, it is obvious that the OBU, the eNodeB, and the MME will not maintain any verification table. There is no verification table used by the proposed scheme. □

Proposition 8. *The ARHAP scheme can achieve privacy protection.*

Proof. By the proposed scheme, in the registration phase, the OBU uses public key Y to encrypt the real identity for the transmission. Only the MME private key can be used to decrypt x. In the handover process, a temporary identity instead of the real identity is used because only the safe entity MME knows R_i. The attacker cannot deduce the true identity of the OBU from the temporary identity IMSI, due to the random number of R_i of the OBU, which is used to process a different unrelated temporary identity. Therefore, the attacker cannot track the OBU path for each OBU handover.

Under emergency conditions, if the OBU misconducts violated the law that damages the VANET, the MME security entities will provide the true identity of the OBU to allow arbitration by law enforcement, according to the nature of the specific situation or operation. Then the MME can obtain the user's real identity IMSI by calculation. □

Proposition 9. *The ARHAP scheme can withstand a replay attack.*

Proof. A replay attack before a legitimate access request $\{A, DID_{OBU}, C, V_1\}$ to the eNodeB will finally receive the message $\{G_{OBU}, W_4\}$. According to the CDLP problem, the attacker cannot compute $A=aP$ as a random number of A, and the attacker cannot calculate the session key $SK=(adB)$. Hence, the proposed scheme can withstand a replay attack. □

4.3. Formal Verification. To ensure that our proposed scheme can resist malicious attacks, with the design of the security goals in mind, we use a formal verification tool of AVISPA for the formal verification of the proposed scheme.

The AVISPA works following a complete set of model checking technologies. It is a standard automatic formal analysis tools. The AVISPA takes the high-level protocol specification language (HLPSL) as the description tool. By the HLPS2IF translator, it converts the description of the proposed scheme by the HLPSL into an intermediate format

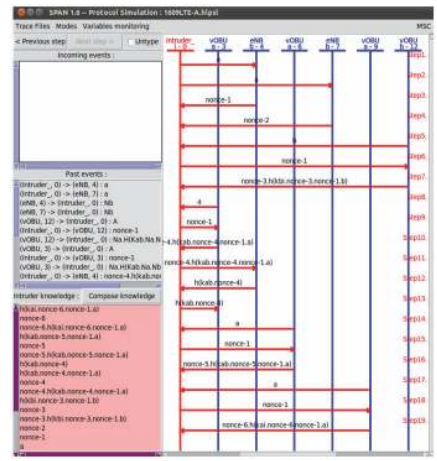

Figure 5: Simulation of intruder attacks.

(IF), and then its model detector is used to verify the security functions. The AVISPA has four security analysis terminals: the On-the-Fly Model Checker (OFMC), the Constraint-Logic-Based Attack Searcher (CLAtSe), the SAT-Based Model Checker (SATMC), and Tree Automata based on Automatic Approximations for the Analysis of Security (TA4SP). The four security analysis terminals have different underlying principles and focuses. If a protocol can reach the expected security goals, the results of the security analysis and the corresponding data will be presented. If the scheme is verified to be unsafe, the terminal will show that it is the unrealized expected safety goal. To formally verify the security functionality of the proposed ARHAP protocol in a LTE/LTE-A based VANET, we use AVISPA to model and verify it.

The ARHAP scheme works for the authentication in the handover procedure from the service eNodeB to the target eNodeB. It is possible for AVISPA to simulate intruders who can receive and send messages from their knowledge. In the HLPSL, an intruder is named *i*, and its initial knowledge is explicitly defined in the specification as the intruder knowledge={...}). In the process of the execution of the ARHAP, the HLPSL is used to describe the basic roles of the OUB and the eNodeB. The result of a simulated intruder attack is shown in Figure 5. We simulate three intruders attacking the execution of our scheme. The first intruder, who can receive all messages, stores them in a knowledge base. Then, it decrypts the information as if it has the key and builds new messages and sends them to any other eNodeBs. The second intruder, named *i*, replay an attack before a legitimate access request to the eNodeB. The third intruder is using a temporary identity instead of a real identity, disguised as an OBU to session with eNodeB. By the simulation of intruder attacks, we can know that the ARHAP scheme is secured.

