A Relay-assisted Secure Handover Mechanism for High-speed Trains

Yue Zhao[1*], Bo Tian[1], Zhouguo Chen[1], Jin Yang[2] and Saifei Li[3]
[1] Science and Technology on Communication Security Laboratory
Chengdu, 610041 - China
[2] College of Cyber Security, Sichuan University
Chengdu, 610065 - China
[3] The School of Information Science and Technology, Southwest Jiaotong University
Chengdu, 611756 - China
[e-mail: yuezhao@foxmail.com, tb_30wish@163.com, czgexcel@163.com, 253960818@qq.com, 20072172@163.com]
*Corresponding author: Yue Zhao

Received July 7, 2018; revised August 27, 2018; accepted September 12, 2018; published February 28, 2019

Abstract

Considering that the existing Long Term Evolution is not suitable for the fast and frequent handovers of high-speed trains, this paper proposes a relay-assisted handover mechanism to solve the problems of long handover authentication time and vulnerable to security attacks. It can achieve mutual authentication for train-ground wireless communication, and data transmission is consistent with one-time pad at the same time. The security analysis, efficiency analysis and simulation results show that the proposed mechanism not only realizes the forward security and resists many common attacks, but also effectively reduces the computational overhead of train antenna during the secure handover process. When the running speed of a train is lower than 500km/h, the handover delay is generally lower than 50ms and the handover outage probability is less than 1.8%. When the running speed of a train is 350km/h, the throughput is higher than 16.4mbps in the process of handover. Therefore, the secure handover mechanism can improve the handover performance of high-speed trains.

Keywords: High-speed trains, Secure handover, Mutual authentication, Signcryption scheme, One-time pad

This research was Supported by the Applied Basic Research Project of Sichuan Province (No. 2017JY0030) and the Fundamental Research Funds for the Central Universities (No.YJ201727).

http://doi.org/10.3837/tiis.2019.02.006 **ISSN : 1976-7277**

1. Introduction

At present, Global System for Mobile Communications-Railway (GSM-R) and broadband IP wireless mobile communication (802.11 series standards) are mainly used in the bidirectional train-ground communication of high-speed trains [1]. With the commercialization of Long Term Evolution (LTE), the LTE-R (LTE-Railway) is becoming a new standard for wireless communication between trains and ground, and it will meet the requirement of trains for the real-time communication during their high-speed running. In that process, the user equipments (UEs) on the train need to carry out mutual authentication with the evolved NodeBs (eNodeBs), and onlyafter the authentication passes, can the communication be carried out; meanwhile, the data transferred should be encrypted [2].

Centering on the LTE-R standard emerges a common concern---the fast and frequent handovers of high-speed trains. The eNodeBs are limited by their fixed position and transmission power, resulting in user equipments (UEs) on the train passing through a plurality of cells during the calling time. Trains is places where are. When the train which is always crowded with people passes through the overlapping area, all the UEs on it will generate group handovers at the same time. A large number of UEs sending handover requests will cause a signaling storm, leading to system congestion or even paralysis.

The existing solution is to collect the information of the users in the train with the train antenna, which interact with eNodeBs in the ground. The train antenna is used as a relay station (RS) to assist UEs in establishing communication with eNodeBs. For the downlink, the first hop is the link from eNodeBs to the RS in the high-speed train, and the second one is the link from the RS to UEs [3, 4]. All UEs in a train thus can be taken as a single UE who sends handover requests to eNodeB, which greatly reduces the signaling interaction load. However, when the train moves at high speed, RSs still generate fast and frequent handovers between multiple eNodeBs. Handover signaling messages remain threatened by attacks such as stealing, tampering, forgery, and replay as before. So it is necessary to design a smooth and seamless secure handover scheme to ensure that all the security attributes are met while minimizing the handover delay being minimized and the outage probability during the process of handover reduced.

In order to cope with the various security threats in the process of the high-speed train's handovers, it is necessary to set up some mechanisms to maintain handover security, especially the access authentication and key agreement. The access authentication is the first step of security protection, and the mutual authentication is indispensable between nodes and networks. The key agreement is a precondition to ensure the communication security in an open network environment. As the introduction of the security mechanism inevitably leads to a decline in handover performance, it is important to further study how to reduce the train handover delay and system overheads.

At present, the research on high-speed train handover focuses on the optimization of the inter-cells handover performance of high-speed trains, while the security needs are rarely considered. In [5], it is proposed to introduce the authentication, authorization and accounting (AAA) mechanism into mobile handovers, and realize the security of authentication and registration among nodes. However, AAA mechanism needs the support of the public key certificate and public key infrastructure, and the performance of high-speed train is thus not high in a fast moving scene. In [6], a fast access authentication based on identity signature (AAIS) mechanism for vehicular networks is proposed to support mutual authentication

between vehicles and networks. But the mechanism lacks effective protection for the confidentiality and integrity of signaling messages during the handover process. In [7], the IPSec mechanism is used for the wireless communication between trains and the ground to achieve the security protection of signaling and data transmission, while Internet key exchange (IKE) protocol is adopted to realize the security association. However, the IPSec mechanism does not support inter-domain handovers, and IKE must be completed by pre-shared key or public key certificate. Therefore, it is not suitable for fast handover, the main characteristic of the high-speed trains.

In the past two years, in addition to the research on the secure handover mechanism for high-speed trains, there are some new research advances in the field of train-ground communication security enhancement. An improved protocol based on proxy signature and elliptic curve cryptography is proposed in [8], aiming at solving the problems of identity leakage, node spoofing, and denial of service (DoS) attacks in access authentication protocol of communication-based train control system. Concentrating on wide security management, multiple access points and difficult signal coverage in the running process of trains, [9] gives some solutions such as the wanring data acquisition, fusion as well as decision, designs and implements of the rail transmit security monitoring and early warning system. [10] presents a novel strategy for visual tracking based on cloud platform in intelligent surveillance systems. The above technical methods have certain reference significance for us to study the fast and secure handover of high-speed trains.

