Improving the Security of Wireless Communications on High-Speed Trains by Efficient Authentication in SCN-R

Tong Xu, Deyun Gao, Senior Member, IEEE, Ping Dong, Chuan Heng Foh, Senior Member, IEEE, Hongke Zhang, Senior Member, IEEE, Victor C. M. Leung, Fellow, IEEE

Abstract—Recently, we have witnessed the remarkable development in high-speed railways around the world. To provide a robust and fast wireless network for the onboard passengers, we have earlier proposed smart collaborative networking for railways (SCN-R). In the realization of SCN-R, its security is challenged by potential exploitation of authentication vulnerabilities since traditional authentication mechanisms are unsuitable for scenarios with fast moving objects due to their complex and relatively timely operations. In this paper, we address this issue by proposing a new efficient authentication mechanism, which is based on a new design of chaotic random number generator (RNG). Comparing with the recent proposal relying on the precise boundaries of chaotic map state-spaces, our RNG uses two logistic maps to avoid the time-consuming boundary location process. The proposed authentication mechanism uses the RNG to generate and validate the one-time password (OTP). To support different authentication applications, different lengths of OTPs can be used to differentiate and identify the applications. We have implemented our proposed authentication mechanism under real world conditions with results showing the feasibility and effectiveness of our authentication mechanism.

Index Terms—Wireless communication, communication system security, chaos, random number generator, cyber attack.

I. INTRODUCTION

In the past decade, high-speed railways have been developed rapidly as a green transportation system. In China, for example, the total length of business high-speed railway has reached 21,000 kilometers, and it transports double the number of passengers than what airplane transports [1]. Furthermore, the electric high-speed train is energy efficiency. Its energy cost is about 13,104 kJ per passenger per kilometer, which is only about 8.5% of the airplane [2].

Since the commute time is usually long, passengers demand Internet connectivity to manage their daily activities during the journey. However, the travelling speed of the high-speed train (typically 350 kilometers per hour) leads to unstable wireless connectivity. Although the modern cellular networks support high-speed movement, their actual performance will be compromised when the moving speed exceeds 120 kilometers per hour, due to frequent handovers and reconnections [3]. To improve the onboard user experience, some advanced radio access networks have been proposed [4-6]. However, they require updating the roadside units which will be both time and resource consuming.

To build a robust wireless network for the passengers without expensive road side unit updates, we have proposed smart collaborative networking for railway (SCN-R) [7]. The SCN-R introduces two types of equipment. One is the onboard smart mobile router (SMR), which supports various wireless network interfaces, such as WCDMA (3G) and TDD/FDD-LTE (4G). The other one is the ground side smart access router (SAR), which serves as a proxy for the SMR and its main responsibility is tracking and communicating with the SMR. In SCN-R, users connect to the SMR directly inside the train. Then the SMR delivers the user data to the SAR using several wireless interfaces concurrently. It can select the wireless interfaces dynamically according to their link status. The SAR further relays the data to the Internet and passes the returning data back to the SMR. It also tracks the current wireless interface IP addresses of the SMR by monitoring its received packets.

In the realization of SCN-R [8, 9], we made an important observation. While adding wireless interfaces on the SMR generally improves the reliability of SCN-R, it has limited effect once the wireless interfaces exceed a certain number. In fact, the reliability of SCN-R depends not only on the wireless links between the SMR and the RAN, but also the wired links in the radio access network (RAN), the core network (CN) and the public network (PN). The unexpected delay on the wired links causes disordered packets. Some delayed packets may still carry outdated information particularly the wireless interface IP addresses of the SMR. This outdated information may confuse SAR and cause delivery of packets to incorrect wireless interface IP address. Confusion may be created intentionally too. For example, replay/spoofing attacks from the public network can disrupt the tracking of a moving SMR. They can aggravate the fluctuation of data delivery delay by replaying legitimate data or fabricating packets that indicate wrong wireless interface IP addresses. On the SMR side,
resource limitation is the main vulnerability. A simple UDP flood attack launched within the public network can exhaust the limited wireless bandwidth through the wired links. They may overload the SMR and even block returning services by flooding lots of non-purposeful data to the SMR. Therefore, SCN-R requires an adequate access control to identify and defend against any malicious activities that can lead to perplexing delay observation in the SAR or excessive non-purposeful data receiving in the SMR. An efficient authentication mechanism is therefore a foundation of dealing with the above problems.

The motivation of this paper is that the existing authentication mechanisms are unsuitable for SCN-R. While there are many robust authentication systems implemented in the real-world, these authentication processes often require complex reversible cryptographic operations, such as the symmetric encryption and asymmetric encryption. If the SMR and the SAR require to carry out such cryptographic operations in the authentication process, cyber attackers can exhaust their computation resources by flooding with excessive fabricated authentication requests. While seeking light to reversible encryption free authentication mechanisms counter such resource-depletion attacks, they require frequent message exchanges which is unsuitable for the high-speed train scenario. For example, as shown in Fig. 1, the life-time of an IP address is about 15 seconds in a moving high-speed train typically. Whereas, the average round-trip time (RTT) is about 1.2 seconds when the IP address changes (i.e. when an authentication is required) [8]. Therefore, more rounds of message exchanges leads to obviously longer authentication process and lower wireless network utilization in the high-speed train scenario.

