Signal Injection Test of Spoofing Attack to GNSS-Based Positioning in Railway Train Control

Jiang Liu[1,2,*], Bai-gen Cai[1,2], De-biao Lu[1,2] and Ying-ying Li[3]

[1]*School of Automation and Intelligence, Beijing Jiaotong University, Beijing 100044, China*

[2]*State Key Laboratory of Advanced Rail Autonomous Operation, Beijing Jiaotong University, Beijing 100044, China*

[3]*China Railway Signal and Communication Research and Design Institute Group Co Ltd, Beijing 100070, China*

Abstract: With the continuous development of the railway transportation system, train operation control is becoming more and more significant as the core to guarantee the operational safety and efficiency. Train control based on Global Navigation Satellite System (GNSS) is an important way to improve on-board sub-system autonomy and reduce the dependence on trackside facilities. However, the vulnerability of GNSS makes GNSS-based train positioning susceptible to the spoofing attack, which affects its ability to be used for novel train control systems. For this reason, it is of great significance to conduct specific test and evaluation for train positioning research, development, and applications. In this study, we construct an overall framework of spoofing injection test for GNSS-based positioning in train control, and analyze the detailed contents of test and evaluation, including spoofing attack configuration, test scenario design and generation, test dataset establishment and analysis, and typical evaluation metrics. In order to fully demonstrate the effectiveness of the proposed framework, a complete spoofing injection test environment is established. Through case studies concerning two typical spoofing modes, we successfully illustrate the effectiveness of the proposed scheme in testing and evaluating the spoofing tolerant capability and performance features of GNSS receivers dedicated to train positioning. Finally, we discuss the direction of subsequent trusted applications of GNSS in train control systems using the presented solution and platform. The results provide relevant ideas for the research of novel GNSS spoofing protection techniques for future intelligent railway systems.

Keywords: Satellite navigation, Railway transportation, Vehicle positioning, Spoofing, Injection test.

1. INTRODUCTION

Since 1990s, the PTS (Positive Train Separation) program in the U.S. has pioneered the application of Global Navigation Satellite Systems (GNSSs) in the positioning and state perception of railway trains. From the viewpoint of the development trend of scientific research, the U.S., the European Union and other countries have made a number of important advances in recent years in different levels of railway train operation control systems [1, 2]. Currently, many countries are constantly deepening the importance of GNSS system resources, including Global Positioning System (GPS), GLONASS, GALILEO and BeiDou Navigation Satellite System (BDS) [3]. As the development of GNSS constellations and services, satellite navigation has become a highly potential industrial field in the world to train operation control as a key direction in the field of railway transportation safety [4, 5]. The GNSS-based train positioning in a novel railway operation control system is capable of enhancing the autonomy level of the train-borne sub-system and enable the flexibility of a train-centric system scheme.

In view of the obvious functional continuity dilemma and environmental sensitivity of satellite navigation itself, many countries in the development of satellite navigation-based train control process always can't avoid facing the availability of GNSS positioning is limited, while the critical safety needs of the train control system cannot be neglected. Thus, the implementation of GNSS technology in the train control system would be constrained from the overall safety assessment and certification of the challenges [6, 7]. Without specific measures overcoming the limitations of the GNSS-alone-mode positioning, the existing GNSS-based train control system has to only play a role as an auxiliary means in the railway systems. In recent years, research works in the field of GNSS-based railway applications mainly focus on the optimization of the functional safety level by enhancing the availability of the positioning service through various multi-sensor fusion methods [8-10]. With the complexity of the open operating environment and the gradual expansion of the scale of the railway network, the signal interference threat that exists at the level of its information security has become an emerging theme in the field of GNSS applications in the railway industry. In view of the possible adverse impact of GNSS signal interference and intrusion against GNSS positioning, including GNSS jamming and spoofing, on the functional safety and efficiency, how to achieve effective defense against the information security

*Address correspondence to this author at the School of Automation and Intelligence, Beijing Jiaotong University, Beijing 100044, China;
E-mail: jiangliu@bjtu.edu.cn

Received on 03-08-2025 Accepted on 25-08-2025 Published on 26-08-2025

E-ISSN: 2409-9694/25

threats at the end-user level and ensure that the train positioning reaches the required level of performance (including accuracy, integrity, availability, safety, and resilience) has become a necessary way to achieve multi-level collaborative security under specific requirements of train control.

For the unintentional or malicious interference attack to GNSS-based train positioning, compared with the signal jamming attack, the spoofing attack is more concealment, and thus its hazards and corresponding means of protection are increasingly becoming a widespread concern in the application process. The research on anti-jamming direction for satellite navigation has put forward many anti-spoofing technology paths [11-13]. However, for the active defense against the potential GNSS spoofing attack in novel train control systems and other related railway applications, there are still many key issues need to be further resolved.

Firstly, there are many different realization modes of GNSS spoofing interference, and thus it will be difficult to pre-determine and obtain a priori knowledge in the real environment. For this reason, existing research on spoofing is difficult to effectively cover the various modes of spoofing that may occur in real operation, which makes it difficult to effectively improve the capability of anti-spoofing methods.

Secondly, there are different levels of mechanisms to cope with the spoofing attack, including spoofing detection, recognition, impact cognition, and interference effect exclusion. Existing research mainly focuses on the primary level of detection. For this reason, it remains to be explored by targeted research on how to further penetrate to the levels of spoofing attack mode identification and active suppression.

Thirdly, the train control system, as a service object of the GNSS positioning function, is in the process of upgrading to different railway lines. The emergence of new railway signaling concepts, like virtual coupling and group control of heavy-haul trains [14, 15], has put forward different needs for the performance of train positioning, especially the performance of train-to-train relative positioning, from the conventional system. For this reason, there is an urgent need to perform research on targeted countermeasures against the GNSS spoofing attack dedicated for group train control systems.

Considering this background, this paper takes into full consideration the practical needs of providing GNSS spoofing interference protection research for the whole life-cycle process of the group control system, and puts forward the research idea of “zero-on-site test” for GNSS spoofing attacks. The overall framework of the spoofing interference test system is designed. The implementation method for the core aspects of test and evaluation is analyzed. On this basis, combined with the group train positioning scenarios, two typical cases are investigated to present and analyze the results of a specific spoofing signal injection test platform, reflecting the actual effect of the test scheme designed in this paper. The results of this research will provide adequate support for the research on active protection against GNSS interference for novel railway train control modes.

2. TEST AND EVALUATION ARCHITECTURE

To address the specific requirements for positioning safety and trustworthiness in train control systems, conducting zero-on-site testing in a laboratory environment can effectively replicate various interference scenarios that may occur during actual operation, thereby evaluating and confirming the ability of a train positioning module to withstand the spoofing attack. In this section, we present the overall framework for signal injection testing in the laboratory and provide a detailed analysis to the key components. Based on this, we explain the GNSS positioning testing and evaluation process for corresponding train control system operation scenarios in conjunction with different spoofing attack modes.

