GPS Solutions (2024) 28:46
https://doi.org/10.1007/s10291-023-01587-2

ORIGINAL ARTICLE

Detection and mitigation of time synchronization attacks based on long short-term memory neural network

Yang Liu[1] · Bo Xu[1] · Zhengkun Chen[2,3,5,6] · Dan Shen[4] · Zhijian Zhou[2,3] · Xiangwei Zhu[2,3]

Received: 5 May 2023 / Accepted: 18 November 2023 / Published online: 18 December 2023

Abstract

Due to its wide-area and high-precision advantages, Global Navigation Satellite System (GNSS) timing is widely employed in critical infrastructures such as power, communication and transportation, maintaining high-precision time synchronization for the system. Nevertheless, due to the lack of authentication and unencrypted structure of civilian GNSS signals, GNSS receiver is vulnerable to be attacked, resulting in disastrous consequences. Therefore, detecting and mitigating a time synchronization attack (TSA) to improve the security of GNSS timing and ensure the normal operation of critical infrastructures is of great significance. We proposed a TSA detection and mitigation algorithm based on long short-term memory (LSTM) neural network. Based on the good nonlinear mapping ability and high self-learning ability of LSTM, the authentic trend of the receiver clock can be learned and clock state can be predicted. Based on the difference between the predicted and measured clock state of the receiver, TSA detection and mitigation can be realized. Experiments and results show that the proposed algorithm can detect and mitigate two well-known types of TSA. In Type I TSA case, the root-mean-square error (RMSE) is improved by 56.41, 89.14 and 0.01 compared with Robust Estimator (RE), Time Synchronization Attack Rejection and Mitigation (TSARM) method and Multi-Layer Perceptron (MLP) neural network, respectively. In Type II TSA case, the RMSE is improved by 41.80, 88.16 and 0.33 compared with RE, TSARM and MLP, respectively. The research results can be applied to time synchronization systems of critical infrastructures, which can improve time synchronization accuracy and security performance.

Keywords Detection and mitigation · GNSS timing · LSTM · Time synchronization attack

Introduction

The Global Navigation Satellite System (GNSS) provides accurate time synchronization services for critical infrastructures such as power systems, communication networks, financial systems and transportation systems that rely on high-precision time synchronization (Schmidt et al. 2021; Yao et al. 2021; Jaduszliwer et al. 2021; Shereen et al. 2020; Matsakis et al. 2007). However, due to the lack of authentication and unencrypted structure of civilian GNSS signals, the receiver may receive false satellite signals sent by malicious attackers and output wrong time information, which threatens the operation of critical infrastructures (Yao et al. 2016; Mosavi et al. 2016; Liang et al. 2017; Borio et al. 2021; Wang et al. 2021; Wang et al. 2018). Therefore, detecting and mitigating the time synchronization attack (TSA) is significant for ensuring the safe operation of critical infrastructures (Risbud et al. 2019; Jiang et al. 2013; Gao et al. 2022).

✉ Bo Xu
xubo27@mail.sysu.edu.cn

✉ Xiangwei Zhu
zhuxw666@mail.sysu.edu.cn

[1] School of Aeronautics and Astronautics, Sun Yat-sen University, Shenzhen, China

[2] School of Electronics and Communication Engineering, Sun Yat-sen University, Shenzhen, China

[3] Shenzhen Key Laboratory of Navigation and Communication Integration, Shenzhen, China

[4] School of Systems Science and Engineering, Sun Yat-sen University, Guangzhou, China

[5] Beijing Institute of Tracking and Telecommunications Technology, Beijing, China

[6] Key Laboratory of Smart Earth, Beijing, China

In recent years, extensive research has been conducted on the detection and mitigation of TSA. Khalajmehrabadi et al. (2018) proposed the GNSS receiver clock model considering interference based on the Kalman filter. The attack on clock bias can be estimated based on energy functional regularization optimization. The attacked clock can be compensated based on the compensation model so that the receiver can provide accurate and reliable time under TSA. Nevertheless, there exists the risk of divergence in the Kalman filter. Lee et al. (2020) proposed a tuning-free robust estimator to mitigate GNSS spoofing attacks. However, the robust estimator models the clock as a first-order model, while a second-order term for the frequency drift in the clock usually exists. Therefore, even in the absence of TSA, the estimator will estimate and correct the frequency drift as part of the TSA. Orouji et al. (2021) proposed a multi-layer perceptron neural network that focuses on the clock state correction in the receiver. It is independent of how TSA is generated to change time. However, the perceptron network is not the most suitable model for time series prediction. Chauhan et al. (2021a) proposed a Residual-based Spoofing Detection and Measurement Correction (RSDMC) algorithm to detect TSA and correct the spoofed Phasor Measurement Unit (PMU) measurements. Chauhan et al. (2021b) proposed a Spoofing-Resilient State Estimator (SR-SE) which uses the extended Kalman filter to fuse GNSS and PMU measurements. Nevertheless, the risk of divergence in the extended Kalman filter also exists. Wang et al. (2022) proposed a weighed double ratio metric to detect TSA on a GNSS receiver.

The existing studies mentioned above can mitigate the TSA to a certain extent. Nevertheless, the accuracy of these methods is an important issue. We proposed a TSA detection and mitigation algorithm based on a long short-term memory (LSTM) neural network. The characteristics of the receiver clock can be learned through the LSTM network, and the clock state can be predicted. TSA detection is realized when the difference between the measured and the predicted clock states exceeds the threshold. When TSA is detected, the predicted clock states are employed to correct the local clock, which achieves TSA mitigation.

The contributions of this research are as follows.