The HLPSL specification has been debugged, while it will be checked for the function of attack detection automatically by four checkers in the system. If the proposed protocol is safe, the checking result will report SAFE in SUMMARY. In Figure 6, the test results show that the proposed handover authentication scheme is secure. We use the backend OFMC

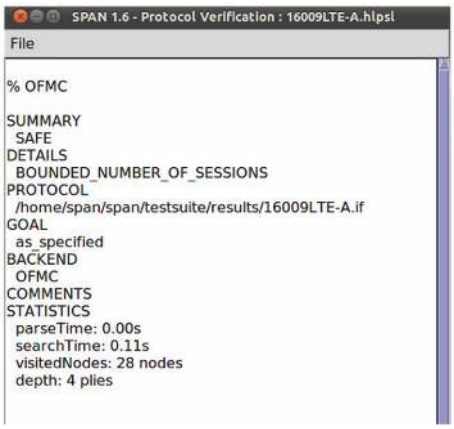

Figure 6: Results reported by the OFMC backend.

for falsification and verification for a bounded number of sessions. We present the safety goal as the confidentiality of the key and the random numbers. The validation of the OBU and the eNodeB is performed by a hash-chain value used for rapid certification. From the presented results, we can conclude that the proposed scheme can successfully implement the anonymity of the OBU, provide mutual authentication, withstand various attacks, and resist other malicious attacks such as replay attacks, Man-in-the-Middle attacks, and secrecy attacks.

4.4. Functionality Comparison. It is obvious from Table 2 that our scheme has many excellent features and is more secure than other similar authentication schemes. The OBU can resist various types of security attacks and achieve anonymity when the vehicle is in a VANET-based LTE-A network. The ARHAP scheme needs relatively few communications and has low computational cost.

5. Performance Evaluation

In this section, we compare the performance of our proposed scheme with several existing schemes. The architecture of the VANET is the same as the one discussed in Section 2, which is the LTE/LTE-A based VANET. Computational and communication overheads are two very important performance indicators. In this analysis, we are mainly considering the computational and communication costs of the ARHAP scheme. To obtain the quantitative results, we have conducted various sets of simulations and compare the ARHAP scheme with several other typical handover authentication protocols. The network environment has almost no difference so that the experimental data from all protocols under the examination can be compared on the same basis.

5.1. Computational Overhead. The system configuration of each OBU is as follows. We computed the execution time of the above cryptographic operations using MIRACL. It is a famous cryptographic operations library and has been widely used to implement cryptographic operations in many environments. Each OBU has a basic frequency of 3 GHz, 64-bit Intel E5-1607 processor with the memory of 7.8 GB. The operations of the OBUs and the eNodeB are modeled by using MATLAB R2014b software. Based on the models, the performance evaluation is conducted. The simulation environment is established with the following parameters. The distance between the service eNodeB and the target eNodeB is 300 m. The distance between the MME and the eNodeB is 10 km. The cryptographic algorithms employed in the simulation are hash function SHA-256, symmetric encryption AES-128, and ECDSA-160. The parameter settings and their values are listed in Table 3. The computational complexity of delay in two components: (1) the mutual authentication and key agreement and (2) handover authentication. It refers to the time required by network unit to process data including data encryption and the time needed to generate the key. Obviously processing delays are heavily dependent on the processing scheme and computational complexity.

The computational cost refers to the time taken by the cryptographic operations in the handover process and the cryptograph computing time. The LTE [26] standard is being expanded by many schemes. Computational cost is an important measure involved in the handover time delay. In the handover process, computational cost mainly includes hash operation time, symmetric/decryption operation time, point scalar multiplication operation time, and linear operation time. Those encryption algorithms generally always have lower overheads. In Table 4, we summarize the computational costs incurred by the ARHAP scheme and by the schemes appeared in [7, 15, 26].