2.1. Overall Framework

The process of conducting signal injection testing in the laboratory generally consists of two parts, including spoofing interference signal generation and the operation of the Receiver-under-test (RUT), which correspond to the two main behaviors of “attack” and “defense” in spoofing attacks. Figure **1** shows the overall framework of the signal injection test system that was constructed.

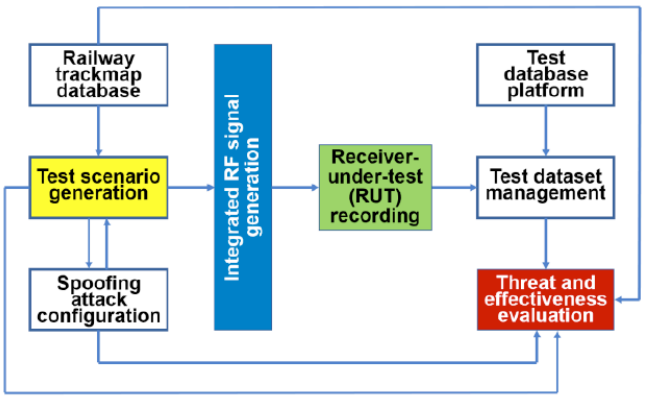

Figure 1: Overall framework of signal injection test system for GNSS-based positioning in group train control.

As shown in Figure **1**, “Integrated RF (Radio Frequency) signal generation” represents the attack

behavior in the test environment. It requires the utilization of a trackmap database to provide fundamental spatial information on the train's operation, combined with specific spoofing interference pattern settings to construct a precise test scenario. The test scenario provides the detailed "script" information, determining the following characteristics.

1. Dynamic operation characteristics of the train to which the positioning unit in the train control system belongs.
2. Scene characteristics of the target railway line.
3. Satellite navigation observation characteristics that are influenced by both the GNSS constellation and the targe railway train.
4. Behavior characteristics of the spoofer and the spoofing interference attack.

The RUT serves as the target object for receiving and acquiring RF signals from the attacker, performing positioning calculations and reflecting the extent and consequences of positioning spoofing on the train. Using the RUT positioning calculation results, test evaluation data samples can be effectively established. A large number of sample data containing RUT positioning calculation information-based characteristics can be collected to form corresponding test datasets. The datasets, when combined with prior knowledge such as test scenario data and spoofing attack settings, can be used to quantitatively evaluate and verify the interference protection performance of the RUT, thereby providing support for selecting appropriate GNSS receivers for the train control systems, optimizing anti-spoofing design, and conducting spoofing interference event analysis.

2.2. Spoofing Attack Configuration

Test scenario generation module and the integrated RF signal generation module, as shown in Figure **1**, have the ability to configure and generate both pure GNSS satellite signals and spoofed signals. The structure of the spoofed signals can be consistent with the pure GNSS signals, but the signal characteristics and information entities carried are different. Typical GNSS spoofing signal attacks that could be utilized in spoofing injection test can be configured in the following three forms.

1. Trajectory spoofing

Trajectory spoofing is the most direct and simple way to induce GNSS receivers. Under the trajectory spoofing injection test configuration, a test operator can configure a certain number of counterfeit satellite signals and import spoofing trajectory script files into the scenario using specific software tools such as SimSAFE. The spoofing signals corresponding to the target satellites use specific channels of the RF signal generation module as transmission channels, so that it broadcasts counterfeit signals that mimic genuine GNSS transmissions. By adjusting the power level of the spoofing signals to overpower authentic signals from satellites, counterfeit satellite signals can intrude into the RUT's acquisition and tracking process, thus making the positioning calculation results converge to the target spoofing trajectory and deviate from the original truth.

2. Pseudo-range spoofing

In the configuration of pseudo-range-type spoofing injection test, a certain number of counterfeit satellite signals, which have the same satellite Psuedo-Random Noise (PRN) numbers, orbit parameters and navigation message information as real satellites, need to be configured by choosing the condition with a well-matched satellite constellation in conjunction with the temporal and spatial status of the train's operation. The scenario configuration tool is able to set the pseudo-code of the spoofing satellites. By adjusting the power level of the spoofed signals and realizing the power advantage, RUT will be to hijacked to lock on to the corresponding spoofing signals, which would result in misleading or even completely wrong positioning solution.

It is worth noting that the pseudo-range spoofing interference setup requires the identification of an explicit pseudo-range changing mode, which defines deviation pattern of the desired virtual satellite signal corresponding to the pseudo-range observation information. Commonly used changing modes can be abstracted to specific signal types, including offset-mode, incremental-step mode, ramp-mode, sinusoidal-mode, and so on. In addition to these common modes, a wider range of pseudo-range variations can be defined by the user, making it difficult for the RUT to fully preform a prevention mechanism.

3. Time spoofing

In the time spoofing injection test configuration, by setting a certain number of spoofing satellites, the scenario configuration tool is able to set the clock drift of the target counterfeit satellites. Fake signals generated by the target spoofing satellites use specific channels of the RF signal generation module as transmission channels. By adjusting the power level of the broadcasted counterfeit signals, a time-spoofing attack would achieve the effect of misleading the receiver to decode it.

2.3. Test Scenario Design and Generation

The scenario design for GNSS spoofing injection test of railway train positioning is significantly different from the conventional test and evaluation carried out only from the level of satellite navigation, and it needs to take into full consideration the train operation characteristics, the environment along the railway line, the working mode of the object train control system and other related factors. Combined with the overall framework shown in Figure **1**, the trackmap database provides the basic constraints of the train's running path for the whole test environment. On this basis, the design and preparation of the test scenario scripts need to focus on two specific aspects.

1. Constraints of train control system modes on train positioning function scenarios

With the continuous development of train control techniques and systems, different types of train control modes with different applicability have been gradually developed for typical railway types, such as low/medium-density lines, high-speed lines, and heavy-haul freight lines. In these system modes, connotations of positioning, physical distribution of positioning functions, and the definition of performance requirements are different, which provide a priori scenario constraints for carrying out dedicated GNSS spoofing interference tests. From the perspective of the specific form of GNSS used for train control, the representative train control system modes can be focused on the following two types as Figure **2**.

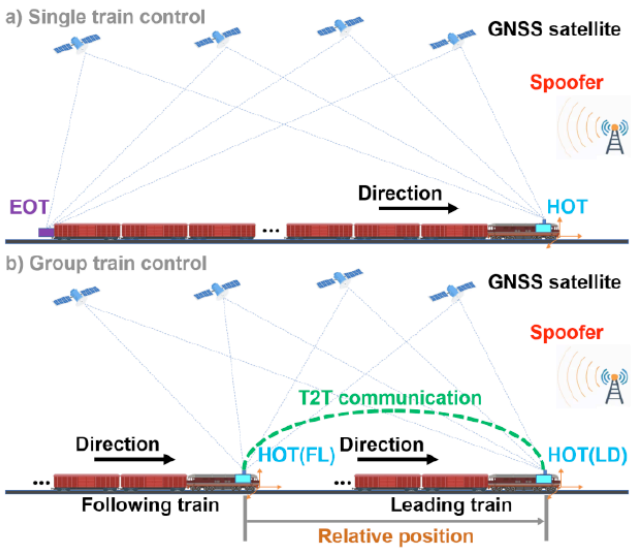

Figure 2: GNSS-based train positioning under spoofer-affected conditions with different train control system modes.