(1) A new TSA detection and mitigation algorithm based on LSTM is proposed, which can not only realize TSA detection but also mitigate the TSA. The proposed algorithm is independent of the TSA generation process, which can defend a large number of TSA without worrying about new attack generation methods;

(2) To the best of our knowledge, this is the first work that LSTM has been employed in TSA detection and mitigation. Based on the good nonlinear mapping ability and high self-learning ability of LSTM, the accuracy of clock prediction can be improved which helps with TSA detection and mitigation;

(3) We collected the measured data and verified the performance of the proposed algorithm. The experimental results show that the proposed algorithm has improved TSA mitigation accuracy compared with traditional TSA mitigation methods.

The principle of GNSS timing and the TSA model is introduced in the following section. The third section introduces the proposed TSA detection and mitigation algorithm based on LSTM. First, the principle of clock prediction based on LSTM is introduced. Then, the TSA detection and mitigation principle is introduced, and finally, the performance evaluation index is introduced. The fourth section introduces the experiments and results analysis. First, the experimental data are introduced, and then the comparative experiments are introduced. Finally, experiment results are analyzed. The conclusions are drawn in the fifth section. The future research directions are indicated.

Model and methodology

In this section, model and methodology are introduced. The first part of this section introduces the principle of GNSS timing. Receiver clock model is introduced in the second part of this section. Based on the GNSS timing and clock model principle, the TSA model is introduced in the third part of this section.

Principle of GNSS timing

GNSS timing solution is based on pseudorange measurement (Borio et al. 2021), and the pseudorange measurement equation is as follows

$$\rho^n = \left\|\vec{P}^n - \vec{P}_u\right\|_2 + cb_u - cb^n + \varepsilon_\rho^n \tag{1}$$

where ρ^n represents the pseudorange between satellite n and receiver; $\vec{P}^n$ denotes the position of satellite n which can be obtained from ephemeris; $\vec{P}_u$ indicates the receiver position; $\left\|\vec{P}^n - \vec{P}_u\right\|_2$ is the true distance between satellite n and the receiver; c denotes the speed of light; b_u represents the receiver clock bias; b^n denotes the clock bias of satellite n which can be obtained from ephemeris; ε_ρ^n indicates the measurement noise of satellite n. In the pseudorange measurement equation, the receiver position $\vec{P}_u$ and clock bias b_u are unknown quantities which can be calculated by observing more than four satellites.

Doppler frequency shift is also one measured parameter of the receiver, which can be used to obtain the velocity of the receiver. Doppler frequency shift can be converted into pseudorange rate, and receiver clock drift can be obtained based on pseudorange rate

$$\dot{\rho}^n = -\lambda f_d^n \tag{2}$$

where $\dot{\rho}^n$ is the pseudorange rate of satellite n; λ denotes the wavelength of the signal; and f_d^n represents the Doppler frequency shift of satellite n.

The pseudorange rate measurement equation is as follows

$$\dot{\rho}^n = \left(\vec{V}^n - \vec{V}_u\right)\frac{\vec{P}^n - \vec{P}_u}{\left\|\vec{P}^n - \vec{P}_u\right\|_2} + c\dot{b}_u - c\dot{b}^n + \dot{\varepsilon}_\rho^n \tag{3}$$

where $\vec{V}^n$ represents the speed of satellite n which can be obtained from ephemeris; $\vec{V}_u$ denotes the velocity of the receiver; $\frac{\vec{P}^n - \vec{P}_u}{\left\|\vec{P}^n - \vec{P}_u\right\|_2}$ represents the normalized vector between satellite n and the receiver; $\dot{b}_u$ indicates the clock drift of the receiver; $\dot{b}^n$ represents the clock drift of satellite n, which can be obtained from ephemeris; $\dot{\varepsilon}_\rho^n$ indicates pseudorange rate measurement noise. In the pseudorange rate measurement equation, the receiver velocity $\vec{V}_u$ and clock drift $\dot{b}_u$ are unknown quantities which can be obtained by observing more than four satellites.

The position, velocity, clock bias and clock drift of the receiver can be solved based on pseudorange and pseudorange rate measurement, which is named as position, velocity and time (PVT) solutions. This research focuses on the determination of the receiver's clock bias and clock drift.

Modeling of the receiver clock

Based on the principle of GNSS timing, the dynamic model of the receiver clock can be established as follows,

$$\begin{bmatrix} b_u(n+1) \\ \dot{b}_u(n+1) \end{bmatrix} = \begin{bmatrix} 1 & \tau \\ 0 & 1 \end{bmatrix}\begin{bmatrix} b_u(n) \\ \dot{b}_u(n) \end{bmatrix} + \vec{q}_n \tag{4}$$

where b_u and $\dot{b}_u$ denote the clock bias and clock drift, respectively; $n+1$ and n represent the numbers of epochs, τ is the time interval between adjacent epochs, and $\vec{q}_n$ denotes the process noise vector. The covariance matrix is as follows

$$Q_n = \begin{bmatrix} \tau\sigma_1^2 + \frac{1}{3}\tau^3\sigma_2^2 & \frac{1}{2}\tau^2\sigma_2^2 \\ \frac{1}{2}\tau^2\sigma_2^2 & \tau\sigma_2^2 \end{bmatrix} \tag{5}$$

where Q_n represents the process noise covariance matrix which is dependent on the statistics of the receiver clock; $\sigma_1^2 = \frac{h_0}{2}$, $\sigma_2^2 = 2\pi^2 h_{-2}$; h_0 is the frequency white noise coefficient; and h_{-2} denotes the frequency random walk noise coefficient of the receiver clock.