In this paper, we propose an efficient authentication mechanism for SCN-R based on chaotic systems and irreversible cryptographic operations. The chaotic systems generate the OTP in the authentication message and the irreversible cryptographic operations protect the authentication message from being tampered. To achieve this, we first design a novel random number generator using chaotic maps that does not involve in the complex chaotic map state-space partition which is present in existing designs. Then we deploy a pair of synchronous random number generators in both SMR and SAR, which generate and check the OTP in the authentication message. In this way, we avoid the need to use reversible cryptographic operations and reduce the processing complexity and communication overheads. Finally, to improve the security property of the proposed authentication mechanism, we further leverage the irreversible cryptographic operations to protect the authentication message from being tampered. The main contributions of this paper are summarized as follows.

- We have proposed a novel chaos-based RNG and prove the randomness of its output. Comparing with the existing designs, our proposal is more efficient since it avoids the complex chaotic map state-space partition process.
- We have designed an efficient authentication mechanism for SCN-R by adopting a pair of the proposed RNGs. Comparing with traditional irreversible encryption based authentication mechanisms, it shows a better performance when dealing with missing OTP and the brute-force attack.
- We have shown the feasibility and effectiveness of our proposed method by implementing and testing the proposed authentication mechanism in both static and fast moving scenarios using the SMR and SAR devices.

The rest of the paper is organized as follows. Section II summarizes the recent progress in the vehicular authentication. In Section III, we review SCN-R and two types of cyber attacks in SCN-R. We also provide the basic knowledge of chaotic map and chaos-based authentication. In Section IV, we propose the novel RNG using the logistic map. The authentication mechanism and the implementation details are provided in Section V. In Section VI, we show the experiments and results of our proposal in both static and high speed moving scenarios. Finally, we draw important conclusions in Section VII.

II. RELATED WORK

A. Asymmetric Encryption Based Authentication Mechanisms in Vehicular Networks

Vehicular networks (e.g. vehicular ad hoc networks) are considered to be an important application scenario for the future wireless communication. To improve the authentication efficient between cars and roadside units, several promising methods have been proposed.

In most of the authentication mechanisms, the vehicle signs and verifies the authentication message using the traditional public key infrastructures (PKIs) [10-12]. To shorten the length of keys and simplify the cryptographic operations, the elliptic curve cryptosystem (ECC)-based PKI is widely used apart from the RSA-based PKI [11]. For different authentication message receivers, they need to hold a large number of private keys and execute the corresponding amount of cryptographic operations [12]. Recently, a proposal of group signature and verification [13, 14] is viewed as a promising way to reduce the number of keys and improve the authentication efficiency. In the group signature and verification mechanisms, a group of vehicles share group public keys and each group member can sign authentication messages on behalf of the other in the same group. However, the main challenge for such a proposal lies in the group membership maintenance of dynamic group members and time-consuming certificate revocation list checking. To address these issues, Vijayakumar et al. [15]
attempt to update the group member list and key settings in a computationally efficient way, in which subscribed vehicles are treated as authorized primary users and they are free from group key negotiation process. Whereas the rest of secondary and unauthorized vehicles require group keys from the trusted authority through the primary users. Besides, Zhu et al. [16] propose replacing the certificate revocation list with a hash message authentication code to shorten the time in signature verification process.

As for the efficient authentication between the vehicle and the roadside unit, the batch verification and the hierarchical authentication are the most adopted techniques. Proposals using the batch verification [17-20] allow the roadside unit to verify multiple authentication messages at the same time, which reduces the overhead and increases the throughput. However, since in these proposals, the verification is processed in batch, responses are released after an adequate number of authentication messages received for processing, delay is expected especially when there are few authentication messages. Besides, the batch verification proposals are generally susceptible to attacks which inject messages with false information to disrupt the verification. To counter this kind of attacks, Liu et al. [21] propose a hierarchical authentication scheme to reduce the workload of the centralized roadside unit. They introduce proxy vehicles which help to verify the authentication messages for nearby vehicles. Then the verified messages are aggregated and forwarded to the roadside unit. Similarly, Zhang et al. [22] focus on combining the batch verification and the hierarchical authentication. They attempt to reduce the waiting time of the vehicle by regulating the authentication message generation.

We note that most of the existing authentication mechanisms rely on the complex asymmetric cryptographic operations. Therefore they are generally susceptible to the resource-depletion attack. These mechanisms are not suitable for our scenario since the SAR has to process a large number of certificates for the SMRs which represents a bottleneck in the design. Besides, the timely requirement for verification due to high travelling speed of SMR does not permit the use of batch verification and the hierarchical authentication in SCN-R.

B. Symmetric Encryption and Hash Chain Based Authentication Mechanisms

In order to simplify the authentication process and reduce communication overhead, many proposals use symmetric encryption instead of asymmetric encryption to code the authentication message. As designed in some proposals [23, 24], the asymmetric encryption is only responsible for the transition of symmetric keys. The symmetric keys are then used in the authentication process. Although such proposals show great advantage in communication overhead control [25] compared with the pure asymmetric encryption based authentication mechanisms, they are still vulnerable to the resource-depletion attack.