(a) GNSS positioning under single train control mode

For single-train operation control, in order to ensure the safety of train operation or to realize the moving block tracing control, it will be necessary to obtain the position estimation of the front end of the train as well as the rear end. For this purpose, GNSS receivers will be adopted by both the Head-of-train (HOT) equipment and the End-of-train (EOT) equipment, respectively. The HOT and EOT receivers, with different positions in the train, have significantly different operating characteristics and GNSS signal observation conditions. In addition, they may also differ in the degree and character of their influence by the spoofer around the railway line. Therefore, these factors need to be fully considered in the design of the spoofed injection test scenarios.

(b) GNSS positioning under group train control mode

For heavy haul freight line transportation, group train control system has become a key direction of research and development in recent years. In this control mode, multiple heavy-haul trains are no longer individually controlled, but are virtually coupled together to form group(s) for the overall operation control. In the group control mode, elements of the traditional single-train oriented train positioning scenarios are still present. At the same time, it is also necessary to further consider the need for real-time determination of the relative position between trains in order to maintain a relatively stable and close virtual-chain configuration of multiple trains within the group. As shown in Figure **2**(**b**), the Train-to-train (T2T) communication maintains the information link between the HOT equipment in the leading train (LD) and following train (FL) in the cluster. For this reason, the high-precision and real-time relative baseline determination becomes an additional requirement. This characteristic needs to be taken into account in the design of the test scenario by integrating the dynamics of multi-train operation.

2. Space-time alignment requirement between train operation and GNSS signal mask profiles

The design of the test scenario needs to pay attention to both the dynamic running characteristics of the train and the observation characteristics of the in-space satellite signal. These two types of features can be consistently associated with each other in the two dimensions of position and time, so that the test scenario will be rich in feature information and reflects the specific conditions of train positioning as realistically as possible.

On the one hand, dynamic train operation profile can be presented through two types of information,

including train operation plan and train speed profile. As shown in the upper part of Figure **3**, the train operation plan provides the macroscopic time constraints of the train during its departure and arrival at stations. At a higher resolution level, the speed-distance curve further characterizes in detail the dynamics of the train at each moment in time, which reflects the result of the change of the train's position along the track over time under the speed limit and different operating conditions, including traction, cruising, coasting, braking, etc.

On the other hand, as shown in the lower part of Figure **3**, environmental characteristics of the train-borne receiver antenna at each specific location and moment will greatly affect the reception and processing results of real GNSS signals and spoofing signals. The signal mask profile, combined with the GNSS ephemeris data, is able to specifically determine the visibility of the GNSS satellite signals and distinguish between the real satellites and the counterfeit ones in the test scenarios.

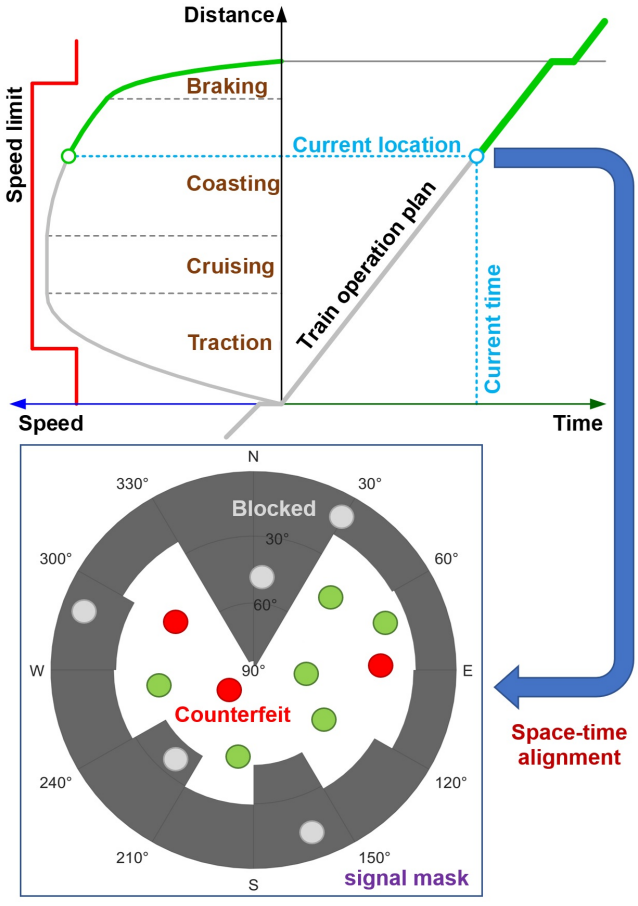

Figure 3: Space-time alignment between train operation profile and GNSS signal mask profile.

All the information from the two types of profiles can be integrated to provide an effective basis for flexible configuration of spoofing attack behavior that is expected to be involved in the tests. In order to correctly associate the two types of features in the test scenario generation, it is necessary to map the information effectively based on the principle of space-time alignment.

2.4. Test Dataset Establishment and Analysis

The observation and calculation information output from the RUT can be used to construct and accumulate test datasets that can be used for evaluation and analysis. Combining the test scenario information can provide the necessary referencing information and spoofing labels for the datasets. For this reason, the key to the realization of each sample record is to quantitatively clarify the features. With GNSS receiver data, different types of sample features can be designed considering three categories according to the information processing stage.

1. Signal domain features

Signal domain features are mainly obtained by acquiring the digital Intermediate Frequency (IF) data and implementing corresponding Software-defined-receiver (SDR) based navigation calculation to obtain the relevant features in signal capture, tracking and other processing stages. Typical signal domain features include the code phase difference, carrier phase difference, Time-domain Cross Ambiguity Function (TCAF), Signal Quality Monitoring (SQM) metrics, TCAF characteristics (maximum TCAF and average power deviation) and so on. The acquisition of such information requires the processing of large GNSS digital IF data files and the implementation of specific receiver signal processing solutions, which needs a relatively large amount of work. Therefore, key characteristics in the signal domain can be used selectively according to the demand supported by the test and evaluation.

2. Observation domain features

Observation domain characteristics mainly reflect specific features of the visible satellite constellation and the degree of deviation of the characteristics due to the spoofing injection. In terms of satellite constellations, the Carrier-to-noise-power-spectrum-density-ratio (C/N_0) most directly reflects the signal strength of each visible satellite, which can be used to reveal the possible differences between real and counterfeit satellites in terms of signal strength levels. The Dilution-of-position (DOP) values, including Horizontal (HDOP), Vertical DOP (VDOP) and Position DOP (PDOP), reflect the spatial distribution of visible satellite constellations, and can also indicate the effect of spoofing attack under specific spoofing behavioral patterns when the spoofing signals change the status

of the visible constellation. In addition, at the level of observation quantities, effects of spoofing interference on the observation process can be explored from the residuals of multiple types of measurements, such as pseudo-range, pseudo-range-rate and the carrier phase. Taking the pseudo-range residual as an example, the physical meanings can be expressed as

$$\eta_i(t) = \rho_i^M(t) - \rho_i^E(t) = [\rho_i(t) + \rho_i^{SP}(t)] - \rho_i^E(t) \quad (1)$$

where $\eta_i(t)$ indicates the pseudo-range residual of the i th visible satellite at time instant t, $\rho_i^M(t)$ is the pseudo-range measurement, $\rho_i(t)$ is the real pseudo-range (also can be the calibrated one), $\rho_i^{SP}(t)$ denotes the deviation caused by the injected spoofing (only for the counterfeit satellite), and $\rho_i^E(t)$ represents estimated pseudo-range measurement.