Modeling of TSA

By distorting the authentic/correct pseudorange and pseudorange rate of the receiver, the clock bias and clock drift of the receiver can be distorted without changing the position and velocity of the receiver (Khalajmehrabadi et al. 2018). This TSA is difficult to be detected by the receiver, and the principle is shown as follows

$$\rho_s^n = \rho^n + s_\rho^n = \left\|\vec{P}^n - \vec{P}_u\right\|_2 + c\left(b_u + \frac{s_\rho^n}{c}\right) - cb^n + \varepsilon_\rho^n \tag{6}$$

$$\dot{\rho}_s^n = \dot{\rho}^n + s_{\dot{\rho}}^n = \left(\vec{V}^n - \vec{V}_u\right)\frac{\vec{P}^n - \vec{P}_u}{\left\|\vec{P}^n - \vec{P}_u\right\|_2} + c\left(\dot{b}_u + \frac{s_{\dot{\rho}}^n}{c}\right) - c\dot{b}^n + \dot{\varepsilon}_\rho^n \tag{7}$$

where ρ_s^n represents the measured pseudorange of satellite n under TSA; s_ρ^n denotes the attack amount on pseudorange to satellite n; $\dot{\rho}_s^n$ indicates the measured pseudorange rate of satellite n under TSA; $s_{\dot{\rho}}^n$ denotes the attack amount on pseudorange rate to satellite n. The definition of other variables is the same as those mentioned before.

According to the above equations, the attack amount on pseudorange and pseudorange rate will be absorbed into clock bias and drift results. Therefore, the TSA can be modeled as the superposition attack on pseudorange and pseudorange rate:

$$\rho_s(m) = \rho(m) + s_\rho(m) \tag{8}$$

$$\dot{\rho}_s(m) = \dot{\rho}(m) + s_{\dot{\rho}}(m) \tag{9}$$

where $\rho_s(m)$ is the pseudorange under TSA; $\rho(m)$ denotes the authentic pseudorange; $s_\rho(m)$ represents the pseudorange attack amount. $\dot{\rho}_s(m)$ is the pseudorange rate under TSA; $\dot{\rho}(m)$ represents the authentic pseudorange rate; $s_{\dot{\rho}}(m)$ denotes the pseudorange rate attack amount.

According to the variation of attack amount on pseudorange and pseudorange rate, TSA can be divided into two types: Type I TSA, the clock abruptly jump attack; Type II TSA, the clock gradually pull bias attack (Khalajmehrabadi et al. 2018; Schmidt et al. 2021).

Type I: clock abruptly jump attack

Through adding a fixed constant C_1 and a corresponding Dirac delta function δ to the authentic pseudorange and pseudorange rate, respectively, Type I TSA can be established,

$$s_\rho(m) = C_1 \tag{10}$$

$$s_{\dot{\rho}}(m) = \delta \tag{11}$$

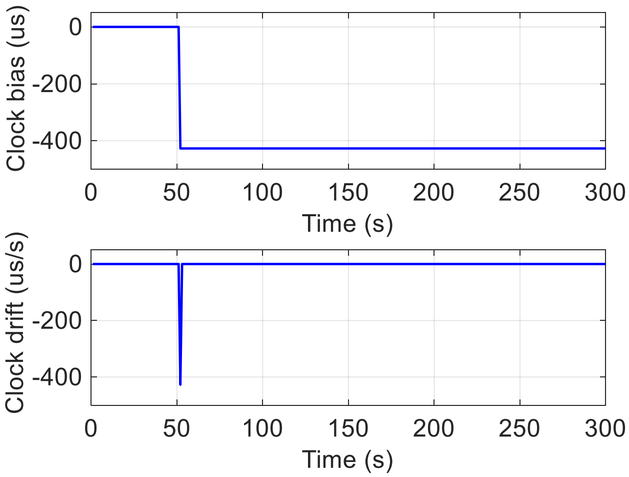


Fig. 1 Effects of Type I TSA

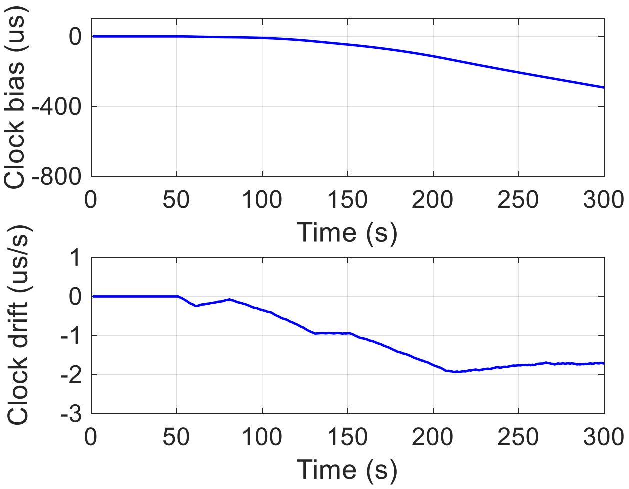


Fig. 2 Effects of Type II TSA

During the PVT solution, the attacks on pseudorange and pseudorange rate are absorbed into clock bias and clock drift, respectively. The effect of this type of TSA is that the clock bias suddenly jumps and the clock drift peaks at the attack moment, as shown in Fig. 1.

Type II: clock gradually pull bias attack

In Type II TSA, the attack amount on pseudorange and pseudorange rate changes gradually with time, which are shown as follows

$$s_{\rho}(m) = s_{\rho}(m-1) + \dot{s}_{\rho}(m)\Delta t \tag{12}$$

$$s_{\dot{\rho}}(m) = s_{\dot{\rho}}(m-1) + \dot{s}_{\dot{\rho}}(m)\Delta t \tag{13}$$

where Δt represents the time interval which is determined by the period of receiver PVT solution; $\dot{s}_{\rho}(m)$ and $\dot{s}_{\dot{\rho}}(m)$ denote the change rate of attack amount on the pseudorange and pseudorange rate, respectively. The attacks on pseudorange and pseudorange rate are absorbed into clock bias and clock drift, respectively. The effect of this type of TSA is that the clock bias is pulled away gradually, and the clock drift changes gradually, as shown in Fig. 2.