To make the authentication mechanism free from reversible cryptographic operations and resource-depletion attacks, some proposals [26-30] attempt to design authentication mechanisms without the symmetric encryption and asymmetric encryption. The common working principle of these proposals is summarized in Fig. 2. They use the hash chain to generate the dynamic one-time password. We denote \( y = h(x) \) to be the secure hash function, where \( x \) is the input in form of arbitrary size and \( y \) is the output in form of a fixed size. Then a secure \( h \) has the property that computing \( y \) with given \( x \) is simple while finding \( x \) with given \( y \) is extremely difficult. As shown in Fig. 2, the access controller first chooses an initial seed \( s \) and a system number \( N \), and sends them to the access user. Then the access user authenticates itself by using a sequence of one-time passwords \( p_i = h^{N-i}(s) \). The differences between the studies [26-30] lie in the design of \( h(x) \) and \( s \). Typically in vehicular ad hoc networks, Vighnesh et al. [31] propose a detail authentication mechanism based on hash chains, in which each vehicle owns an unique master key as its seed \( s \) and the authentication center knows the master key. In their proposal, the system number \( N \) is randomly selected by the vehicle and transmitted to the authentication center in ciphertext.

The main security issue of using hash chain to generate and check OTPs is that the OTPs are chained. Due to the connections between OTPs, when an OTP is missing, the chain is broken, and the authentication process needs to renegotiate a new initial seed \( S \) and system number \( N \). For example, as shown in Fig. 2, when \( p_0 \) is missing in the authentication process, the access controller will fail to check \( p_1 \). Similarly, all the OTPs generated after \( p_1 \) will also be invalidated until a new initialization state is established between the access user and the access controller. In fact, the missing of OTPs happens quite commonly in high speed moving scenarios due to unstable wireless link status, which leads to an unexpected increase of communication overhead and lower wireless bandwidth utilization in SCN-R. Besides, the secret hash chains are challenged by the modern collision attack, which is well known as the birthday attack. Since knowing massive history OTPs means knowing massive input-output pairs of the secret hash chains, attackers can disrupt the hash chain based authentication process by finding the collision (e.g. finding an illegal OTP \( p'_1 \), which satisfies \( p'_1 \neq p_1 \) but \( h(p'_1) = p_0 \)) or cracking the secret hash chains (i.e. finding unused legal OTPs). Based on that, attackers may deceive the authentication controller using the modified OTPs.

![Fig. 2. The authentication process of the hash chain based mechanisms.](image-url)
III. SCN-R AND ITS SECURITY CHALLENGES

A. The Working Principle of SCN-R

We first illustrate the operation of SCN-R by using an example given in Fig. 3. In our example, an onboard SMR initially connects to the Internet via 3G cellular network. It then encapsulates the user data with the IP address assigned by the NodeB. With the movement of the train carrying a SMR, the SMR has moved out of the coverage of the 3G cellular network and detected a 4G cellular network. It quickly makes connection to the eNodeB and begins to packetize the user data with the newly assigned IP address. The SAR will monitor such outer IP address changes of the encapsulated packets when it fetches services for the user. The SAR is aware of the movement of the SMR and its current active IP address. Therefore, the SAR can return the services to the latest IP address of the moving SMR. In this way, SCN-R provides a stable and fast wireless network for the onboard user.

B. Security Challenges and Attack Models

In evaluating the robustness of SCN-R, we noticed several vulnerabilities in the process that can compromise the SAR and the SMR. We discuss the challenges in the aspect of content and communications as follows.

The message exchange between SAR and SMR can be sniffed and man-in-the-middle (MITM) attacks can be launched. Authentication is a means to defend MITM attacks. Here we introduce an authentication procedure to defend such attacks. While there are many existing robust authentication solutions, the lifetime of a session in our scenario is very short as discussed and shown in Fig. 1, we seek lightweight approach to fulfill the authentication need. However, vulnerabilities exist in the current lightweight authentication solutions such as hash-based OTP authentication. The hashed content can be sniffed, cracked, and used for attacks in the current and future sessions. Attacking the current session will be challenging given the very short lifetime of a session and the significant effort to crack the OTPs. However, attacking a future session is possible if the OTPs are chained, as a result, future OTPs can be derived by sniffing and cracking observable OTPs. Our solution particularly addresses this by using OTPs that are not chained. Because OTPs are independent, observing current OTPs does not provide any useful information to derive any future OTPs. Direct attack on the contents is discouraged with our solution.

In terms of communications, the robustness of SCN-R demands the SAR to properly track the IP address of all SMRs. However, due to the handover, excessive delay presence in the RAN, CN or PN may compromise the packet delivery order and cause tracking confusion in the SAR. This issue may occur when an SMR is disconnected from an out of range network and reestablish a connection to another network. As shown in the example illustrated in Fig. 4, a new wireless interface IP address assigned by the eNodeB in 4G cellular network will take over the communication replacing the previous IP address. However, packets using the previous outdated IP address may suffer from excessive delay and arrive at the SAR later than those packets using the newly assigned IP address. The later arrival of the packets with outdated IP address may cause the SAR to switch to the outdated IP address for subsequent communications. Apart from attacking the communication handshake procedure, it is also possible to attack the communication resources. Flooding attack is a common attack.