Due to the stability of the deployment topology of eNodeBs and the routes of trains, it is possible to identify in advance the target eNodeB that RS will access, so it is expected to reduce the delay caused by the processing overhead of security mechanism during the handover process. According to the typical scenario of a high-speed train's handovers, this paper designs a secure handover based on pre-authentication (SHPA) mechanism, which combines the mutual authentication and session key agreement mechanism into the handover process. The security analysis and simulations show that the proposed handover mechanism not only has high security, but also effectively reduces the handover delay and outage probability, while maintaining a more stable throughput, significantly improving the wireless communication handover performance. The remainder of this paper is organized as follows: section 2 introduces the RS based wireless communication model and the idea about its fast handover; section 3 presents the SHPA mechanism as well as its implementation process to realize the mutual authentication and the key agreement between high-speed trains and the target eNodeB; section 4 analyzes the security and computational efficiency of SHPA mechanism; section 5 describes the simulation environment, and carries out handover performance analysis, while section 6 concludes this paper.

2. System Model

The model of the wireless communication between an eNodeB and UEs as well as a RS is shown in **Fig. 1**. When on or near the train, the UEs switch from eNodeB to the RS at the top of the train, and then will connect to eNodeB through RS. The eNodeB sends affiliation update messages to a mobility management entity (MME) [11, 12]. The MME is the key control-node for the LTE access-network. It is responsible for authenticating the user by interacting with the eNodeB. Since the UE is connected with the RS before it is connected with the eNodeB, the eNodeB has the UE certificate, and the UE also has the eNodeB authentication and authorization information. Since the UE is connected with the RS before connected with eNodeB, the eNodeB has the UE's certificate, and the UE also gets the authentication and

authorization information of eNodeBs as well. In addition, RS, as an eNodeB user, needs to undertake a mutual authentication and a session key agreement with the eNodeB when accessing the network. The trust relationship is established via eNodeB to achieve indirect mutual authentication between UE and RS.

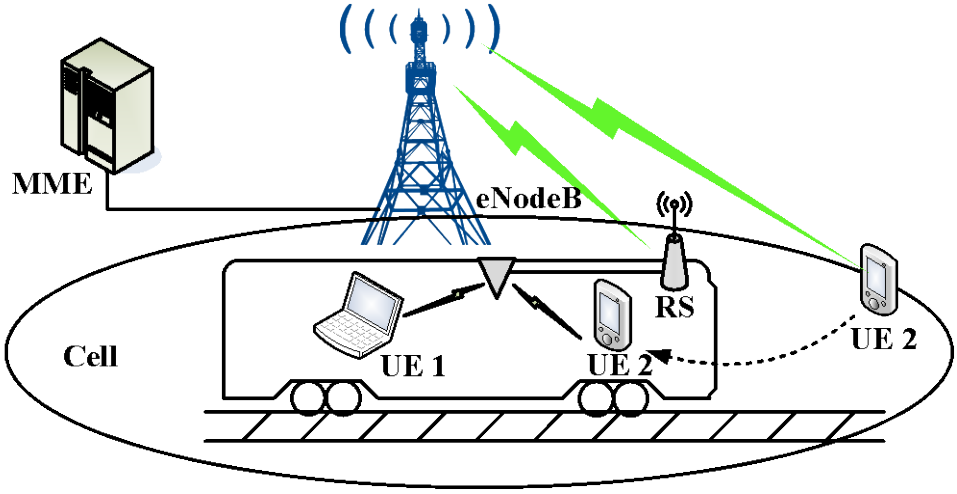

Fig. 1. The wireless communication model of UEs in the train

The above access authentication scheme is mainly to achieve mutual authentication among UE, RS and eNodeB. Because there is no direct trust relationship between UE and RS, eNodeB is required to transmit authentication information and achieve mutual trust. In addition, two different Diffie-Hellman key exchanges are required between UE and RS as well as between RS and BS to generate the shared key K_{RU} between RS and UE and the shared key K_{BR} between eNodeB and RS, respectively. The access authentication scheme includes the following steps of information exchange process.

Step 1. RS generates temporary private key y, temporary public key yP and random number R_{RS}, sends R_{RS}, yP, RS's certificate $Cert_{RS}$ and identity identification ID_{RS} to UE as an authentication activation message, and triggers the mutual authentication process with UE.

Step 2. When receiving the authentication activation message sent by RS, the UE generates the temporary private key x, the temporary public key xP, and the random number R_{UE}, and then calculates the authentication message $Auth_{UE}$ and the session key K_{RU} as

$$Auth_{UE} = Sig_{UE}(xP \,|\, yP \,|\, ID_{RS} \,|\, R_{UE} \,|\, R_{RS} | Cert_{UE} \,|\, Cert_{RS}) \quad (1),$$

$$K_{RU} = \text{HMAC-SHA 256}(xyP, ID_{UE} \,|\, ID_{RS} \,|\, R_{UE} \,|\, R_{RS}) \quad (2),$$

where ID_{UE} is the identity of UE and $Cert_{UE}$ is the certificate of UE. UE sends xP, ID_{UE} and $Auth_{UE}$ together as an access authentication request message to RS.

Step 3. After receiving the access authentication request message from UE, RS generates K_{RU} in the same way as does UE, and then constructs a certificate authentication message including R_{UE}, R_{RS}, $Cert_{UE}$, $Cert_{RS}$ and $Auth_{UE}$ to send to eNodeB.

Step 4. When eNodeB receives the certificate authentication message, it verifies $Cert_{UE}$ and $Cert_{RS}$ respectively, produces the corresponding verification results V_{UE} and V_{RS}, and then calculates the session key K_{BR} as

$$K_{BR} = \text{HMAC-SHA 256}(yzP, ID_{UE} \,|\, ID_{RS} \,|\, R_{UE} \,|\, R_{RS}) \quad (3),$$

where zP is the temporary public key of eNodeB. After that, eNodeB constructs certificate authentication response information sent to RS, including zP, R_{UE}, R_{RS}, V_{UE}, V_{RS}.