TSA detection and mitigation based on LSTM

This section introduces the detection and mitigation of TSA based on LSTM in detail. The first part of this section introduces the principle of clock prediction based on LSTM. Principles of TSA detection and mitigation are introduced in the second and third parts of this section. TSA can be detected and mitigated by comparing the difference between predicted and measured clock states. Finally, the performance evaluation index is introduced.

Clock prediction based on LSTM

Deep learning method has been widely used in solving nonlinear problems. Recurrent neural network (RNN) is a kind of artificial neural network. The core idea of RNN is to find the sequence correlation by using the characteristics of the network structure, which is suitable for time series prediction. Nevertheless, RNN faces difficulties in handling long-distance dependence. LSTM has made improvements to RNN to address long-term storage capacity shortages and the possibility of gradient explosion or vanishing (Hochreiter et al. 1997; Huang et al. 2021). To achieve better prediction accuracy, the LSTM network is employed to predict the clock state of the receiver. Details are as below.

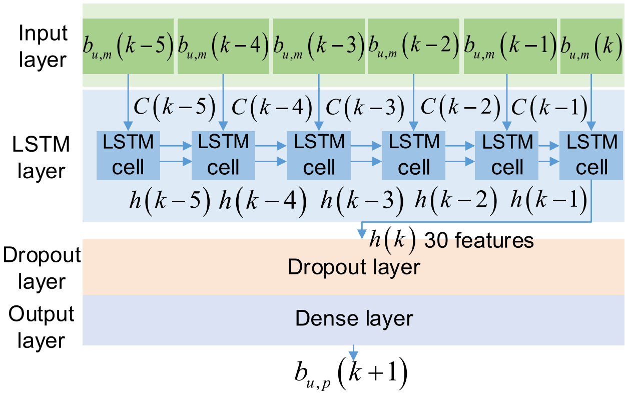


Fig. 3 Network structure of LSTM model

Network structure and model parameter

The network structure of LSTM is shown in Fig. 3. The LSTM neural network structure mainly consists of three core parts: input layer, hidden layer and output layer. The input layer is responsible for processing the input clock time series, which can make the data meet the input requirements of LSTM neurons. The input of the LSTM network is the historical measured receiver clock bias $\left[b_{u,m}(k), b_{u,m}(k-1), b_{u,m}(k-2) \cdots b_{u,m}(k-n)\right]$, where $n=5$. The first hidden layer is a recurrent neural network based on LSTM neurons. The number of LSTM cells in the LSTM network is 6. Each LSTM cell in the LSTM layer fed with only one input (Ma et al. 2020). The LSTM layer outputs 30 features. The second hidden layer is a dropout layer. The dropout is applied to the neurons to prevent overfitting. The output layer is a dense layer which is responsible for the output of prediction results. The output of the LSTM network is the predicted receiver clock bias $b_{u,p}(k+1)$ at next epoch.

The network training and parameter optimization is also important. In the network training, the Adam algorithm is employed to train the network. Grid search and cross-validation algorithm are used to optimize the parameters. Details of LSTM model parameter are shown in Table 1.

The gate mechanism of LSTM

By introducing the gate mechanism, LSTM neural network has stronger storage capacity and can obtain better prediction results in a longer sequence (Hochreiter et al. 1997; Huang et al. 2021).

The cell structure of LSTM is shown in Fig. 4. There are four gates in the LSTM cell, which are the forget gate, the input gate, the select gate and the output gate. The forget gate determines how many cell states of the last moment are forgotten or retained. The input gate and select gate determine how many current inputs are input to the current cell state. The output gate determines how much of the current cell state is added to the output value at the current time. These gates are considered fully connected layers composed of multiple neurons. The number of neurons of fully connected layers is 30. The LSTM layer outputs 30 features.

Table 1 LSTM model parameter setting information

Number	Parameters	Value
1	Loss	MAE
2	Metrics	MAPE
3	Optimizer	Adam
4	Number of LSTM layers	1 layer (6 cells)
5	Number of dropout layers	1 layer
6	Number of dense layers	1 layer
7	Number of epochs	4000
8	Dropout value	0.5
9	Input dimension size	6
10	Output dimension size	1
11	Size of batch	72

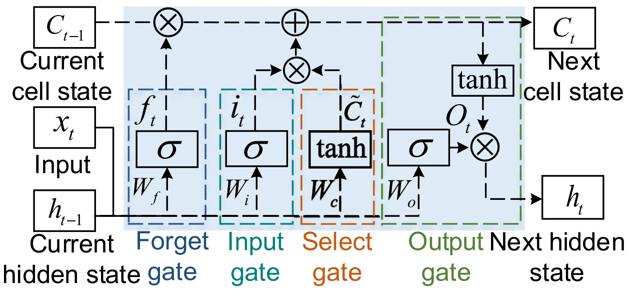


Fig. 4 The internal structure of the LSTM model

The expression of the input gate and select gate is shown as follows

$$i_t = \sigma\left(W_i \cdot \left[h_{t-1}, x_t\right] + b_i\right) \tag{14}$$

$$\tilde{C}_t = \tanh\left(W_C \cdot \left[h_{t-1}, x_t\right] + b_C\right) \tag{15}$$

where i_t and $\tilde{C}_t$ represent the input gate and the select gate at time t, respectively; σ and tanh represent the sigmoid and tanh activation function, respectively; W_i and W_c denote the weight matrix of the input gate and the select gate, respectively; h_{t-1} denotes the hidden state at time t-1; x_t represents the input at time t; b_i and b_c are the offset of the input gate and the select gate, respectively.