With the exception of the DOP values, the other main features are associated with individual satellite signal channels. Therefore, the effect of dynamic changes in the number of visible satellites needs to be concerned in the sample data generation process.

3. Localization domain features

The corresponding features within the localization domain reflect more intuitively the influence of spoofing interference at the level of the train position calculation results. Based on the scenario truth or specific reference data, we are encouraged to quantify the position deviation of RUT in the along-track direction, cross-track direction and the three-dimensional ECEF coordinates. With such information, a complete feature set together with all those mention features can be established.

2.5. Evaluation Metrics

The critical safety requirement of train control system and the performance need for train speed/location determination provide top-level constraints for carrying out GNSS spoofing interference-oriented testing and evaluation. However, different from the conventional train positioning module development scheme and functional safety scenario-oriented testing, considering the mapping of threats caused by GNSS spoofing at the information security level in the functional safety domain and positioning performance domain, it is of great necessity to integrate the commonly used GNSS-domain indicator system with the railway dedicated Reliability, Availability, Maintainability and Safety (RAMS) indicator system. At present, there is still no unified and railway-dedicated performance evaluation specification. For this reason, the conventional GNSS Required Navigation Performance (RNP) performance system is extended, and the following key indicators can be focused on quantitative assessment in the analysis of train positioning test datasets.

1. Accuracy

Accuracy is the most basic indicator to evaluate the degree of conformance between the position reported by the RUT and the true position from the test scenario. It can be quantitatively described by the position error as

$$e_q(t) = \rho_q(t) - \bar{\rho}_q(t) \quad (2)$$

where $e_q(t)$ represents the q th error component at t under a specific position frame system, $\rho_q(t)$ and $\bar{\rho}_q(t)$ denote the RUT derived position component and its truth or a reliable reference value.

Specifically, the Along-track (AT) position error and the Cross-track (CT) error would be investigated for the train positioning case under the 1D along track position frame system compared with the 3D ECEF system. In addition, accuracy is usually a statistical value that is specified at a given confidence level, *e.g.*, 95%.

2. Spoofing tolerance

Spoofing tolerance reflects the trust that can be placed in the correctness of the positioning results from the RUT under different probable GNSS spoofing attack conditions. It is expected that an advanced RUT with sufficient anti-spoofing capability is able to provide Position, Velocity and Timing (PVT) output and always satisfy the performance needs of a train control system, *e.g.* position error below a given threshold.

3. Alarm capability

Considering that the RUT cannot effectively tolerate all the spoofing attack conditions, under the demand of information security guarantee, the train control system requires the train positioning module to be able to deliver a spoofing intrusion alarm when it suffers from spoofing interference and the GNSS receiver can no longer give correct and credible positioning results. With the alarm information, the train positioning module can make timely and effective disposition of GNSS receiver information to prevent the untrustworthy or even misleading positioning information from influencing the decision-making of the overall train positioning module.

The alarm capability can be reflected by two metrics.

(1) Time-to-alarm

It can be evaluated by the maximum allowable time between an alarm condition occurring and the alarm being present at the output.

(2) Alarm risk

It describes the probability that a RUT fails to trigger an alarm correctly within the time to alarm when it is no longer able to resist the injected GNSS spoofing interference and experiences unacceptable degradation.

4. Continuity

Continuity is defined as the probability that the RUT is able to determine the train position within the specified accuracy level and is able to detect and proactively protect against the intrusion of probable GNSS spoofing attacks over the operation time.

5. Availability

Availability indicates the probability that the RUT is operating satisfactorily at any point in time under the test scenario with specifically injected spoofing conditions.

3. TEST AND ANALYSIS

In order to implement and verify the spoofing signal injection test scheme proposed in this paper, a complete test environment was set up in the laboratory, as shown in Figure **4**. As can be seen in the figure, the overall test environment mainly consists of three parts, including the test instrument, the system under test, and the display control system.

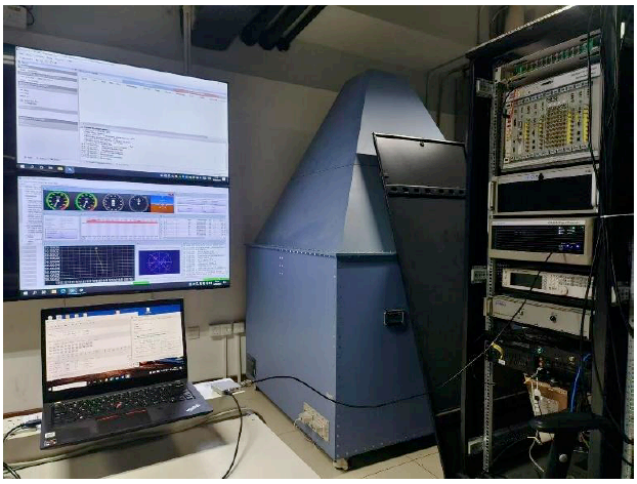

Figure 4: Spoofing injection test environment in laboratory.

1. Test instrument

Test instrument is the core of the overall environment. It primarily performs the functions mentioned in Figure **1**, including spoofing attack configuration, test scenario generation, and RF signal generation. Through an upper-level processing terminal serving as the management and control system for the entire environment, it calls upon railway trackmap data and scenario script files, and drives the RF signal generation device to transmit mixed signals containing pure GNSS signal and spoofing interference signals. Test scenario generation is essential to ensuring that RUT operates under conditions closely resembling real-world operational processes. To achieve this, it is necessary to fully utilize fundamental data provided by the trackmap database and the train operational dynamic profile to create test signals that conform to the train's dynamics, railway line environmental characteristics, and satellite/spoofing signal observation models.

2. System under test

RUT is the core of the system under test, responsible for receiving and processing test signals and reflecting the effects of spoofing interference in its own positioning calculation process and results. Under the same spoofing interference condition, different RUTs may exhibit differentiated performance characteristics. On the one hand, the differences in results can reflect the strength and scope of the spoofer's actions, and on the other hand, they also reflect the ability of the RUT device to resist the spoofing attack. In addition to the RUT device, a host computer is required to record and store the receiver data. Furthermore, to capture the characteristics of signals received by the RUT at the signal level, an IF signal acquisition device combined with an SDR also can be used as the RUT to build the required test datasets.

3. Display control system

Display control system is responsible for centrally displaying the operation and execution interface of the test instrument and the system under test to the test execution operators, and providing process information on the running scenario to achieve human-machine interaction for test operations.