Step 5. RS obtains the certificate validation result V_{RS} after receiving the certificate authentication response message, then generates K_{BR} in the same way as eNodeB and calculates $Auth_{RS}$ as

$$Auth_{RS} = Sig_{RS}(zP \mid ID_{UE} \mid R_{UE} \mid R_{RS} \mid V_{UE} \mid V_{RS}) \quad (4).$$

RS sends $Auth_{RS}$ as an access authentication response message to UE. The security association between UE and RS is formally established.

A train moves, so do the UEs in the train. They therefore maintain the original security association and need no re-certification between them. The UEs getting off the train and on the platform establish new security associations with the eNodeB within the signal range. The key problem with a moving train is the secure handover between the RS and the eNodeB. Due to the regularity in the deployment of eNodeBs, it is possible to judge in advance that the RS will switch to the set of eNodeBs on the way. The train arrival and departure time, as well as the travel speed in each section are required to comply with the relevant provisions. Therefore, it is possible to determine the number of eNodeBs which the RS switches to in different time periods, according to the location and the direction of the train as well as the deployment topology of eNodeBs. In addition, before and after the RS swithes, the eNodeBs are generally located in adjacent positions and can communicate directly through the fiber optic cable.

As shown in **Fig. 2**, the RS on the train can periodically detect its coordinate position via the global positioning system. Assuming the position information (x_0, y_0) at time t_0, the position information (x_1, y_1) at time t_1, the moving direction vector of the RS according to the positions of two different times is represented as

$$\boldsymbol{V} = ((x_1 - x_0), (y_1 - y_0)) \quad (5).$$

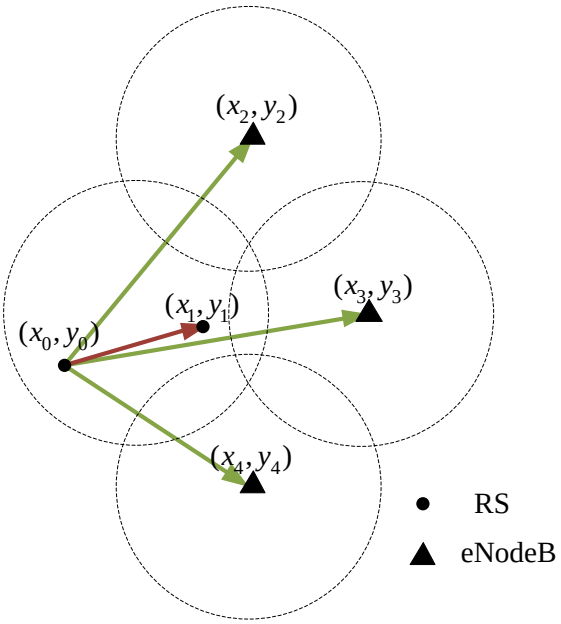

Fig. 2. The target eNodeB selection method based on the moving direction and position of a train

The moving direction vector from the original RS position (x_0, y_0) to the adjacent eNodeB j is expressed as

$$\boldsymbol{W}_j = ((x_j - x_0),(y_j - y_0)) \quad (6),$$

where (x_j, y_j) denotes the location information of each adjacent eNodeB j, j=2,3,4. If the angle between $\boldsymbol{W}_j$ and $\boldsymbol{V}$ of eNodeB i is minimum, i.e.

$$\delta_j = \arg\min_j \left(\arccos \frac{\boldsymbol{V} \cdot \boldsymbol{W}_j}{\left| \boldsymbol{V} \cdot \boldsymbol{W}_j \right|} \right) \quad (7),$$

the eNodeB j is selected as the target eNodeB for subsequent access. In light of the above-mentioned characteristics of the wireless communication between trains and the ground, the RS can communicate with the target eNodeB through the currently connected eNodeB so that the address configuration and the access authentication can be completed in advance. Thereby the RS can quickly switch to the target eNodeB, greatly reducing the handover delay caused by authentication and key agreement mechanisms and effectively improving the network performance when handovers occur. For high-speed trains, the demand for fast handover is particularly urgent. The time the high-speed trains spend in the overlapping area of two adjacent eNodeBs is quite short. In order to minimize the outage probability of the handover process and maintain a stable communication connection, it is necessary to optimize the handover process.

3. The Secure Handover Based on Pre-authentication Mechanism

The SHPA mechanism combines the authenticated key agreement protocol to achieve mutual authentication between RS and target eNodeB and generate shared session keys, thereby providing confidentiality protection for subsequent signaling messages or network traffic. The secure handover process during the train running is shown in **Fig. 3**. Before arriving at the coverage of the target eNodeB, the RS carries out address configuration via the current connection eNodeB, makes the mutual authentication with the target eNodeB, and negotiates the session key agreement at the same time. When entering the coverage area of the target eNodeB, the RS can immediately register the locations of both the RS and its connected UEs, and then performs the link layer handover to activate the new connections. The main procedures of the secure handover mechanism are described as follows.

Step 1. When a train with a RS is located in the coverage area of the eNodeB 1, it is determined that the RS is going to access the target eNodeB. When the RS receives the pilot signal intensity of eNodeB 2 higher than that of eNodeB 1, the RS begins to prepare pre-configuration and pre-authentication processes. The RS sends a handover preparation request message m_1 to eNodeB 1. The first part of m_1 includes the identity identification ID_{RS} of the RS, the new IP address IP_{RS} after the handover, and the IP address IP_2 of eNodeB 2. This part of the message is encrypted by the session key K_1 between RS and eNodeB 1. Then, the RS chooses an integer $\alpha \in \boldsymbol{Z}_q^*$, which is a multiplicative group consisting of q-1 non-zero elements on a finite field [13, 14]. The RS calculates $T_1=g^{\alpha}$ as the first half of the Diffie-Hellman handshake message, generating a random number R, and then obtains $H_{RS}(R)$ by SHA-256 operation on R. The RS performs signcryption operations on (IP_{RS}, g^{α}, R) with its