The expression of the forget gate is as follows

$$f_t = \sigma\left(W_f \cdot \left[h_{t-1}, x_t\right] + b_f\right) \tag{16}$$

where f_t represents the forget gate at time t; W_f denotes the weight matrix of the forget gate; and b_f is the bias of the forget gate.

The expression of the output gate is shown as follows,

$$o_t = \sigma\left(W_o \cdot \left[h_{t-1}, x_t\right] + b_o\right) \tag{17}$$

$$h_t = o_t * \tanh\left(C_t\right) \tag{18}$$

where o_t represents the output gate at time t; h_t denotes the hidden state at time t and C_t represents the cell state at time t; the symbol $*$ represents the Hadamard product operator. The expression of the cell state is as follows,

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t \tag{19}$$

where C_{t-1} represents the cell state at time t-1.

Network training/test and clock prediction

There are two stages included in the clock prediction based on LSTM: the network training/test and the clock prediction. The characteristics of the receiver clock are learned in the network training/test stage, and the clock prediction is realized in the network prediction stage.

In this article, the role of LSTM network is as a predictor to achieve receiver clock characteristic learning and clock prediction. The data input to the network during the training and test phase is all authentic clock data without TSA. The data are randomly divided into two parts, 80% of which is training data, which is used to adjust the network structure parameters and reduce the error. The remaining 20% is used as test data to test the performance of the network. Through the training of the LSTM network, the clock characteristics can be learned.

In the prediction stage, the authentic clock bias is input to the network to realize clock prediction when no TSA occurs. When TSA occurs, the clock bias after TSA mitigation is employed to input to the network to realize clock prediction.

The variations of clock biases and clock drifts reflect clock characteristics that the LSTM network needs to learn. The variations of the clock biases and clock drifts in both the training/test phase and prediction phase are introduced in this part.

In the training/test phase, the input data are clean data without TSA and the clock biases and drifts change according to the clock model. The clock model is shown as follows

$$b_u(t) = b_u(t-\tau)+\dot{b}_u(t)\cdot\tau+\varepsilon(t) \tag{20}$$

$$\dot{b}_u(t) = \dot{b}_u(t-\tau)+\dot{\varepsilon}(t) \tag{21}$$

where $b_u(t)$ and $b_u(t-\tau)$ represent clock biases at epoch t and $t-\tau$, respectively; $\dot{b}_u(t)$ and $\dot{b}_u(t-\tau)$ represent clock drifts at epoch t and $t-\tau$, respectively; τ is the time interval between epochs; $\varepsilon(t)$ and $\dot{\varepsilon}(t)$ denote phase noises and frequency noises.

In the prediction phase, the data input to the network can be divided into two types: authentic clock bias when no TSA occurs and clock bias after TSA mitigation when TSA occurs. The clock biases and clock drifts change according to the clock model shown in Eqs. 20 and 21.

Because the LSTM network is employed to learn the characteristics of the receiver clock and realize clock prediction, we employ the same LSTM network with the same parameters and hyperparameters for mitigating both type I and II attacks. The input data of the LSTM network are the real measured receiver clock bias in the training phase. Each piece of data has a similar pattern shift behavior to the others in terms of clock, and the network is trained only once. Therefore, the same LSTM network is employed to learn the characteristics of the receiver clock and realize clock prediction. Then the predicted clock biases and drifts are employed to mitigate the type I and II attacks.

The evolution of the LSTM network output error and inputs of LSTM over time also need to be discussed. In LSTM, the network's input values are authentic data at the initial stage of TSA, and the network's output value is accurate. The network's previous outputs will eventually become its input values. As time goes by, more output values become inputs and there is a potential for the output inaccuracy to grow. As a result, output errors may accumulate over time. However, it is important to note that this error does not grow indefinitely. The network's ability to correct its own errors and learn from past mistakes will limit the growth of the output error. The output error evolution can be seen as a trade-off between the ability of LSTM to learn patterns in the data and its ability to maintain accurate predictions over time. Therefore, the output error of the network may accumulate over time, but it will not grow infinitely.

TSA detection

The TSA detection is the premise of TSA mitigation. TSA detection is realized based on the difference between the measured and the predicted clock states. The details of TSA detection under Type I and Type II TSA conditions are as follows.

Type I *TSA*

The principle of Type I TSA detection is shown as follows,

$$\varepsilon_{b_u}\left(t_s\right)=b_{u,m}\left(t_s\right)-b_{u,p}\left(t_s\right) \tag{22}$$

where $b_{u,m}\left(t_s\right)$ and $b_{u,p}\left(t_s\right)$ represent the measured and predicted clock bias, respectively; $\varepsilon_{b_u}\left(t_s\right)$ indicates the difference between the measured and predicted clock bias. When the difference between the measured and predicted clock bias $\varepsilon_{b_u}\left(t_s\right)$ exceeds the threshold L_{b_u}, it is considered that the measured clock bias is abnormal, and Type I TSA detection is realized. The accuracy requirement for time synchronization determines the threshold L_{b_u}. For example, the time synchronization accuracy requirement for smart substation is better than 1 microsecond, in which case the threshold L_{b_u} can be set as 1 microsecond.

Type II *TSA*

The principle of Type II TSA detection is shown as follows

$$\varepsilon_{\dot{b}_u}\left(t_s\right)=\dot{b}_{u,m}\left(t_s\right)-\dot{b}_{u,p}\left(t_s\right) \tag{23}$$

where $\dot{b}_{u,m}\left(t_s\right)$ and $\dot{b}_{u,p}\left(t_s\right)$ represent the measured and predicted clock drift, respectively; $\varepsilon_{\dot{b}_u}\left(t_s\right)$ denotes the difference between the measured and predicted clock drift. When the difference between the measured and predicted clock drift $\varepsilon_{\dot{b}_u}\left(t_s\right)$ exceeds the threshold $L_{\dot{b}_u}$, it is considered that the measured clock drift is abnormal, and the detection of Type II TSA is realized. The accuracy requirement for clock drift determines the threshold $L_{\dot{b}_u}$. For example, the clock drift requirement for smart substation is less than 0.2 microseconds/s, in which case the threshold $L_{\dot{b}_u}$ can be set as 0.2 microseconds/s.