Although our ARHAP scheme has been proved to be safe against various types of attacks tested, other types of malicious attacks, as well as unknown types of attacks that cannot be predicted, may interrupt the execution of the protocol during the authentication and key establishment phases. Therefore, it is assumed that any type of an attack may randomly occur at any step of the protocol execution during the authentication and key establishment phases. The ARHAP scheme cannot proceed if an attack successfully interrupts its execution. With an increasing number of successful attacks, the average total time delay for a successful execution of the protocol will be longer. The comparison of the average total time delay of the tested protocols is shown in Figure 7. The number of executions of the authentication processes is 10000. And in one execution of the process, it is assumed that there will be one attack to appear on average. It is shown that the ARHAP scheme has lower computational overhead than that of the other schemes [7, 15, 26]. Assuming that the probability of successful attacks is 50%, the figure reveals that the average total time delay incurred by SEAA [7] scheme or the HashHand [15] scheme is higher, while the delay incurred by the ARHAP scheme is obviously lower.

5.2. Communications Overhead. The communications cost is the time taken for the message exchanges in the authentication processes for the handovers. In the process of the handover authentication, the communication goes mainly between the OBU and the eNodeB, between the eNodeB and the MME, and between the service eNodeB and the target eNodeB. In Table 5, we compare the communication

Table 2: Functionality comparison between the ARHAP scheme and others.

	ARHAP	SEAA [7]	ASUA [12]	NAPP [13]	ESAA [14]	HashHand [15]	Nframe [23]
User anonymity	Yes	Yes	No	Yes	No	Yes	Yes
Mutual authentication	Yes	Yes	Yes	Yes	No	Yes	Yes
Against impersonation attack	Yes	Yes	Yes	Yes	No	Yes	Yes
Resists eNodeB impersonation attack	Yes	No	Yes	Yes	No	Yes	Yes
Resists MME impersonation attack	Yes	No	Yes	Yes	No	Yes	Yes
Resists replay attack	Yes	Yes	Yes	No	No	Yes	Yes
Resists perfect forward attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Resists perfect backward attack	Yes	No	No	No	No	Yes	Yes
Resists offline password-guessing attack	Yes	Yes	Yes	Yes	No	Yes	Yes
Resists insider attack	Yes	Yes	Yes	Yes	No	Yes	Yes
No verification table	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local password verification	Yes	Yes	Yes	No	No	No	No
Correct password change	Yes	Yes	Yes	Yes	No	No	No

Table 3: Parameter settings.

Parameters	Value (bits)
xP	1024
$g^x \bmod p$	1024
Identity ID_x	160
Random number	128
Hash function h(x)	160
Encryption/decryption	1024

Table 4: Computational cost notations.

Notation	Meaning
T_H	Hash operation time
T_S	Symmetric/decryption operation time
T_M	Point scalar multiplication operation time
T_P	Linear operation time

Table 5: Comparison of communication costs.

Scheme	Communication (bits)
SEAA [7]	3808
HashHand [15]	4480
LTE [26]	8350
ARHAP	3552

costs of the ARHAP and those of other schemes. The results show that a vehicular network requires high frequency of communication between the OBU and the MME. The two schemes of SEAA [7] and HashHand [15] require more time for the handshaking communications, while the communication cost of the ARHAP scheme is concentrated on the short distance between the OBU and the eNodeB. On the whole, it can meet the requirements of the communication costs of the OBU in a vehicle with limited resource.

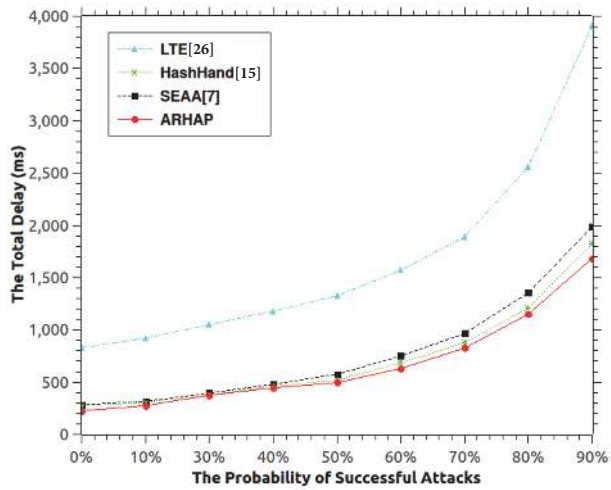

Figure 7: Total computational overhead of tested protocols.