Using this test environment, script of a single train positioning scenario is constructed using the practical railway operation data logs, which contains the signal observation scenario information of multiple GPS satellites. In the settings of the spoofing interference, two pseudo-range spoofing modes, including *offset* and *incremental-step* spoofing attack modes, are selected to inject interference in the pure GPS signal, and the Ublox M8T receiver is adopted as the RUT to collect test dataset. The corresponding test evaluation and analysis results are shown as follows.

3.1. Test Under Offset-Spoofing Mode

At the RF signal generation end, the SimSAFE tool is used to configure the spoofing configuration command. The *offset* spoofing mode is selected. Six of the visible satellite channels in the operational scenario, PRN=10,14,20,31,32, are selected to inject a constant offset from the 600s after the test startup operation. In this spoofing attack mode, an offset of 240m is added to the original-scenario-defined pseudo-ranges of the spoofed satellite channels. At the same time, the spoofing signal power is set to be increased by 0.1 dB/s. By setting the gradually increasing spoofing interference behavior in terms of both the pseudo-range and interference power, the RUT is expected to be spoofed gradually by the corresponding channels. With the gradual increase of the spoofing signal power level, the RUT is expected to be affected by the spoofing attack in operation by receiving and processing the spoofing signals, leading to noticeable degradation of positioning performance. Figure **5** depicts the trajectory of the train by the RUT under the offset-spoofing attack test scenario, where the trajectory under the non-spoofing condition is also given for the purpose of comparison.

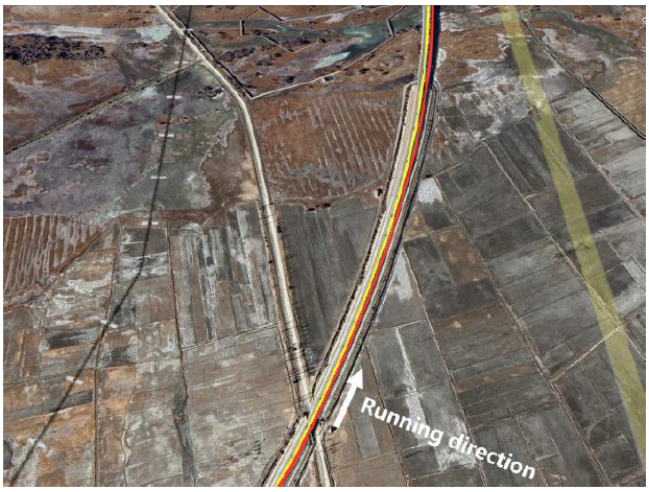

Figure 5: Trajectories under non-spoofing and offset-spoofing-attack scenarios (Yellow: non-spoofing, Red: spoofing affected).

From the Figure **5**, it can be seen that the injection of spoofing interference leads to a significant shift of the train trajectory obtained from RUT compared with the non-spoofing condition. In order to further quantitatively assess the impact of the spoofing attack on the signal processing and RUT performance, the relevant feature quantities related to the quality of the navigation observations are demonstrated and analyzed in conjunction with the process of constructing the test datasets. Figure **6** and Figure **7** show the variation of parameters such as C/N_0 and DOP value of all the six channels that are stably visible to the RUT during the test. It has to be noted that, based on the satellite ephemeris data loaded according to the test scenario and the test time, the actually observed satellites are with PRN=10, 12, 20, 21, 25, and 32. Among these, the three satellites involved in the spoofing injection settings (PRN=10, 20, 32) were observed by RUT during the test and played a deceptive role, while the two pre-set spoofing satellites (PRN=14, 31) were not tracked by RUT and were not utilized in the final navigation calculation. Figure **8** and Figure **9** present the results of reference pseudo-range residual and pseudo-range-rate residuals over time, respectively. From the above results, it can be seen that the injection of the fixed-offset spoofing component and the gradual increase of the spoofing power cause the RUT to gradually track to the spoofing signals since the beginning of the interference injection. The RUT undergoes a significant change in the satellite signal observation status and the measurement features.

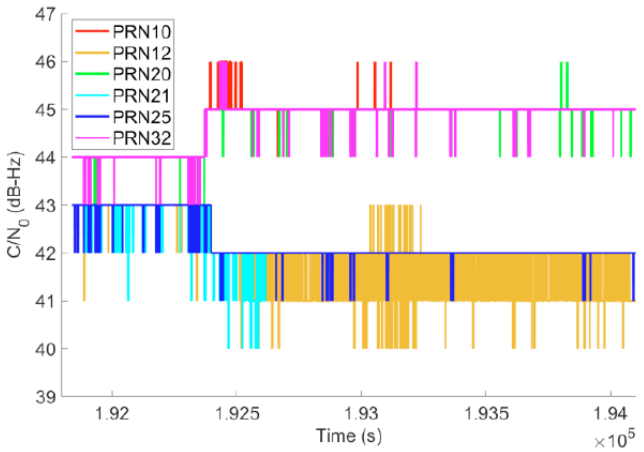

Figure 6: C/N_0 values of all GNSS satellite channels under offset-spoofing-attack scenario.

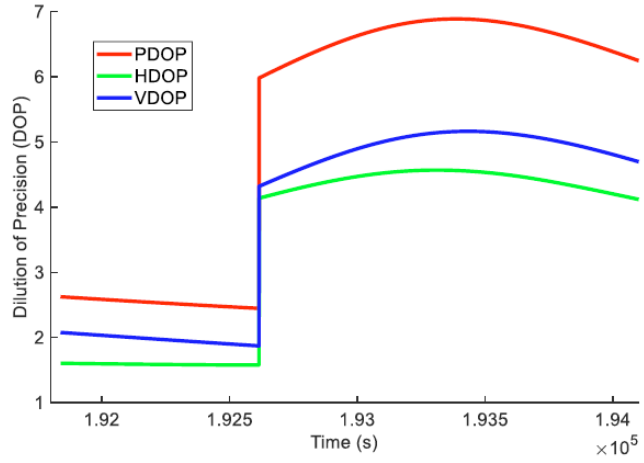

Figure 7: DOP values under offset-spoofing-attack scenario.

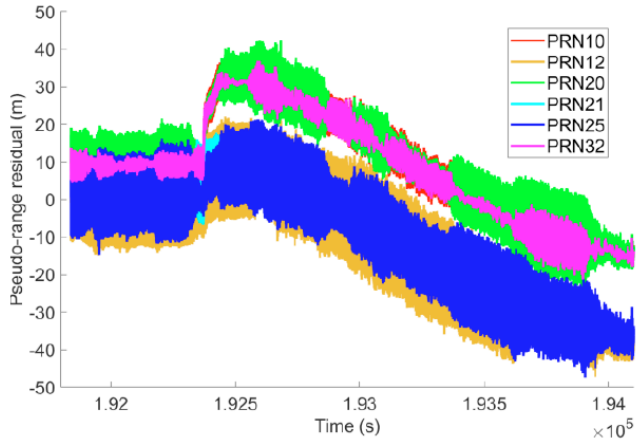

Figure 8: Pseudo-range residuals of all satellite channels under offset-spoofing-attack scenario.