TSA mitigation

After the TSA is detected, the clock bias and clock drift measured by the receiver need to be corrected. The TSA needs to be mitigated. The details of TSA mitigation under Type I and Type II TSA conditions are introduced as follows.

Type I *TSA*

After Type I TSA is detected at time t_s, the clock bias measured by the receiver at and after the time t_s should be corrected.

$$b_u(t) = b_{u,m}(t) - \varepsilon_{b_u}(t), t \geq t_s \tag{24}$$

where $b_u(t)$ denotes the corrected clock bias at time t. The difference between the measured and predicted clock bias is deducted from the measured clock bias to mitigate the effect of Type I TSA on receiver clock bias.

Type II *TSA*

After Type II TSA is detected at the time t_s, the clock drift measured by the receiver at and after the time t_s should be corrected.

$$\dot{b}_u(t) = \dot{b}_{u,m}(t) - \varepsilon_{\dot{b}_u}(t), t \geq t_s \tag{25}$$

where $\dot{b}_u(t)$ denotes the corrected clock drift at time t. The difference between the measured and predicted clock drift is deducted from the measured clock drift to mitigate the effect of Type II TSA on receiver clock drift.

After Type II TSA is detected at the time t_s, the clock bias measured by the receiver at and after the time t_s should also be corrected.

$$b_u(t) = b_{u,m}(t) - \varepsilon_{\dot{b}_u}(t) \cdot \left(t - t_s\right), t \geq t_s \tag{26}$$

where $b_u(t)$ denotes the corrected clock bias at time t. The product of the clock drift attack amount and the time interval is deducted from the measured clock bias to mitigate the effect of Type II TSA on receiver clock bias.

Performance evaluation

The root-mean-square error (RMSE) which shows the average error between the true value and the estimated value is employed to evaluate the prediction accuracy and TSA mitigation performance

$$RMSE = \sqrt{\frac{1}{K}\sum_{k=0}^{K-1}\left(ct_u(k) - \widetilde{ct}_u(k)\right)^2} \tag{27}$$

where K denotes the data length; $ct_u(k)$ is the true value; and $\widetilde{ct}_u(k)$ represents the estimated value.

Test and results

Experiments and results analysis are introduced in this section. First, the experimental data are introduced. Then the comparative experiment design is introduced. Finally, experiment results are analyzed.

Experimental data

Smartphones are widely used in daily life. Most smartphones have built-in GNSS receiver chips, which can achieve GNSS positioning and timing. Therefore, a smartphone can be considered as a GNSS receiver. Due to the widespread application, easy access and susceptibility to TSA of smartphones, we employed the smartphone to collect GNSS data for TSA detection and mitigation experiments.

The HUAWEI P40 smartphone with an embedded GNSS chipset is employed to collect real GNSS signals. The location of the smartphone receiver is the sports field of Shenzhen campus of the Sun Yat-sen University, which is an open area shown in Fig. 5. It should be noted that

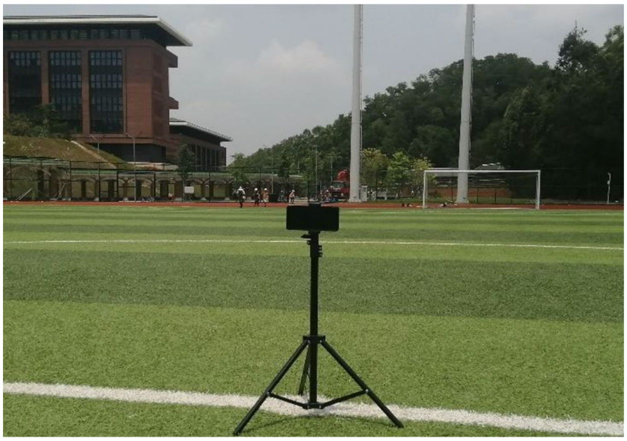


Fig. 5 Data collection

the smartphone is stationary during the data collection procedure. The signal collection date is April 15, 2023, and the data collection lasted 300 s.

The Android application GNSSLogger released by Google is employed to record and output raw GNSS measurements. The related postprocessing MATLAB codes are employed to postprocess the original GNSS data to obtain pseudorange and pseudorange rate data (Google 2020). Experimental conditions setting is shown in Table 2.

The ground truth (GT) of the clock bias and clock drift is obtained through taking the weighted least square (WLS) solution for the stationary device. Type I and Type II TSA are simulated and injected into pseudorange and pseudorange rate data to simulate Type I and Type II TSA (Khalajmehrabadi et al. 2018).

Comparative experiment design

The performance of different algorithms can be compared by conducting comparative experiments. The comparative experiments are introduced in this section, and relative information is shown in Table 3.

As mentioned above, the ground truth (GT) of the clock bias and clock drift estimation is obtained through taking the WLS solution for the stationary device. The ground truth is the baseline for testing the TSA detection and mitigation performance.

The PVT solutions such as WLS, the extended Kalman filter (EKF) and the classical Luenberger observer (LBG) (Luenberger et al. 1966) are employed to evaluate the performance of typical PVT solutions under TSA.