As shown in Figure 8, the total transmission overhead of the ARHAP scheme is significantly lower than that of LTE standard [26]. The communications overheads of all the authentication schemes grow linearly with the increase of the probability of successful attacks. After a successful attack with 50% probability is reached, by the SEAA in [7], the communications overhead only slightly exceeds that of the HashHand's [15]. Each of the schemes has a larger overhead when the probability of successful attacks exceeds 60%.

5.3. Comparison of Handover Processes. In Table 6, we compare the total operation time required for the handover processes between the proposed scheme and other existing schemes. Since the standard LTE [26] only has a hash operation, it is computationally fast lacking the requisite security and anonymity. LTE [26] is very vulnerable to the replay, man-in-the-middle, and secrecy attacks. Between the OBU and the eNodeB, the SEAA scheme mainly uses

Table 6: Comparison of the duration of handover processes.

Scheme	OBU	eNodeB
SEAA [7]	$6T_H+0T_S+3T_M+0T_P$	$5T_H+4T_S+5T_M+0T_P$
HashHand [15]	$5T_H+2T_S+T_M+3T_P$	$5T_H+3T_S+T_M+2T_P$
LTE [26]	$4T_H+0T_S+0T_M+0T_P$	$2T_H+0T_S+0T_M+0T_P$
ARHAP	$2T_H+2T_S+3T_M+T_P$	$3T_H+T_S+2T_M+T_P$

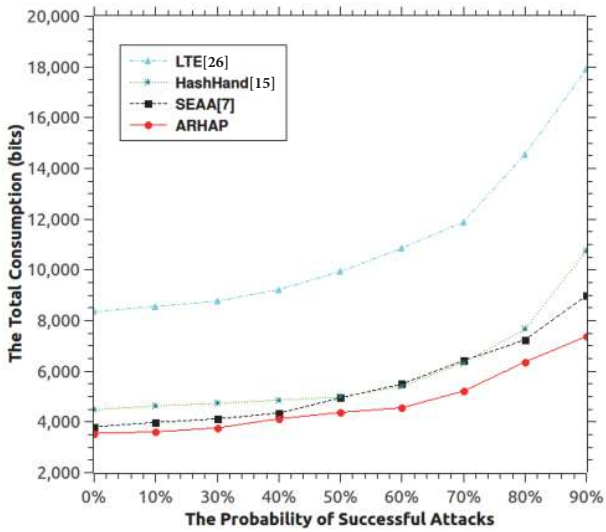

Figure 8: Total communications overhead of protocols.

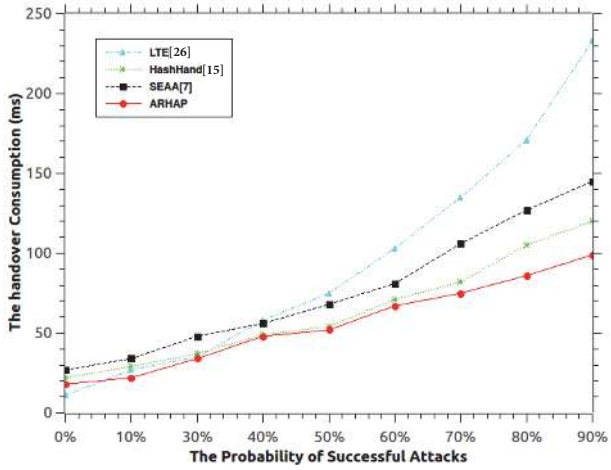

Figure 9: Handover time consumption of an OBU.

hash operation and point scalar multiplication operation, which need to increase computational ability for the OBU. The HashHand [15] improves the security functionality with efficiency. But it needs more linear and symmetric/decryption operations. The ARHAP scheme uses a hash calculation, so that the lower handover time inherent in the hash functions reduces the computational overhead in the overall certification process.