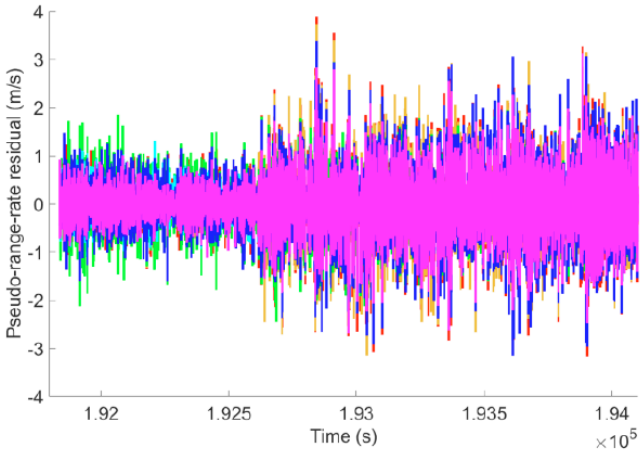

Figure 9: Pseudo-range-rate residuals of all satellite channels under offset-spoofing-attack scenario.

As described in Sec. 2.5, many performance factors can be considered for evaluating the impact of spoofing interference. Here, the most direct localization accuracy is used to analyze the extent to which the RUT localization performance is affected under the *offset* mode attack scenario. Figure **10** illustrates the 3D position error of RUT over time. It can be seen that in the initial stage of spoofing injection, navigation calculation of the RUT is interrupted for part of the time period, reflecting that the continuity of localization functionality is impaired because the spoofing signals gradually occupies the receiver channels. After the RUT has stabilized the tracking of spoofing signals, it starts to work continuously and normally, but the position accuracy level is affected to a certain extent, and the deterioration tendency is particularly obvious in the Z-axis direction.

Combined with the test results, it can be seen that under the *offset* mode spoofing condition, the average 3D errors by the RUT reach 1.53m, 39.05m, and 15.51m respectively, which are obviously far beyond the requirements of the train control system for positioning accuracy. For this reason, the involved RUT cannot be used independently to implement train positioning in the environment with GNSS spoofing interference, and other metrics than the accuracy mentioned in Sec. 2.5 are not further investigated any more. For possible applications in the train positioning module, this receiver must be enhanced by advanced anti-interference GNSS devices or compensated by other assistant sensors.

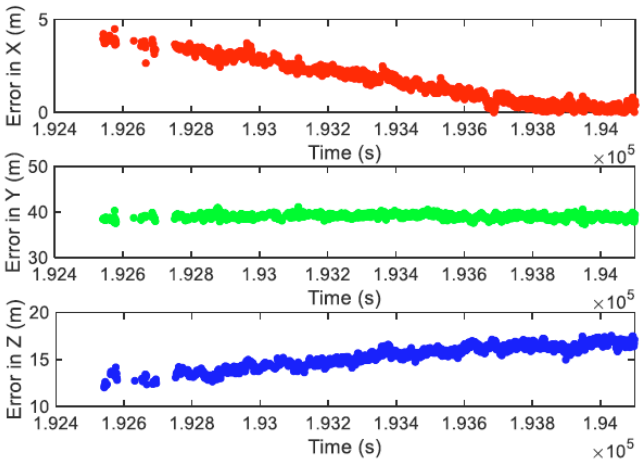

Figure 10: Position errors under offset-spoofing-attack scenario.

3.2. Test Under Incremental-Step-Spoofing Mode

Considering to further complicate the attack behavior and to achieve a gradual spoofing signal signature, the *incremental-step* spoofing mode is configured in the SimSAFE tool. Using the same settings as the *offset* mode, spoofing injection is also performed for the five target satellite channels in this scenario. The difference with the *offset* mode is that the injection of pseudo-range deviation adopts a gradual self-incremental behavior, which means an increasing deviation with an increment of 0.06m over the previous moment (T=1s) is added to the current pseudo-range of all the spoofed satellite channels. At the same time,

Figure 11: Trajectories under non-spoofing and incremental-step-spoofing scenarios (Yellow: non-spoofing, Red: spoofing attack affected).

the spoofing signal power is also set to increase by 0.1 dB/s. With the gradual increase of both the pseudo-range deviation and the spoofing power strength, more serious degradation of positioning performance over the simple *offset* mode is expected. Figure **11** depicts the trajectory of the train by the RUT under the *incremental-step* spoofing scenario with the referencing trajectory under the non-spoofing case.

From Figure **11**, it can be seen that the train trajectory offset caused by the *incremental-step* mode spoofing interference is more significant relative to the *offset* mode shown in Figure **5**. Compared with the reference trajectory under the non-spoofing condition, the trajectory obtained from the RUT solution has significantly deviated from the spatial range of the mainline track. In order to further reflect the impact of *incremental-step* mode spoofing interference at the level of satellite observation quality, the above four types of characteristics are demonstrated separately. Figure **12** and Figure **13** show the variation of C/N_0 and DOP values with time, respectively. The reference pseudo-range residuals and pseudo-range-rate residuals over time are illustrated in Figure **14** and Figure **15**, respectively.

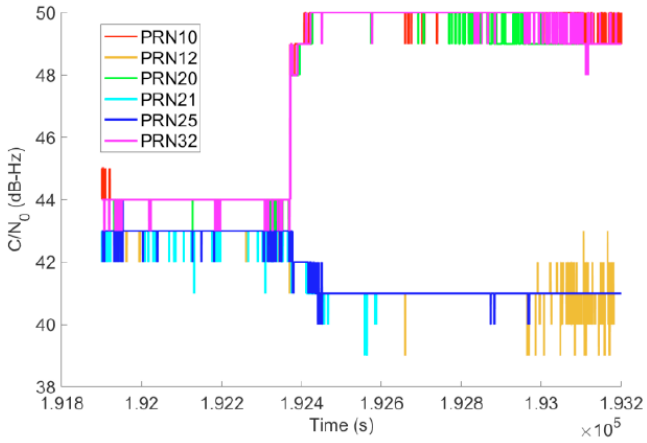

Figure 12: C/N_0 values of all GNSS satellite channels under incremental-step-spoofing-attack scenario.

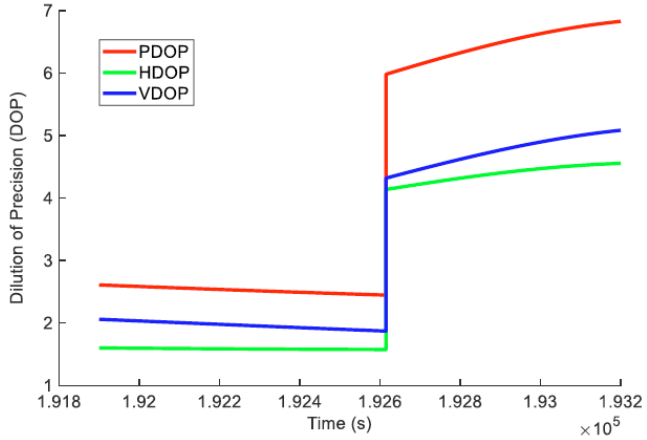

Figure 13: DOP values under incremental-step-spoofing-attack scenario.