The Robust Estimator (RE) (Lee et al. 2020), the Time Synchronization Attack Rejection and Mitigation (TSARM) method (Khalajmehrabadi et al. 2018), the Multi-Layer Perceptron (MLP) neural network method (Orouji et al. 2021) and the proposed TSA detection and mitigation method based on LSTM (LSTM) are employed to detect and mitigate TSA and for performance comparison. They are employed to evaluate the performance of TSA detection and mitigation methods under TSA.

Table 2 Experimental conditions setting

Number	Parameters	Value
1	Equipment version	HUAWEI P40
2	System version	Harmony OS 3.0.0
3	GNSSLogger version	GNSSLogger 2.0.0.1
4	Starting time	April 15, 2023 3:24:37 (UTC)
5	End time	April 15, 2023 3:29:37 (UTC)
6	Data length	300 s

Table 3 Comparative experiment design

Number	Method	Type
1	GT	Ground truth
2	WLS	Typical PVT solution
3	EKF	Typical PVT solution
4	LBG	Typical estimation method
5	RE	Existing TSA mitigation method
6	TSARM	Existing TSA mitigation method
7	MLP	Existing TSA mitigation method
8	LSTM	Proposed TSA mitigation method

Experiment results analysis

Experiment results analysis is introduced in this section. First, clock prediction precision is analyzed. Then, TSA mitigation performance under Type I and Type II TSA conditions is analyzed.

Clock prediction

The accuracy of clock prediction affects the performance of TSA detection and mitigation. Therefore, the accuracy of clock prediction is first analyzed. Widely used clock prediction methods, the Kalman filter (KF) and quadratic polynomial (QP), are employed as comparison.

As shown in Fig. 6, the prediction errors of KF, QP and LSTM are exhibited. The performance of prediction error of LSTM is the best due to the use of a neural network to learn clock characteristics accurately.

The RMSE of KF, QP and LSTM is exhibited in Table 4. The RMSE of LSTM is the smallest, which indicates the LSTM is with the best prediction performance. The RMSE of KF is better than QP.

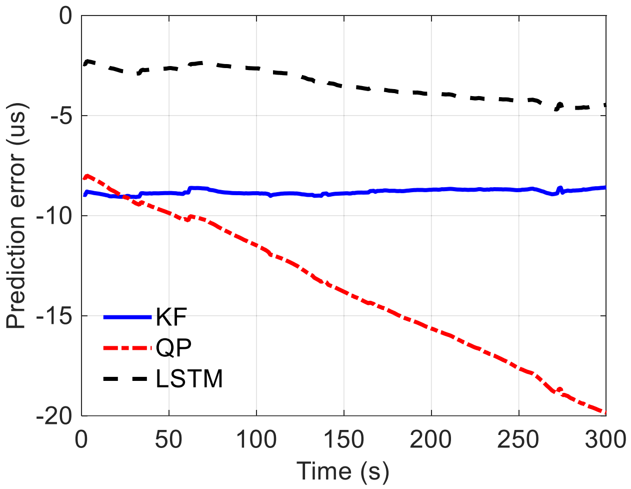


Fig. 6 Clock prediction accuracy

Table 4 RMSE of clock prediction

Method	KF	QP	LSTM
RMSE	8.81	14.16	3.51

The LSTM clock prediction method is better than widely employed prediction methods, which is good for TSA detection and mitigation. The TSA mitigation performance is analyzed in the next part.

TSA mitigation

After evaluating the prediction performance, the TSA mitigation performance is analyzed in this part. The TSA mitigation performance under Type I and Type II TSA conditions is analyzed.

Type I TSA As shown in Fig. 7, the performance of typical PVT solutions under Type I TSA is exhibited. After Type I TSA is applied from $t=50$ s to $t=300$ s, the clock biases of the WLS, EKF and LBG jumped nearly 427 microseconds and the clock drifts of the WLS, EKF and LBG suddenly jumped. This indicates that the typical PVT solutions cannot withstand the Type I TSA.

The performance of TSA mitigation methods is shown in Fig. 8. As shown in Fig. 8, there exist a sudden jump and recovery of clock bias and drift in the RE method. There exists bias between the TSARM method and ground truth. Meanwhile, the clock bias and the clock drift curve of LSTM are closest to ground truth. This indicates that the LSTM TSA mitigation method performs the best under Type I TSA.

The RMSE of the estimated clock bias under Type I TSA is shown in Table 5. The RMSE values of typical PVT solutions, WLS, EKF and LBG, are in the 10^2 order of magnitude, while the RMSE of RE and TSARM is in the 10^1 order of magnitude. The RMSE values of MLP and LSTM are in the 10^{-2} order of magnitude. The RMSE of LSTM is smaller than that of MLP. This indicates that the TSA mitigation methods, RE, TSARM, MLP and LSTM can mitigate Type I TSA and the proposed LSTM method has the best TSA mitigation performance.