private key SK_{RS} and the public key PK_2 of eNodeB 2. Signcryption operations can accomplish both digital signature and public key encryption in one single step, and its computation and communication overheads are lower than those of the traditional signature-then-encryption approach. According to the authentication method of public keys, signcryption schemes can be classified as PKI-based signcryption, identity-based signcryption and certificateless signcryption. The PKI-based signcryption used in this paper is a classic signcryption scheme based on elliptic curve cryptography proposed by Zheng [15, 16]. This part of the message performed by signcryption is forwarded to eNodeB 2 via eNodeB 1 to request access authentication. Therefore, the message m_1 sent by RS to eNodeB 1 is represented as

$$m_1 = E_{K_1}(ID_{RS}, IP_{RS}, IP_2) \| SignCrypt_{SK_{RS}, PK_2}(IP_{RS}, g^{\alpha}, R) \quad (8).$$

Step 2. After receiving the handover preparation request message, eNodeB 1 decrypts the first part of message m_1 by the session key K_1, and matches ID_{RS} with the ID stored in the database to confirm the RS identity. If not match, the authentication fails. Otherwise, eNodeB 1 learns the new IP address of RS and sends the second part of the message to the eNodeB 2 through the optical fiber link.

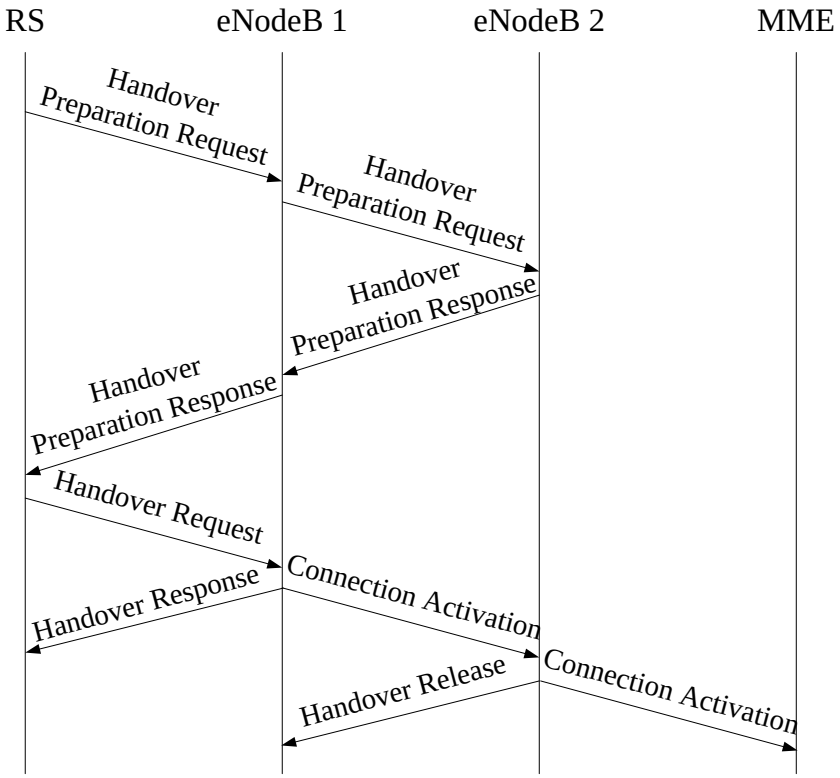

Fig. 3. The specific process of SHPA

Step 3. The eNodeB 2 receives the handover preparation request message of RS and performs a check operation by its private key SK_2 and the RS's public key PK_{RS} to obtain the second part of m_1. After the eNodeB 2 gets the new IP address of the RS, it performs duplicate address detection. If there already exists the same IP address, the RS is informed via eNodeB 1 to regenerate a new IP address for authentication. The eNodeB 2 also performs SHA-256

operation on R to get $H_2(R)$. The eNodeB 2 selects another integer $\beta \in \boldsymbol{Z}_q^*$, and calculates $T_2=g^{\beta}$ as the other half of the Diffie-Hellman handshake information. The session key is calculated as $K_2=g^{\alpha\beta}$, and K_2 is also operated on SHA-256 to obtain $H_2(K_2)$. The eNodeB 2 then uses its private key SK_2 and the RS's public key PK_{RS} to signcrypt（g^{β}, $H_2(K_2)$, $H_2(R)$）. The handover preparation response message m_2 that eNodeB 2 sends to RS via eNodeB 1 is expressed as

$$m_2 = SignCrypt_{SK_2, PK_{RS}}(g^{\beta}, H_2(K_2), H_2(R)) \quad (9).$$

Step 4. After receiving the handover preparation response message from eNodeB 1, RS uses its private key SK_{RS} and the public key PK_2 of eNodeB 2 to perform the check operation, and obtains $H_2(R)$, g^{β}, and $H_2(K_2)$. Comparing $H_2(R)$ with $H_{RS}(R)$, RS will reject the authentication request if they are not equal. Otherwise, RS calculates $K'=g^{\alpha\beta}$, and obtains $H_{RS}(K')$ by operating K' on SHA-256. RS verifies whether $H_{RS}(K')$ and $H_2(K_2)$ are equal. If equal, the session key agreement between RS and eNodeB 2 is completed. The session key K' (K_2) can be used to encrypt the subsequent signaling information.

Step 5. When a train enters the coverage area of eNodeB 2 from the coverage area of eNodeB 1, if the pilot strength of eNodeB 2 received by the RS is higher than that of eNodeB 1 by a threshold value, the RS will send a handover request message to eNodeB 1 to interrupt the wireless connection to eNodeB 1. The eNodeB 1 returns the handover response message after the handover request message is received. Both the two signaling messages are encrypted using K_1.