Since deriving full knowledge of the OTPs is discouraged, we shall focus on attacks that do not rely on the knowledge of OTPs. We have identified replay, spoofing and flooding attacks as key threats which are discussed in the following.

1) Replay and Spoofing Attacks: The tracking of IP address may be compromised deliberatley. A replay or spoofing attacker can actively pollute the data traffic to prevent the SAR from tracking the current IP address of the SMR. The attacker first listens to the packets from the SMR to the SAR.

---

Fig. 3. The working principle of SCN-R.

Fig. 4. Two security challenges in SCN-R.
Then the attacker may attempt to fabricate packets with a fake wireless interface IP address (the outer source IP in Fig. 3) and send such packets to the SAR pretending to be a legitimated user. Focusing on applications for mobile users, Chankasame et al. propose a novel chaotic map and design an authentication mechanism[35]. The message that need to be sent is viewed as the input $x_0$ of the chaotic map. Their authentication mechanism uses 8 chaotic maps $y = f(x)$ to generate different highly random outputs $f^N(x_0)$. Instead of building a RNG, the authors leverage hash functions to convert the output $f^N(x_0)$ into fixed length. However, these proposals usually require frequent intercommunication to update the initial state on the access user.

Clearly, the existing authentication mechanisms in their current form are unsuitable for our considered scenario. In this paper we make an attempt to improve the authentication mechanism by addressing these weaknesses. In particular, we improve the chaotic map-based approach by further reduce the intercommunication overhead to achieve a lighter and faster process.

IV. Chaos-Based Random Number Generator

In this section, we provide a new random number generator, which is the foundation of designing our authentication mechanism. The random number generator is widely used in authentication and synchronization applications. Traditional random number generators rely on the unpredictable physical process, such as the thermal noise in the circuit or the white noise in the radio. However, in the real world operation, the unpredictable physical processes are often difficult to control. Recently, deterministic chaotic systems are widely discussed to be used as the information sources in the random number generator. Stojanovski et al. [36, 37] have provided a comprehensive analysis of the randomness in deterministic chaos. Particularly, they have proved that many chaotic maps (e.g. logistic map) can be utilized to generate random numbers.

According to the studies of Stojanovski et al. [36, 37], given a chaotic map $f : S \rightarrow S$ (where $S$ is the state space of $f$) and an expected output symbol set $O = \{O_1, ..., O_m\}$, before it can be used to generate random numbers, a partition of $S$ (we denote it as $\alpha = \{\alpha_1, ..., \alpha_m\}$) should be calculated first. The partition needs to meet the following conditions

\[
\left\{ \begin{array}{l}
\bigcup_{i=1}^{i=m} \alpha_i = S \\
\alpha_i \cap \alpha_j = \emptyset \\
\forall \alpha_i, \alpha_j \quad P[f(x) \in \alpha_i] = P[f(x) \in \alpha_j].
\end{array} \right.
\] (1)

For example, if we use the logistic map $x_{n+1} = r x_n (1 - x_n)$ to generate a series of binary random numbers (i.e., $O_1 = 1$, $O_2 = 0$, $m = 2$), we need to find the boundary between region $\alpha_1$ and region $\alpha_2$ which satisfies (1). The parameter $r$ decides the chaos property of $x_n$ when the initial state $x_0$ is selected. When $r$ is set to 4, for almost all initial states, the outputs can go into chaos quickly. Then we decide the $n$th random number in the output queue (OQ) as follow.

\[
OQ_n = \begin{cases} 
O_1 & f(x_n) \in \alpha_1 \\
O_2 & f(x_n) \in \alpha_2.
\end{cases}
\] (2)
However, it should be noted that we cannot use finite iteration results to calculate the precise boundaries between the partition regions in S, since the boundaries change with the increase of the iterations. Besides, although the iteration results of the chaotic map are distributed randomly in S, their distribution is uneven. That explains why the boundary between the two partition regions is not always equal to half of the supremum of S.

In order to find a solution to generate random numbers without the calculation of precise boundaries, we propose Algorithm 1 using two logistic maps with the same r but different initial state x0. We denote one logistic map f1 : S → S as the master map, the other logistic map f2 : S → S as the slave map. The initial state of the master map is x0 and that of the slave map is x0. For each iteration, both the master map and the slave map calculate their outputs x1 = f1(x0) and x1 = f2(x0). Then we decide the output binary of the iteration as follow.

\[
OQ_n = \begin{cases} 
O_1 & x_1 > x_2 \\
O_2 & x_1 < x_2
\end{cases}
\]

Since computer programs calculate iteration results with a limited accuracy, the inaccuracy may lead to the condition where x1 = x2 while iterating the chaotic maps. To avoid such an issue in the process, in our design given in Algorithm 1, the slave map iterates with extra times until x1 ≠ x2.