The operations of the OBUs and the eNodeB are modeled using MATLAB R2014b software. The computational cost is modeled as an unknown function (UF), which can be got from the equation $UF= r_1T_H+ r_2T_S+ r_3T_M+ r_4T_P+r_5$, in which. r_1, r_2, r_3 r_4, and r_5 are random numbers. Meanwhile, the T_H, T_S, T_M, and T_P are all called unknown functions for testing. The computing process of UF is as follows. Firstly, one number from the set [r_1, r_2, r_3, r_4, r_5] is generated randomly, and the other numbers are set to the fixed value as 1. Secondly, two numbers from the set [r_1, r_2, r_3, r_4, r_5] are generated randomly, and the other numbers are 1. This process will continue until all the numbers in the set [r r_1, r_2, r_3, r_4, r_5] are generated randomly. Since more numbers in the set [r_1, r_2, r_3, r_4, r_5] are generated randomly, the higher probability of successful attacks can be obtained. At the same time, the corresponding complexity and the value of UF will be also increased. Figures 9 and 10 complement the information in Table 6. It is obvious that from 0% to 50% of the probability of successful attacks, the time consumption for the handover between the OBU and the eNodeB incurred by the ARHAP scheme is obviously less than that for the SEAA [7] and the HashHand [15] schemes. And it is a little bit higher than that for the LTE [26]. Due to the limited bandwidth available in various new mobile networks (e.g., body area sensor networks, BSNs, and vehicle-to-grid networks), minimal communication overhead is required for any deployed security solution. HashHand [15] provides a key update mechanism. It is very similar with ARHAP. We find that from 50% to 90% of the probability of successful attacks the computational cost of the modular operation is still high. However, ARHAP has included the password verification, which has improved anonymity, security, and efficiency. A slight increase in overhead is justifiable. It is clear that a reliable authentication scheme design should adopt suitable cryptographic operations with less computational overhead in order to achieve better performance and efficiency.

6. Conclusions

In this paper, we have proposed an anonymous handover authentication scheme for the LTE-A based VAVETs. Based on the technique of the ECC, the proposed scheme can successfully achieve the security requirements including the anonymous handover and the secure key agreement, privacy preserving, and the ability to resist various malicious attacks. By using BAN logic, we have proved that the ARHAP scheme can meet the security requirements in the handover processes in the VANETs. Furthermore, the ARHAP scheme is proved to correctly realize a mutual authentication between an OBU and a target eNodeB in the handover process with the ability against various malicious attacks. Compared with other

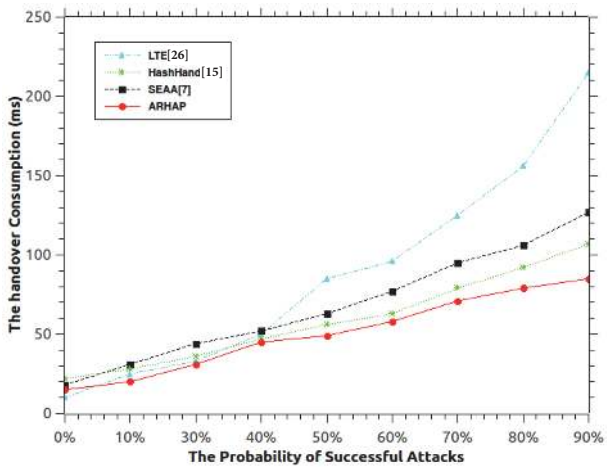

Figure 10: Handover time consumption of eNodeB.

existing authentication schemes, the ARHAP scheme has a much better performance and can be applied to LTE/LTE-A based VAVETs. We conclude that the proposed protocol can efficiently reduce the computational and communication costs.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by Joint Funds of National Natural Science Foundation of China and Xinjiang under Grant U1603261, in part by the State Key Program of National Natural Science Foundation of China under Grant 91420202, and in part by the Project of High-level Teachers in Beijing Municipal Universities in the period of the 13th five-year plan under Grant IDHT20170511.

References

[1] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: a review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[2] Y. Qiu, M. Ma, and X. Wang, "A proxy signature-based handover authentication scheme for LTE wireless networks," *Journal of Network and Computer Applications*, vol. 83, pp. 63–71, 2017.