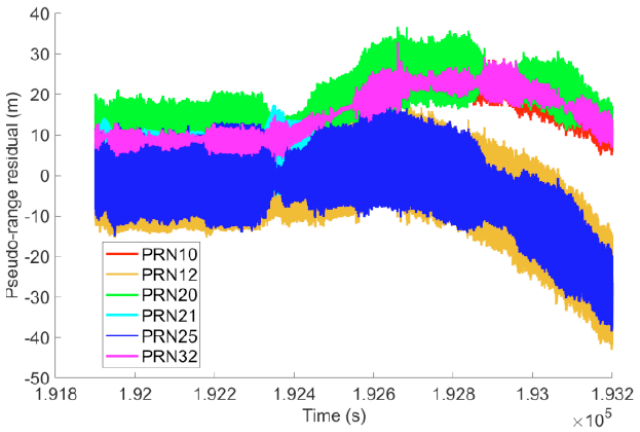

Figure 14: Pseudo-range residuals of all satellite channels under incremental-step-spoofing-attack scenario.

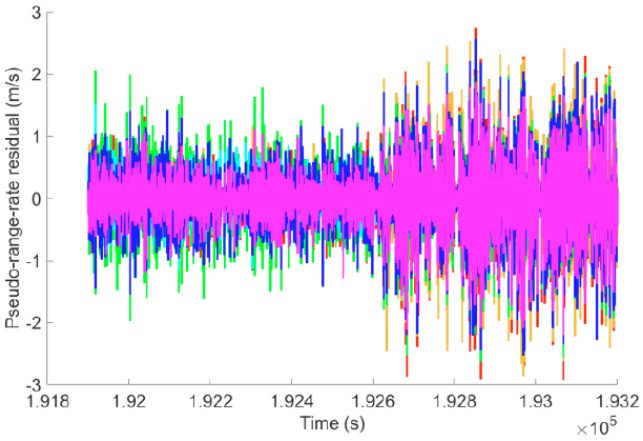

Figure 15: Pseudo-range-rate residuals of all satellite channels under incremental-step-spoofing-attack scenario.

From the above results, it can be seen that with the injection of spoofing signals, a sensitive response of the receiver can be clearly seen in the observation quality-related indicators, such as C/N_0. Three spoofing signals (PRN=10,20,32) are tracked by RUT into the navigation calculation process, and it can be clearly seen that their intensities are much higher than those pure satellite channels. Correspondingly, the level of variance of the pseudo-range and pseudo-range-rate residuals also increases significantly with respect to the fixed-level *offset* spoofing mode. In particular, the absolute values of the pseudo-range residuals for some of the channels (PRN=12,25) are approaching a high level over 100m beyond the time period scope of Figure **14**, which will lead to a significant impact on the RUT position estimation performance. Figure **16** gives the 3D errors over time, where the mean values reach 2.25m, 27.67m, and 10.22m, respectively. Although the level of average errors does not increase significantly with respect to the *offset* spoofing case, the temporal development trend of errors shows a very precise asymptotic increase characteristic. It can be predicted that the growth of errors will continue during the following RUT operation, causing continuous deterioration of the positioning performance.

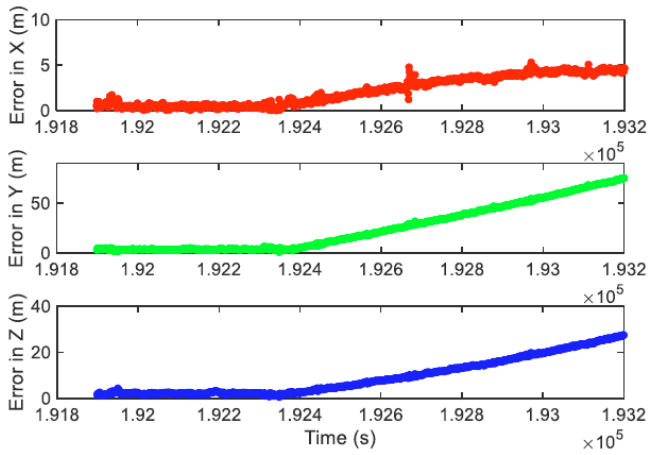

Figure 16: Position errors under incremental-step-spoofing-attack scenario.

Through the above analysis, it can be seen that the *incremental-step* mode, as a typical GNSS pseudo-range spoofing case, is characterized by the trend evolution and cumulative effect. Obviously, the RUT involved in this test fails to effectively resist the influence of this kind of spoofing interference. It suffers from the biased guidance under the effect of spoofing injection, resulting in time-varying growth deviation of the positioning calculation results. The performance of the RUT cannot meet the requirements of train control on the performance of GNSS receiver. For this reason, timely and effective detection of the existence of such progressive spoofing and appropriate suppression or exclusion of the interference effect will be crucial to ensure safety and trustworthiness of the entire train positioning module.

4. DISCUSSION

This paper analyzes the spoofing signal injection testing for GNSS-based train positioning, focusing on the overall framework, core elements, and implementation cases. Results from the corresponding cases demonstrate the effects of spoofing interference on the evaluation characteristics under the given spoofing attack modes. However, it is foreseeable that the forms and possibilities of spoofing interference threats that train control systems may encounter in the real-world environments are diverse, and their behavioral characteristics may be more complex. Therefore, within the framework shown in Figure **1**, on one hand, further exploration can be conducted by enriching test scenarios and increasing the diversity of spoofing signal injection modes. On the other hand, targeted protection measures can be developed based on the assessment of attack threat and RUT performance, and further investigation can be conducted from multiple aspects as follows.

4.1. Application of Advanced Learning Methods

Conducting zero-on-site tests under multiple scenarios and different spoofing types can yield a large amount of test sample data. As the dataset continues to expand, the amount of information it contains regarding the characteristics of spoofing attack behavior will also increase. Therefore, fully exploring the patterns reflected in the sample datasets regarding how train positioning performance is affected by spoofing will be significant for establishing appropriate countermeasures against the GNSS attack. Advanced artificial intelligence methods, such as machine learning and large-scale models, are with great potentials to provide important conditions for fully leveraging the capabilities of large sample datasets. Current research has already employed supervised learning solutions to establish associations between interference-related feature metrics and the degradation of train positioning performance. In the future, the introduction of more advanced intelligent methods will enable deeper proactive cognition and understanding of spoofing scenarios, thereby making it possible for a train positioning system to acquire the proactive reasoning and decision-making capabilities.