In the following, we shall show the randomness property of our proposed algorithm. Precisely, we need to prove that

\[
P(OQ_i = O_1) = P(OQ_i = O_2) = 0.5, \quad 1 \leq i \leq n. \tag{4}
\]

For the master map and the slave map, we assume that \(\alpha^1 \) = \(\{\alpha_1, ..., \alpha_m\}\) and \(\alpha^2 \) = \(\{\alpha_1, ..., \alpha_m\}\) are their partitions in the state spaces. According to (1), they satisfy that

\[
\forall \alpha^1, \alpha^2 \quad P(f_1(x) \in \alpha^1) = P(f_2(x) \in \alpha^2) = \frac{1}{m}. \tag{5}
\]

Since f1 and f2 have the same r and the same number of iterations n, when n → ∞, the boundaries of the regions in \(\alpha^1\) are the same with that in \(\alpha^2\). For each iteration (e.g., ith), the corresponding iteration results f1(x0) and f2(x0) are independent, and they fall into two regions. Then \(O_1\) occurs with the probability where

\[
P(OQ_i = O_1) = \lim_{m \to \infty} \sum_{k_1=1}^{m-1} \sum_{k_2=k_1+1}^{m} \frac{1}{m} = 0.5.
\]

Similarly, \(O_2\) occurs with the probability where

\[
P(OQ_i = O_2) = \lim_{m \to \infty} \sum_{k_1=2}^{m} \sum_{k_2=1}^{k_1-1} \frac{1}{m} = 0.5.
\]

V. AUTHENTICATION MECHANISM AND IMPLEMENTATION DETAILS

In this section, we first provide the proposed authentication mechanism. Then we describe the implementation details that address the aforementioned security challenges described in Section III.

A. Authentication Mechanism

1) Normal Operation: Fig. 6 shows the working principle of the proposed authentication mechanism. The authentication mechanism is based on deterministic chaotic maps. The underlying idea is to build two same random number generators. One resides inside the SMR and the other one resides inside the SAR. To make sure their outputs are synchronous, the SMR and the SAR use the same iteration step and accuracy.

More specifically, the entire procedure consists of two phases, i.e., the initialization process and the authentication process. In the initialization process, the SAR sends a pair of secret initial states (x0 and x0) to the SMR. For different SMRs, their secret initial states are unique. With the public chaotic maps (f1 and f2), the SMR and the SAR build their own random number generators as described in Section IV.

In the authentication process, using the secret initial state x0 and x0, the SMR first iterates the public chaotic map f1 and f2 with 2N times, thus getting the N-bit main OTP (MOTP, e.g., p1 and p2) and the N-bit secondary OTP (SOTP, e.g., sp1 and sp2) from its random number generator. Next the SMR sends the MOTP to the SAR while holding the SOTP. The SAR checks the MOTP with its own random number generator and calculates the corresponding SOTP by executing the same task. Finally, to acknowledge the correctness of the MOTP, the SAR returns the SOTP to the SMR as an
acknowledgement. As shown in Fig. 6, both the SMR and the SAR update their initial states with step $2N$ (i.e. the $x_0^1 = f_{2N}(x_0^0)$ and $x_0^2 = f_{2N}(x_0^1)$ shown in Fig. 6) once the authentication is finished. The updated initial states can be used for the subsequent authentication.

2) Case 1: OTP Transmission Failure: One main challenge with the high-speed movement scenario is the unstable wireless connectivity leading to the failure of packet delivery. Packet loss may occur during the authentication procedure. The failure to deliver messages during the authentication procedure directly affects the synchronization between the SMR and the SAR. This may affect the judgement of the SAR and make the SAR fail to identify the subsequent legitimate OTPs when an earlier one is missing. To improve the robustness of synchronization, we introduce additional message to assist the process synchronization. In particular, we use an 8-bit value to record the number of time that OTP transmission fails (TOTF).

For example, as shown in Fig. 6, when the SAR misses a 1-bit OTP, it will return $x_{18}^0$ to the SMR (in the 3rd authentication), the SMR tries a fresh MOTP, and announces $TOTF=1$. As the SAR revives the fresh MOTP, it first iterates the public maps $2N \cdot TOTF$ times to update its initial states. Then it checks the fresh MOTP and calculates the corresponding SOTP as depicted in Fig. 6. When the authentication process is completed, the SMR and the SAR updates their initial states with $2N \cdot (TOTF + 1)$ steps. As for missing SOTP, upon detection, the SMR simply uses a new pair of MOTP and SOTP to launch a new authentication.

Since the attackers can hardly know which OTP is missing on the unstable links between the SMR and the SAR, it is difficult for them to re-send the missing OTP exactly and massively. In this case, even when an attacker re-sends $p_3$ and $TOTF=0$ to the SAR before the 4th authentication, the authentication packets will be invalidated unless they carry the correct packet headers because of the MD fields shown in the following Case 2. Then the SAR will return $sp_3$ to the SMR, consequently the missing OTP is filled by the attacker.