[3] J. Zhou, M. Ma, Y. Feng, and T. N. Nguyen, "A symmetric key-based pre-authentication protocol for secure handover in mobile WiMAX networks," *The Journal of Supercomputing*, vol. 72, no. 7, pp. 2734–2751, 2016.

[4] Z. Hameed Mir and F. Filali, "LTE and IEEE 802.11p for vehicular networking: a performance evaluation," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1–15, 2014.

[5] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," *IEEE Communications Magazine*, vol. 51, no. 5, pp. 148–157, 2013.

[6] 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.

[7] D. Zhao, H. Peng, L. Li, and Y. Yang, "A secure and effective anonymous authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 78, no. 1, pp. 247–269, 2014.

[8] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks*, vol. 57, no. 17, pp. 3492–3510, 2013.

[9] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 2, pp. 457–468, 2014.

[10] M. Taha, L. Parra, L. Garcia, and J. Lloret, "An Intelligent handover process algorithm in 5G networks: The use case of mobile cameras for environmental surveillance," in *Proceedings of the 2017 IEEE International Conference on Communications Workshops, ICC Workshops 2017*, pp. 840–844, Paris, France, May 2017.

[11] D. He, S. Chan, C. Chen, J. Bu, and R. Fan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," *Wireless Personal Communications*, vol. 61, no. 2, pp. 465–476, 2011.

[12] D.-J. He, M.-D. Ma, Y. Zhang, C. Chen, and J.-J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Computer Communications*, vol. 34, no. 3, pp. 367–374, 2011.

[13] C.-T. Li and C.-C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 35–44, 2012.

[14] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 214–222, 2012.

[15] D. He, S. Chan, and M. Guizani, "Handover authentication for mobile networks: Security and efficiency aspects," *IEEE Network*, vol. 29, no. 3, pp. 96–103, 2015.

[16] M. Taha, J. M. Jimenez, A. Canovas, and J. Lloret, "Intelligent Algorithm for Enhancing MPEG-DASH QoE in eMBMS," *Network Protocols and Algorithms*, vol. 9, no. 3-4, p. 94, 2018.

[17] M. F. Feteiha and H. S. Hassanein, "Enabling cooperative relaying VANET clouds over LTE-A networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 4, pp. 1468–1479, 2015.

[18] 3GPP, "Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB) (Rel 11)," 3GPP TS 3GPP TS 22.220 V11.6.0, 3rd Generation Partnership Project, 2012.

[19] 3GPP, "Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks (Rel 11)," 3GPP TS 3GPP TS 24.302 V11.4.0, 3rd Generation Partnership Project, 2012.

[20] 3GPP, "Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC) (Rel 12)," 3GPP TS 3GPP TS 22.368 V12.0.0, 3rd Generation Partnership Project, 2012.

[21] C. Wang, M. Ma, and L. Zhang, "An Efficient EAP-Based Pre-Authentication for Inter-WRAN Handover in TV White Space," *IEEE Access*, vol. 5, pp. 9785–9796, 2017.

[22] A. Vinel, "3GPP LTE versus IEEE 802.11p/WAVE: which technology is able to support cooperative vehicular safety applications?" *IEEE Wireless Communications Letters*, vol. 1, no. 2, pp. 125–128, 2012.

[23] A. Fu, N. Qin, Y. Wang, Q. Li, and G. Zhang, "Nframe: A privacy-preserving with non-frameability handover authentication protocol based on (t, n) secret sharing for LTE/LTE-A networks," *Wireless Networks*, vol. 23, no. 7, pp. 2165–2176, 2017.

[24] M. Cohen and M. Dam, "Logical Omniscience in the Semantics of BAN Logic," in *Proceedings of the Foundations of Computer Security Workshop*, pp. 121–132, 2003.

[25] J. Liu, Q. Li, R. Yan, and R. Sun, "Efficient authenticated key exchange protocols for wireless body area networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, pp. 1–11, 2015.

[26] 3GPP, "Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Rel 12)," 3GPP TS 3GPP TS 33.401 V12.10.0, 3rd Generation Partnership Project, 2013.