Step 6. The eNodeB 1 sends the connection activation message to eNodeB 2 to establish the communication connection to RS. The eNodeB 2 uses the handover release message to inform eNodeB 1 to release the previously occupied link resources, and forwards the connection activation message to the MME, including the RS's identity ID_{RS}, the RS's new affiliation, and the new IP address IP_{RS} after handover.

Step 7. After the above-mentioned handover is completed, each time when a new message is generated, the session key then gets updated as

$$\begin{cases} K_2^{(n+1)} = \text{HMAC-SHA 256}(K_2^{(n)}, \mathbf{0X01}) \\ K'^{(n+1)} = \text{HMAC-SHA 256}(K'^{(n)}, \mathbf{0X01}) \end{cases} \quad (10).$$

The new session key can be obtained from the hash computation on the original session key and an invariant constant. The secrecy of previously established session keys should not be affected even if the subsequent session keys are leaking. In this way, every message has a message number n correlating to the sending/receiving chains. $K_2^{(n)}$ and $K'^{(n)}$ represent the session key of the message number n on both sides of eNodeB 2 and RS. In the case of one-time pad, the following messages will be encrypted with the constantly updated session key K_2 (K') to realize the confidentiality protection of the messages between eNodeB 2 and RS.

4. Mechanism Analysis

4.1 Security Analysis

1. To realize the forward security. The SHPA mechanism can provide authentication and

one-time pad at the same time. It combines the authenticated key agreement protocol, uses elliptic curve digital signature, identity identification and SHA-256 encryption to achieve identity authentication, and obtains the shared key $K_2=K'=g^{\alpha\beta}$. The attackers cannot capture α and β from the message g^{α} and g^{β} in the key agreement process, either can they calculate $g^{\alpha\beta}$, unless they can overcome the difficult elliptic curve discrete logarithmic problem [17, 18]. Since the session key is only determined by the random number $g^{\alpha\beta}$, the security of the previously established session key will not be affected even if the private keys of RS and eNodeB 2 are leaked. Therefore, the SHPA mechanism has perfect forward security.

2. To resist node spoofing attacks. The authenticated key agreement protocol with signature mechanism can achieve mutual authentication. In addition, the eNodeB and the RS use their private keys to sign important parameters, key agreement messages and so on, in order to complete the identification of key agreement message and realize identity authentication. Even if the attackers fake RS or eNodeB identity and IP address to send messages, they are not able to forge signatures because they do not know the private keys of participants in both sides. Therefore, the SHPA mechanism can effectively prevent illegal users from performing forgery attacks.

3. To prevent denial-of-service attacks. Denial-of-service attack means that a large number of invalid authentication requests are sent by the attackers to trigger the receiver to perform frequent check operations based on elliptic curve cryptography, thus occupying the computing resources of the receiver. In the SHPA mechanism, the RS and eNodeB 2 establish a connection through eNodeB 1. The messages exchanged between the RS and eNodeB are encrypted by the session key. The eNodeB 1 forwards the successfully decrypted message only to the eNodeB 2 via the fiber link. Since not knowing the relevant information about the key, attackers cannot establish the session key with eNodeB 1 and eNodeB 2. Therefore, the eNodeB 2 can effectively verify the validity of the authentication request, decide whether to perform a check operation and prevent from denial-of-service attacks. Moreover, the traffic detection methods can defend against the denial-of-service attacks which occupy channel resources [19, 20]. It will not be described further in this paper.

4. To resist replay attacks. In the authentication messages, a random number is used as a challenge only once to prove the freshness of the message. Since the timeliness of the random number is expired, an attacker cannot initiate replay attacks even if intercepting the message, therefore cannot pass identity authentication.

4.2 Efficiency Analysis

Considering the difference of computing ability between RS and eNodeB, this paper mainly analyzes the RS's overheads in the secure handover process. To analyze difference in handover performance from two aspects of the calculation amount and the number of interactions, SHPA is compared with AAA, AAIS and IPSec presented in [5-7], respectively. The comparison results are shown in **Table 1**.

Table 1. Comparison of computational overheads of secure handover mechanisms

Handover Mechanisms	AAA	AAIS	IPSec	SHPA
Number of hash operations	4	2	2	2
Number of symmetric encryption / decryption	4	2	3	3
Number of modular exponential operations	2	2	2	2
Number of message interactions	5	3	4	2
Mutual authentication	4	5	6	4
Key agreement in advance	N	Y	Y	Y

According to the SHPA mechanism, the RS only performs two hash operations, two public key operations and two modular exponentiation operations. The computational overheads of SHPA mechanism are significantly smaller, in comparison with the AAA and IPSec mechanisms. Compared with AAIS mechanism, the SHAP mechanism adopts the elliptic curve cryptography for mutual authentication, ensures secure communication through one-time pad methodand and provides better security protection to the confidentiality and integrity of signaling messages.

5. Performance Evaluation

In the MATLAB simulation experiments, the secure handover performance of the high-speed train with a RS moving between eNodeBs are compared and analyzed in terms of SHPA, AAA, AAIS, and IPSec mechanisms. The system-level simulation parameters are shown in **Table 2**. The simulation parameters such as handover delay, throughput and outage probability are analyzed because they are the main factors, which affect the network performance.

Table 2. Simulation model and parameters of high-speed train secure handover

Parameter		Value
Antenna pattern		Onmi [21]
Channel bandwidth/MHz		10
Carrier frequency/GHz		2.4
eNodeB-eNodeB distance/m		5000
eNodeB-RS (Railway) distance/m		100
Propagation model		WINNER II D2a [22]
Standard deviation of shadowing（L_R/L_A）/dB		3.4/8
eNodeB	Transmission power/W	50
	Antenna height/m	32
	Noise figure/dB	5
RS	Transmission power /W	30
	Antenna height/m	5
	Noise figure/dB	7
UE	Antenna height/m	2
	Number of MSs per train	100
	Traffic rate	153.6kbps
Hash operation delay/ms [23]		2
Symmetric encryption or decryption delay/ms		3
Public key encryption or decryption delay/ms		8
Modular exponentiation operation delay/ms		5

Fig. 4 gives the simulation results of the handover delay of four kinds of secure handover mechanisms for high-speed trains at different running speeds. We can observe that the handover delay is generally lower than 50ms by adopting SHPA mechanism. When RS's mobile handover occurs, if some UEs on the train are in active voice communicating, the handover delay less than 50ms will not be obviously felt by human ears [24]. However, the handover delays of AAA and IPSec mechanisms are higher than 60ms, which may leads to a temporary interruption of voice communication. Although the computational overheads of the AAIS mechanism are lower than that of the SHPA mechanism, the handover delay is similar to the SHPA mechanism because it generates more message interactions. In addition, the handover delay increases along with the acceleration of the train speed. It is because higher

moving speed causes more serious Doppler effects [25], resulting in the deterioration of bit error rate performance and the delay of handover signaling transmission. Therefore, the high mobility has a certain impact on handover performance.