3) Case 2: Authentication Tampering: Besides serving as the authentication acknowledgement, the SOTP is also designed to protect the MOTP and TOTF from being tampered. Since the MOTP and TOTF are sent in plaintext, attackers may intercept the transmission and replace the IP headers or TOF in order to disrupt the authentication process. While the potential of such an attack is very low due to the high-speed movement of the train which creates a challenging environment for the attack to be success, a simple solution exists to counter the attack which makes it worthwhile to implement. We use an irreversible encryption algorithm (e.g. MD5) to counter the attack. As shown in Fig. 7, when the SMR receives the MOTP and the SOTP from its random number generator, it calculates the message digest (MD) taking consideration of the IP headers, the MOTP, TOTF and the SOTP. Then the SAR replaces the SOTP with the MD before it sends the authentication packets to the SAR. Since attackers do not have the SOTP, they cannot falsify the authentication packets. The SOTP can be transmitted in plaintext, since it does not provide any useful information for attackers to interfere the authentication process and derive any MOTP or SOTP that are used in the subsequent sessions.

The strength of this authentication mechanism is due to the property of chaotic maps, which is sensitive to the initial states. Even if eavesdroppers collect history OTPs and the public chaotic maps, without the precise secret initial states, the future N-bit OTPs cannot be derived directly. Exhaustive OTP search may be possible but it is extremely time consuming especially when $N$ is large. To achieve a satisfactory security level, the recommended $N$ is usually larger than 128 [38]. As for the security property of adopting MD5 algorithm, we believe it is adequate for our scenario. This is because firstly, the length of the input in our mechanism is larger than 256 bits (i.e. the total length of the MOTP and the SOTP) which is sufficiently large enough to discourage an attack. According to the commercial MD5 crack website [39], a real-time crack service is available for only inputs of 100 bits or shorter. Secondly, although the commercial MD5 crack website can break over 90% MD5 encrypted message that is longer than
100 bits, the time required is around one hour which is much longer than the lifetime of the wireless interface IP addresses in our high speed moving scenario which is usually less than 20 seconds. The lifetime of our OTP stays within the lifetime of a wireless interface IP address. Finally, unlike the OTPs generated by hash chains, our OTPs are not chained. In other words, even attackers can record the history MD5-encrypted OTPs and eventually crack them, the history of OTPs does not provide any useful information to derive any future OTP.

We recognized that our authentication mechanism can be further enhanced in several aspects. An immediate enhancement is to consider modern message digest algorithm, such as SHA-160 and SHA-256 to replace MD5. However, due to the time-sensitive authentication process in SCN-R, some of the robust but complex message digest algorithms may not be appropriate and demand further investigation. Another enhancement is to remove the MOTP field in the authentication packets sent from the SMR as shown in Fig. 7. This keeps the OTPs further away from eavesdroppers and further improves the security of our proposed solution.

**B. Defending the Cyber Attacks Using the Proposed Authentication Mechanism**

Fig. 8 depicts the implementation environment of our proposed authentication mechanism. In the real world operation, the SMR can send different lengths of OTPs for different authentication applications.

SMR. Then the SMR receives the acknowledgment from the SAR (which contains the SOTP shown in Fig. 7), and starts to forward user data using the new wireless interface IP address. When the SAR receives a series of delayed or attack packets using the outdated or fake IP address of the SMR, since these packets do not carry fresh MOTPs, the SAR will immediately detect that their outer IP address is invalid. This will prevent any third party who has not got enough knowledge to generate a correct OTP from fabricating authentication packets to the SAR. As a result, the tracking of the SMR can be protected.

To authenticate a compromised wireless interface IP address and mitigate the UDP flood attacks, the SMR sends four same authentication packets when it monitors an increasing proportion of not-purposeful packets. The authentication packets are constructed by an outer IP header (which includes the compromised interface IP address of the SMR), an inner IP header (which indicates the SAR is the final destination) and a 160-bit MOTP. Once the SAR receives and confirms the message, it quickly abandons the existing wireless interface IP address which has been compromised, and redirects data to other available interfaces.

Both the MOTP and the SOTP are the output of the RNG. Therefore, to save the computation cost in the authentication process, the SMR and the SAR can use their RNGs to prepare enough outputs and store them locally before the authentication begins.

**VI. EXPERIMENTS AND RESULTS**

To test the proposed RNG and authentication mechanism, we conduct a series of experiments in both static and high speed moving environments. We also compare our authentication mechanism with two existing reversible encryption free schemes.

**A. Experiment and Result in Static Environment**

In the static environment, we use our developed SMR shown in Fig. 9 and our SAR deployed in Alibaba Cloud [40]. In the experiments, we install three 3G/4G wireless interfaces (i.e. CMCC TD-LTE, CUCC FDD-LTE and CTCC EV-DO) in the SMR.

First, we test the new wireless interface IP authentication mechanism, which is designed to defend against replay/spoofing attacks to SCN-R. In this experiment, to launch...
a real attack to the SAR, some earlier received packets on
the ingress of the SAR are replayed to Alibaba Cloud from a
laptop (i.e. the attacker) in our laboratory. At the same time,
a normal user attempts to retrieve live videos from a public
video site using the SMR shown in Fig. 9. The attack packets
last for 60 seconds. We collect statistics in the attack and the
adjacent time periods (also 60 seconds).

Figs. 10(a) and (b) show the wireless bandwidth utiliza-
tion between the SMR and the RAN without and with the use
of our proposed authentication mechanism respectively. As
can be seen in Fig. 10(a), the repeated packets cause the SAR
failing to trace the correct wireless interface IP address and
failing to return the videos to the user. With our proposed au-
thentication mechanism, when the SAR checks the IP address
changes with the OTPs in the payload, the attack packets fail
to hijack the normal traffic as shown in Fig. 10(b).