4.2. Enhancement Through Multi-Sensor Fusion

Under the stringent requirements of train control systems, the train positioning system with GNSS must adopt a redundant architecture, similar to other train-borne components, to enhance system reliability and safety. Conventional research and system design widely adopt multi-source sensor fusion strategies, integrating non-GNSS sensors, such as odometer, image sensor, and LiDAR, to compensate for scenarios where GNSS availability is constrained or GNSS performance is degraded. Therefore, considering the possibility of GNSS being subjected to spoofing attacks, the train positioning system must be able to detect the presence and evaluate the impact of spoofing interference early, which is important to prevent spoofing-affected GNSS information from being used in multi-sensor fusion. Non-GNSS sensors, which are unaffected by GNSS spoofing, can provide rich reference information for the GNSS receiver. Thus, by incorporating strategies such as channel-to-channel comparison and spoofing detection and warning on top of the basic multi-source information fusion logic, the value of non-GNSS sensor information can be further leveraged, thereby enhancing the overall capabilities of the train positioning system.

4.3. Infrastructure-Assisted Threat Monitoring

Current research on spoofing interference protection for railway train positioning primarily focuses

on on-board equipment, aiming to enhance the ability to detect and identify spoofing interference through the overlay and enhancement of on-board information processing logic layers. For train control systems operating within large-scale railway transportation networks, relying solely on on-board detection and feedback is still insufficient to achieve precise and accurate situational awareness across the entire railway network. Therefore, expanding from individual trains to the regional railway network scope, and constructing dedicated electromagnetic environment monitoring infrastructure to continuously inspect the GNSS interference threat level in the areas surrounding railway lines, will also be a significant topic to provide extensive support for a wider range of railway systems beyond GNSS-based train control.

4.4. Spoofer Identification and Localization

As the socio-economic environment continues to evolve, the causes and effects of GNSS spoofing around railway areas will become increasingly complex. To proactively address interference incidents, in addition to strengthening protective measures on the affected GNSS receivers, it is also of great necessity to develop effective methods to accurately identify and diagnose the location of the interference source. Proactively identifying the spoofers can help eliminate risks at the source edge and strengthen spatial electromagnetic security management along railway lines. To this end, utilizing a dedicated spoofing injection test environment to conduct more detailed analyses of GNSS spoofers' behavior can better leverage the support provided by zero-on-site testing for the security of railway GNSS applications.

5. CONCLUSION

In this study, we investigate and implement a signal injection test framework for zero-on-site testing of GNSS spoofing attack for railway train positioning. Details of the framework have been introduced from both the spoofing attacker and RUT sides. In order to demonstrate the effect of GNSS spoofing attack on train positioning, two typical cases are studied to reveal the performance affected by the attack and performance of the RUT. In the final stage, discussions on the utilization and developing directions of the GNSS spoofing injection test scheme are made, which provide a valuable reference for the future related research.

ACKNOWLEDGMENT

This research was funded by National Key Research and Development Program of China (2023YFB3907301), National Natural Science Foundation of China (62027809, T2222015).

CONFLICTS OF INTEREST

No potential conflict of interest was reported by the author(s).

REFERENCES

[1] Singh P, Dulebenets M, Pasha J, Gonzalez E, Lau Y, Kampmann R. Deployment of Autonomous Trains in Rail Transportation: Current Trends and Existing Challenges [J]. IEEE Access, 2021, 9: 91427-91461. https://doi.org/10.1109/ACCESS.2021.3091550

[2] Ait A, Eliasson J. European Railway Deregulation: An Overview of Market Organization and Capacity Allocation [J]. Transportmetrica A: Transport Science, 2022, 18(3): 594-618. https://doi.org/10.1080/23249935.2021.1885521

[3] Shu Y, Xu P, Niu X, Chen Q, Qiao L, Liu J. High-Rate Attitude Determination of Moving Vehicles with GNSS: GPS, BDS, GLONASS, and Galileo [J]. IEEE Transactions on Instrumentation and Measurement, 2022, 71: 1-13. https://doi.org/10.1109/TIM.2022.3168896

[4] Chrzan M, Ciszewski T, Nowakowski W. Selected Applications of Satellite Technologies in Rail Transport [J]. Archives of Transport, 2024, 71(3): 91-105. https://doi.org/10.61089/aot2024.z1bfx011

[5] Steuer M, Burdzik R, Piednoir F. Implementation of Global Navigation Satellite Systems in Railway Traffic Control Systems: Overview of Navigation Systems, Application Areas, and Implementation Plans [J]. Applied Sciences, 2025, 15(1): 356-356. https://doi.org/10.3390/app15010356

[6] Himrane O, Beugin J, Ghazel M. Implementation of a Model-oriented Approach for Supporting Safe Integration of GNSS-based Virtual Balises in ERTMS/ETCS Level 3 [J]. IEEE Open Journal of Intelligent Transportation Systems, 2023, 4: 294-310. https://doi.org/10.1109/OJITS.2023.3267142

[7] Wu Z, Liang C, Zhang Y. Blockchain-based Authentication of GNSS Civil Navigation Message [J]. IEEE Transactions on Aerospace and Electronic Systems, 2023, 59(4): 4380-4392. https://doi.org/10.1109/TAES.2023.3241041

[8] Elsanhoury M, Koljonen J, Välisuo P, Elmusrati M, Kuusniemi H. Survey on Recent Advances in Integrated GNSSs Towards Seamless Navigation Using Multi-Sensor Fusion Technology [C]. The 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2021), 2021, pp. 2754-2765. https://doi.org/10.33012/2021.17961

[9] Zhu J, Zhou H, Wang Z, Yang S. Improved Multi-Sensor Fusion Positioning System based on GNSS/LiDAR/Vision/IMU With Semi-Tight Coupling and Graph Optimization in GNSS Challenging Environments [J]. IEEE Access, 2023, 11: 95711-95723. https://doi.org/10.1109/ACCESS.2023.3311359

[10] Cho S, Chae M, Shin K. Reliability Analysis of the Integrated Navigation System Based on Real Trajectory and Calculation of Safety Margin Between Trains [J]. IEEE Access, 2021, 9: 32986-32996. https://doi.org/10.1109/ACCESS.2021.3061070

[11] Meng L, Yang L, Yang W, Zhang L. A Survey of GNSS Spoofing and Anti-Spoofing Technology [J]. Remote Sensing, 2022, 14(19): 1-24. https://doi.org/10.3390/rs14194826

[12] Radoš K, Brkić M, Begušić D. Recent Advances on Jamming and Spoofing Detection in GNSS [J]. Sensors, 2024, 24(13): 1-28. https://doi.org/10.3390/s24134210

[13] Gao Y, Li G. A Slowly Varying Spoofing Algorithm Avoiding Tightly-Coupled GNSS/IMU With Multiple Anti-Spoofing Techniques [J]. IEEE Transactions on Vehicular Technology, 2022, 71(8): 8864-8876. https://doi.org/10.1109/TVT.2022.3174406

[14] Aoun J, Quaglietta E, Goverde R. Investigating Market Potentials and Operational Scenarios of Virtual Coupling Railway Signaling [J]. Transportation Research Record, 2020, 2674(8): 799-812. https://doi.org/10.1177/0361198120925074

[15] Zhang C, Wang W. Research on Heavy Haul Group Train Operation Control System [J]. Railway Signaling & Communication Engineering, 2024, 7: 1-6.

https://doi.org/10.31875/2409-9694.2025.12.03