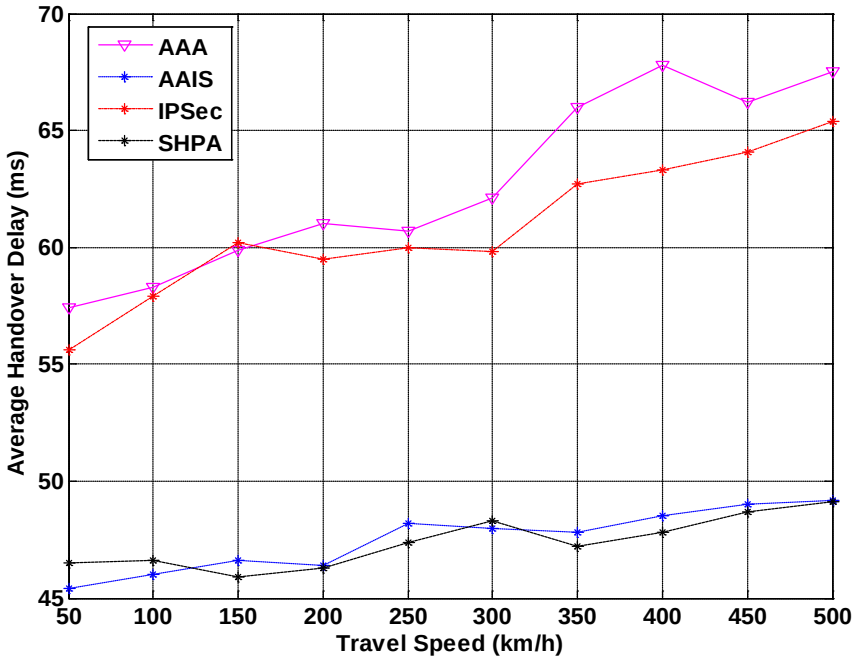

Fig. 4. Comparison of handover delay among four secure handover mechanisms

Fig. 5 shows the average throughput of the RS in a high-speed train when it is switched between two eNodeBs at a speed of 350km/h. The handover area where the differences in throughput among four kinds of secure handover mechanisms occur is about 2400-2600m from the eNodeB. It can be seen that when the RS's handover occurs, the throughput of the four mechanisms decline; especially when the distance between RS and eNodeB is 2520m, the throughputs reach the lowest value. It is because when high-speed trains meet the handover conditions, they usually have travelled a distance, so they are closer to the target eNodeB. The high mobility of train results in handover delay. As the train moves forward, the throughput will recover gradually and finally reach a same level among the four mechanisms. As the handover delay of SHPA mechanism is relatively small, the throughput decreases slightly. The throughput of handover process is generally higher than 16.4mbps. Compared with the other three mechanisms AAA, AAIS and IPSec, the throughput of SHPA increases by 13.2%, 9.6% and 3.8% respectively, when the distance between RS and eNodeB is about 2520m.

Outage probability is defined as the probability that information rate is less than the required threshold information rate. It is the probability that an outage will occur within a specified period. If the signal quality cannot meet the communication requirements, the high-speed train will be interrupted when the mobile handover occurs. The handover delay becomes longer with the faster train speed, and the farther the distance between RS and eNodeB, the higher the handover outage probability is. **Fig. 6** represents the outage probability of four secure handover mechanisms when the train speed is raised to 500km/h. The outage probability of SHPA mechanism is significantly lower than the other handover schemes. The SHPA mechanism prejudges the target eNodeB which the RS will access, and performs the handover

preparation in advance. When the distance between RS and eNodeB is 2520m, the average outage probability will reach a maximum value of 1.8% in SHPA mechanism. Compared with other secure handover mechanisms, the SHPA mechanism can decrease the outage probability remarkably during handover and guarantee the reliability of train to ground communication.