To have a deeper insight to the attack, we count the packet
loss rate of the wireless interfaces on the SMR in Fig 11. As
can be seen in Fig. 11(a) showing the packet loss rate without
using our proposed authentication mechanism, the repeated
packets first interrupt the CMCC TDD-LTE wireless interface
and push the packet loss rate up to around 30% at the 21th
time slot, then they compromise the CUCC FDD-LTE wireless
interface and bring the packet loss rate to around 27% at the
31th time slot. Such high packet loss rates eventually cut off
the legitimate live video service. In contrast, the new wireless
interface IP authentication mechanism prevents the replay
attacks and keeps the packet loss rate within the acceptable
range shown in Fig. 11(b).

The corresponding RTT statistics of this experiment are
summarized in Fig. 12. For the case without our proposed
authentication mechanism, the repeated packets mislead the
video services to a wrong destination (i.e. the attacker), the
requests from the SMR fail to receive their response in time.
During the simulated attack, as shown in Fig. 12(a), the
RTT of the CMCC TDD-LTE wireless interface increases
dramatically to around 900ms and the RTT of the CUCC FDD-
LTE increases drastically to just over 800ms. These sudden
increase in RTT affects many applications especially those
involving in delivering real-time packets such as live video.
Fig. 12(b) shows the benefit of the authentication mechanism
where RTT remains low throughout the experiment.

We can see that, even both the normal packets and the
authentication packets are repeated by the attacker, they cannot
interfere the tracking of the SMR since the authentication
packets can only be used once. The repeated authentication
packets have no effect on the SAR apart from indicating to the
SAR that the communications may be under certain attacks.

Second, we test the effectiveness of the authentication mech-
anism against flooding attacks to the SMR. In this experiment,
to launch a UDP flood attack to the SMR, we rent a server
in Alibaba Cloud and deploy an application to continuously
send UDP data to a single wireless interface while a normal
user is watching live videos using the SMR. The attack rate
is set to higher than the upper limit of the bandwidth of the
wireless interface. In the experiment, according to our test,
for the CMCC TDD-LTE or the CUCC FDD-LTE wireless
interface, the upper limit of the bandwidth is about 50Mbps.
Therefore, we set the attack rate to be 60Mbps. The flooding
of UDP packets lasts for 60 seconds.

Without the authentication mechanism, we observe from
Fig. 13(a) that the UDP data consumes more than 95% of
the bandwidth between the SMR and the RAN while the
user data only utilizes about 5%. Even the live videos are
not interrupted under the flooding of UDP packets, the UDP
packets cost additional bandwidth and computing resources.
B. Experiment and Result in High Speed Moving Environment

In the high speed moving environment, we use our developed SMR shown in Fig. 15 and the SAR deployed in the information technology center on our campus. In the experiment, the SMR is deployed on a high-speed train (350Km/h) on the Beijing-Shanghai express railway. We install three 3G/4G wireless interfaces (i.e. CMCC TD-LTE, CUCC WCDMA/FDD-LTE and CTCC EV-DO) in the SMR.

Fig. 15. The used SMR in the high speed moving environment.

In order to test the new wireless interface IP authentication mechanism, we repeat the packets from the SMR at the ingress of our campus information technology center to simulate the replayed attack from the PN while the train is moving and the authentication mechanism is working. The repeat operation lasts about 20 minutes. During the 20 minutes, we turn off the authentication mechanism for 3 minutes to observe the benefits of the authentication mechanism. As shown in Fig. 16, once the authentication mechanism is turned off, all the three wireless interfaces fail to receive the data which indicates transmission disruption due to the replayed attack. As soon as the authentication mechanism is resumed, the SAR immediately distinguishes the outdated wireless interface IP addresses from the normal ones and the wireless bandwidth consumption returns back to the normal range.

Fig. 16. The fluctuation of the wireless bandwidth between the SMR and the SAR in the high speed moving environment.

We also record the packet loss rate performance in Fig. 17. When the authentication mechanism is turned off, the SAR...
fails to trace the correct wireless interface IP addresses of the SMR and consequently returns most of the packets to the outdated IP addresses claimed by the repeat operation. Therefore, the packet loss rates obtained from the moving SMR increase drastically. With the resumption of the new wireless interface IP authentication mechanism at the 10th minute shown in Fig. 17, the packet loss rates decrease immediately. We further record the corresponding RTTs in Fig. 18. In our measurement, we cap the RTT measures to 5000ms as any RTT measure exceeding the cap simply indicates an abnormal event. We can see from Fig. 18 that most RTT measures give 5000ms when the authentication mechanism is turned off.