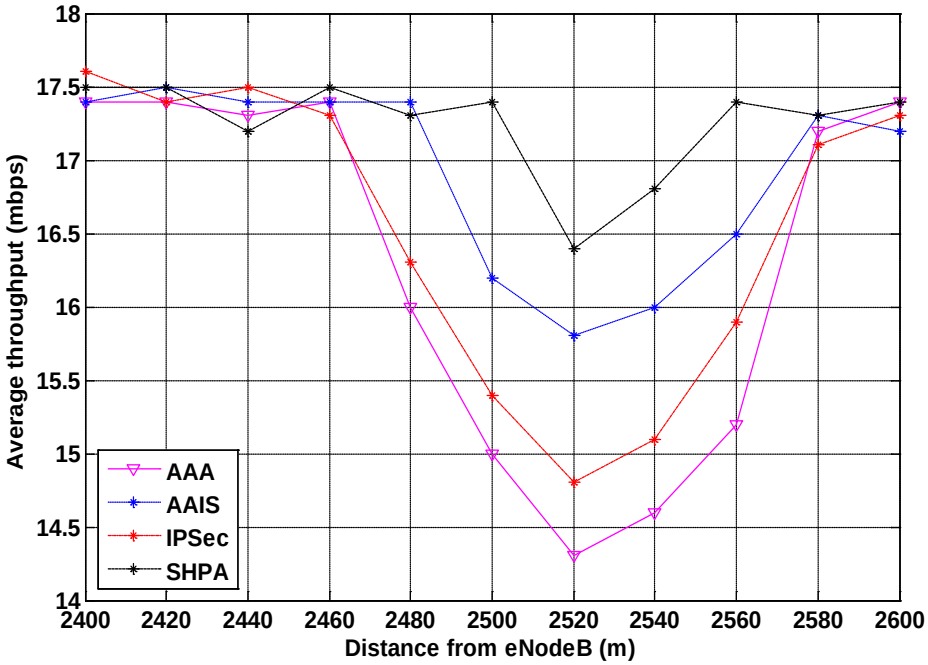

Fig. 5. Comparison of throughput among four secure handover mechanisms

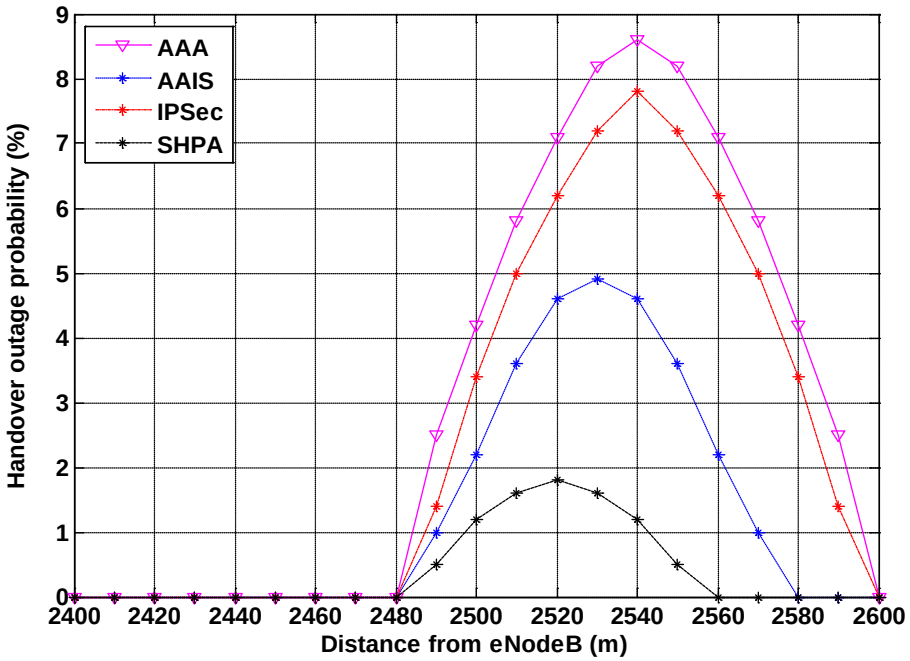

Fig. 6. Comparison of outage probability among four secure handover mechanisms

6. Conclusion

This paper focuses on how to realize the secure handover for high-speed trains in the process of running with relay stations. The target eNodeB that RS will access is prejudged through the location and the direction of the trains as well as the deployment topology of eNodeBs. On this basis, a pre-authentication based secure handover mechanism is designed for high-speed trains to realize mutual authentication between RS and target eNodeB, and generate the shared session keys with the authenticated key agreement protocol. The security analysis, efficiency analysis and simulation results show that the proposed SHPA mechanism not only can realize the secure handover, but also will effectively reduce the computational overhead of RS in the process of secure handover. When the running speed of a train is lower than 500km/h, the handover delay is generally lower than 50ms and the handover outage probability is less than 1.8%. When the running speed of a train is 350km/h, the throughput is higher than 16.4mbps in the process of handover. Therefore, the SHPA mechanism can improve the handover performance of high-speed trains and is expected to provide reference for the planning and designing of railway transportation information system in the future.

References

[1] R. He, B Ai, G. Wang, K. Guan, Z. Zhong, A. Molisch, C. Briso-Rodriguez, C. Oestges, "High-speed railway communications: From GSM-R to LTE-R," *IEEE Vehicular Technology Magazine*, vol.11, no.3, pp: 49-58, 2016. Article (CrossRef Link)

[2] J. Lee, C. Jang, O. Yi, "Analysis of radio based train control system using LTE-R and analysis of security requirements: The security of the radio based train control system," in *Proc. of International Conference on Computer Applications and Information Processing Technology*, pp: 1-4, August 2017. Article (CrossRef Link)

[3] H. Song, X. Fang, L. Yan, "Handover scheme for 5G C/U plane split heterogeneous network in high-speed railway," *IEEE Transactions on Vehicular Technology*, vol.63, no.9, pp: 4633-4646, 2014. Article (CrossRef Link)

[4] L. Yan, X. Fang, Y. Fang, "Control and data signaling decoupled architecture for railway wireless networks," *IEEE Wireless Communications*, vol.22, no.1, pp: 103-111, 2015. Article (CrossRef Link)

[5] A. Jabir, S. Shamala, Z. Zuriati, N. Hamid, "Fast handoff scheme for cluster-based proxy mobile Ipv6 protocol," *IEICE Transactions on Communications*, vol.E97-B, no.8, pp: 1667-1678, 2014. Article (CrossRef Link)

[6] M. Almulla, Y. Wang, A. Boukerche, Z. Zhang, "A fast location-based handoff scheme for vehicular networks," *IEEE International Conference on Communications*, pp: 1464-1468, June 2013. Article (CrossRef Link)

[7] I. Lopez, M. Aguado, "Cyber security analysis of the European train control system," *IEEE Communications Magazine*, vol.53, no.10, pp: 110-116, 2015. Article (CrossRef Link)

[8] X. Wang, C. He. "Safety function design and application of CTCS on-board equipment in high-speed railway of China," in *Proc. of International Conference on Electromagnetics in Advanced Applications*, pp: 677-679, October 2017. Article (CrossRef Link)

[9] J. H. Lin, L. Liu, C. Yi, W. Y. Wu. "Research on evolution law of service performance of high-speed train based on tracking monitoring," in *Proc. of IET Conference on Railway Condition Monitoring*, pp: 1-8, September 2016. Article (CrossRef Link)

[10] Z. Pan, S. Liu, A. K. Sangaiah, K. Muhammad. "Visual attention feature (VAF): a novel strategy for visual tracking based on cloud platform in intelligent surveillance systems," *Journal of Parallel & Distributed Computing*, vol. 120, pp: 182-194, 2018. Article (CrossRef Link)

[11] E. Aqeeli, A. Moubayed, A. Shami. "Towards intelligent LTE mobility management through MME Pooling," in *Proc. of IEEE Global Communications Conference*, pp: 1-6, December 2015. Article (CrossRef Link)
[12] S. Li, L. Yan, "Enhanced robustness of control network for Chinese train control system level 3 (CTCS-3) facilitated by software defined networking," *International Journal of Rail Transportation*, vol.2, no.4, pp: 239-252, 2014. Article (CrossRef Link)
[13] Y. Zhao, B. Tian, Z. Chen, Y. Liu, J. Ding, "An energy-efficient key agreement mechanism for underwater sensor networks," iCatse Conference on IT Convergence and Security, pp: 146-158, September 2017. Article (CrossRef Link)
[14] S. Liu, X. Cheng, W. Fu, Y. Zhou, Q. Li, "Numeric characteristics of generalized M-set with its asymptote," *Applied Mathematics & Computation*, vol. 243, pp: 767-774, 2014. Article (CrossRef Link)
[15] Y. Zheng, H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Information Processing Letters*, vol. 68, no.5, pp: 227-233, 1998. Article (CrossRef Link)
[16] Y. Li, Y. Qi, L. Lu, "Secure and efficient V2V communications for heterogeneous vehicle Ad Hoc networks," in *Proc. of International Conference on Networking and Network Applications*, pp: 93-99, October 2017. Article (CrossRef Link)
[17] M. Abdeljebbar, R. Elkouch, "Security analysis of LTE/SAE networks over E-UTRAN," International Conference on Information Technology for Organizations Development, pp: 1-5, March 2016. Article (CrossRef Link)
[18] S. Liu, W. Fu, L. He, J Zhou, M Ma, "Distribution of primary additional errors in fractal encoding method," *Multimedia Tools & Applications*, vol. 76, no.4, pp: 5787-5802, 2017. Article (CrossRef Link)
[19] R Sanodiya, "DoS attacks: A simulation study," in *Proc. of International Conference on Energy, Communication, Data Analytics and Soft Computing*, pp: 2553-2558, August 2017. Article (CrossRef Link)
[20] S. Zargar, J. Joshi, D. Tipper, "DiCoTraM: A distributed and coordinated DDoS flooding attack tailored traffic monitoring," in *Proc. of IEEE International Conference on Information Reuse and Integration*, pp: 120-129, August 2014. Article (CrossRef Link)
[21] Y. Zhao, X. Fang, R. Huang, Y. Fang, "Joint Interference Coordination and Load Balancing for OFDMA Multihop Cellular Networks," *IEEE Transactions on Mobile Computing*, vol.13, no.1, pp: 89-101, 2014. Article (CrossRef Link)
[22] H. Song, X. Fang, C. Wang, "Cost-reliability tradeoff in licensed and unlicensed spectra interoperable networks with guaranteed user data rate requirements," *IEEE Journal on Selected Areas in Communications*, vol.35, no.1, pp: 200-214, 2017. Article (CrossRef Link)
[23] Z. Haddad, M. Mahmoud, I. A. Saroit, S. Taha, "Secure and efficient uniform handover scheme for LTE-A networks," in *Proc. of IEEE Wireless Communications and Networking Conference*, pp: 1-6, September 2016. Article (CrossRef Link)
[24] W. Khedr, M. Abdalla, A. Elsheikh, "Enhanced inter-access service network handover authentication scheme for IEEE 802.16m network," *IET Information Security*, vol. 9, no.6, pp: 334-343, 2015. Article (CrossRef Link)
[25] P. A. Rohman, R. Indrawijaya, T. Miftahushudur, B. A. Wael, "Performance analysis of curve-shaped NLFM against Doppler effect and background noise," in *Proc. of International Conference on Radar, Antenna, Microwave, Electronics and Telecommunications*, pp: 54-58, October 2016. Article (CrossRef Link)

Yue Zhao received the BS degree in communication engineering in 2006 from the North China Institute of Science and Technology, Langfang, China, and the PhD degree in information and communication systems in 2012 from Southwest Jiaotong University, Chengdu, China. From September 2010 to September 2011, he was a visiting student in the Department of Electrical and Computer Engineering, University of Florida. He is currently a senior engineer of science and technology on communication security laboratory, Chengdu, China His research interests include wireless network and information security.

Bo Tian was born in 1970. He received a M.S. degree in communication engineering from University of Electronic Seience and Technology of China (UESTC), in 1997. Currently, he is a professor status high level engineer of Science and Technology on Communication Security Laboratory, Chengdu, China. His main research interests include cyberspace security and communication information system.

Zhouguo Chen was born in 1980. He received a M.S. degree in signal and information processing from University of Electronic Seience and Technology of China (UESTC), in 2006. Currently, he is a network security senior engineer of science and technology on communication security laboratory, Chengdu, China. His main research interests include network security, big data and network forensics.

JIN YANG received the M.S. and Ph.D. degrees in computer science from Sichuan University, Sichuan, China, in 2004 and 2007 respectively. He is currently an Associate Researcher with the College of CyberSecurity, Sichuan University, China. His main research interests include network security, articial immune systems, knowledge discovery, and expert systems.

Saifei LI was born in 1988. He received the B.E. and Ph.D degree in communication engineering from Southwest Jiaotong University. He is currently a lecturer with Southwest Jiaotong University. His research interests include network security and software defined networking.