To test the effectiveness of the proposed authentication mechanism against flooding attack from the PN while the train is moving. We simulate the attack by duplicating the packets from the SAR at the egress of our campus information technology center. The duplication operation lasts for about 5 minutes. In Fig. 19(a), we first show the results without the authentication mechanism. We can observe that most of the wireless bandwidth is occupied by the duplicated packets, and user traffic only utilizes less than 5%. Since the authentication mechanism is turned off, such a low utilization of user traffic continues right through the flooding attack. Fig. 19(b) shows the throughput performance of the compromised wireless interface IP with the proposed authentication mechanism. When the SMR receives too much non-purposeful data and detects low wireless bandwidth utilization, the SMR informs the SAR about the compromised wireless interface IP address and seeks a new wireless interface to relay the service. The SMR changes the wireless interface IP address 6 times in this experiment which saves more than a half wireless bandwidth consumption during the flooding attack.

C. Performance Comparison and Randomness Test

We further compare the performance of our proposed authentication mechanism with both the hash chain based and the existing chaotic map based authentication mechanisms. Fig. 20 shows the communication overheads of these mechanisms measured by the number of interactions between the SMR and the SAR. For the existing chaotic map based mechanism, its communication overhead is at least two times of the hash chain based mechanism and our proposed solution. This is because of that the OTPs in the hash chain based mechanism and our proposed solution can be derived sequently using the original seed or initial states in the algorithms. In contrast, the existing chaotic map based mechanism needs to update the initial states timely when an OTP is sent and validated.

While the hash chain based mechanism has similar low overhead compared with our proposed approach, it is less secure than both our proposed approach and the existing chaotic map based mechanism when using the same OTP length. According to the definition of cryptosystem’s security level, if the fastest way to break the system is the exhaustive
key search and the key is an uniformly distributed random $N$-bit value, then the security level is traditionally said to be $N$. Therefore, using the same OTP length of $N$ bits and assuming that the OTPs behave like uniformly distributed random $N$-bit value in the existing mechanisms, the security level of the hash chain based mechanism is $0.5N$ [38] due to the birthday attack and the security level of chaotic map based mechanism is $N$. Although we have proven the randomness of our mechanism’s OTP in Section IV, here we test its randomness again using the NIST Statistical Test Suite [41]. We capture and use 100 groups of 1-Mb OTP streams. The corresponding test items and results are summarized in Table 1 which confirms the randomness of our RNG. These test items investigate the randomness of the OTP using different mathematical methods. Therefore, we can conclude that the security level of our mechanism is $N$.

![Graph](image1)

**TABLE I**

<table>
<thead>
<tr>
<th>NIST randomness tests</th>
<th>The average of P-value</th>
<th>Pass rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>0.5276</td>
<td>99%</td>
</tr>
<tr>
<td>Block Frequency</td>
<td>0.4645</td>
<td>98%</td>
</tr>
<tr>
<td>CuSum-F</td>
<td>0.5410</td>
<td>99%</td>
</tr>
<tr>
<td>CuSum-R</td>
<td>0.5620</td>
<td>96%</td>
</tr>
<tr>
<td>Runs</td>
<td>0.5253</td>
<td>98%</td>
</tr>
<tr>
<td>Long Runs of Ones</td>
<td>0.4619</td>
<td>98%</td>
</tr>
<tr>
<td>Rank</td>
<td>0.4694</td>
<td>97%</td>
</tr>
<tr>
<td>Universal</td>
<td>0.5371</td>
<td>100%</td>
</tr>
<tr>
<td>Approximate Entropy</td>
<td>0.4888</td>
<td>100%</td>
</tr>
<tr>
<td>Non Overlapping Template</td>
<td>0.5199</td>
<td>100%</td>
</tr>
<tr>
<td>Linear Complexity</td>
<td>0.5145</td>
<td>100%</td>
</tr>
<tr>
<td>Random Excursions</td>
<td>0.5288</td>
<td>98%</td>
</tr>
<tr>
<td>Random Excursions Variant</td>
<td>0.4887</td>
<td>97%</td>
</tr>
</tbody>
</table>

Fig. 21 shows the security properties of different authentication mechanisms. Since our OTP solution behaves like uniformly distributed random $N$-bit value, the only way to break the proposed authentication mechanism is by using the brute-force attack. With 16-Byte and 20-Byte OTPs, our authentication mechanism can withstand an exhaustive OTP search at the rate of $10^{38}$.

VII. CONCLUSION

In this paper, we examined the data delivery security of SCN-R with practical considerations in high-speed trains. We first concluded that an authentication mechanism was needed to protect SCN-R under replay/spoofing attacks and UDP flood attacks. However, since the lifetime of a connection session was short in our scenario, the existing authentication mechanisms that were unsuitable for our scenario due to their complicated handshake and lengthy procedure. We addressed the issue by seeking a lightweight approach for authentication. We proposed a new chaos-based random number generator to build the one-time used passwords. An efficient authentication mechanism was designed using a pair of random number generators. Our approach overcome some shortcomings of the existing lightweight authentication. Particularly, our approach addressed the vulnerability of the hash based approach and reduced the intercommunication overhead of the existing chaos-based approach. We implemented our solution and performed extensive experiments to show the effectiveness of our authentication mechanisms against attacks. We demonstrated that an attempt to compromise a wireless interface IP address can be detected and rectified to minimize the performance degradation.

While our proposed authentication solution was shown to be effective in our considered application, the solution is immediately applicable also to other scenarios where communication resources are very limited and connections are lossy such as IoT networks.

REFERENCES