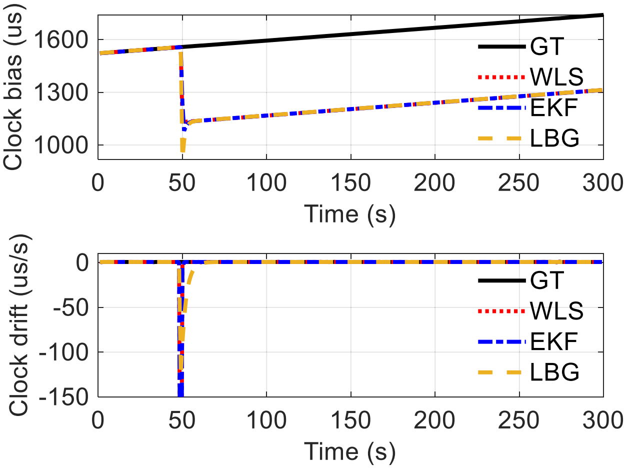


Fig. 7 Typical PVT solution performance under Type I TSA

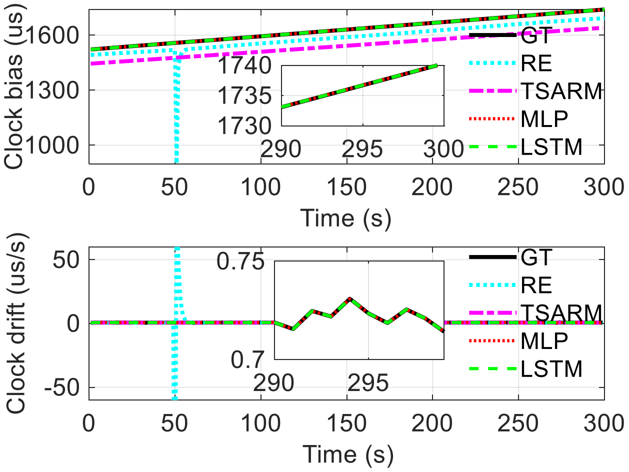


Fig. 8 Type I TSA detection and mitigation performance

The LSTM-based method improves the RMSE by an amount 0.01 compared with MLP method under type I attack. This improvement can improve timing accuracy by 0.01 microseconds. Assuming PDOP value is 3, the algorithm proposed in this article can improve positioning accuracy by nearly 8.99 m. Therefore, the proposed algorithm can improve the positioning accuracy and timing accuracy under type I attack, which is significant for high-precision positioning and timing.

The processing time of the employed methods under Type I TSA is shown in Table 6. The processing time of typical PVT solutions and RE is in the 10^0 order of magnitude, while the processing time of TSARM, MLP and LSTM is in the 10^1 order of magnitude. This indicates that compared with typical PVT solutions and RE, TSARM, MLP and LSTM have a higher computational complexity. For LSTM, this algorithm achieves higher TSA mitigation precision at the cost of higher computational complexity.

Type II TSA As shown in Fig. 9, typical PVT solution performance under Type II TSA is exhibited. After the Type II attack is applied from $t=50$ s to $t=300$ s, the clock biases of the WLS, EKF and LBG are gradually pulled away from the ground truth. The clock drifts of the WLS, EKF and LBG are gradually pulled away from the ground truth. This indicates that the typical PVT solutions cannot withstand the Type II TSA.

The performance of TSA mitigation methods is shown in Fig. 10. For both the clock bias and clock drift curves,

Table 5 RMSE under Type I TSA

Method	WLS	EKF	LBG	RE	TSARM	MLP	LSTM
RMSE	390.54	390.29	391.50	56.42	89.15	0.02	0.01

Table 6 Processing time of the employed methods under Type I TSA

Method	WLS	EKF	LBG	RE	TSARM	MLP	LSTM
Time/s	2.84	3.12	2.91	4.05	56.40	17.87	26.70

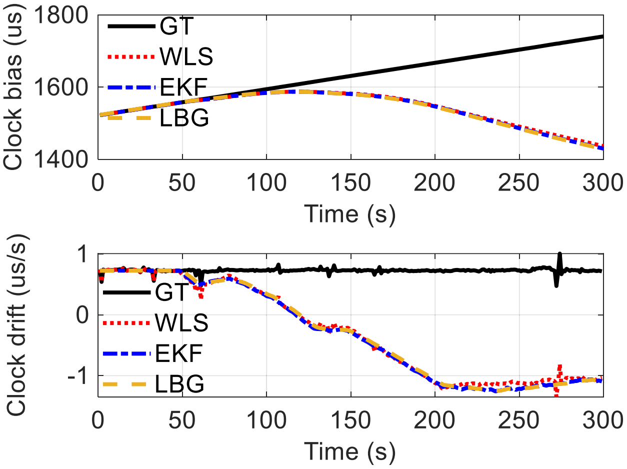


Fig. 9 Typical PVT solution performance under Type II TSA

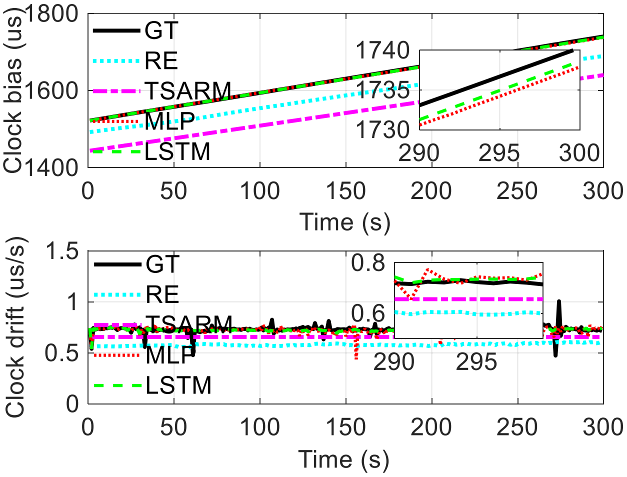


Fig. 10 Type II TSA detection and mitigation performance

there exists bias between RE, TSARM and the ground truth. Meanwhile, the clock bias and clock drift curve of LSTM are closest to that of the ground truth. This indicates that the LSTM TSA mitigation performance is the best.

The RMSE of the estimated clock bias under Type II TSA is shown in Table 7. The RMSE values of typical PVT solutions, WLS, EKF and LBG, are in the 10^2 order of magnitude. Meanwhile, the RMSE values of RE and TSARM are in the 10^1 order of magnitude. The RMSE value of MLP is in the 10^0 order of magnitude. The RMSE value of LSTM is in the 10^{-1} order of magnitude. The RMSE of LSTM is smaller than that of MLP. This indicates that the TSA mitigation methods, RE, TSARM, MLP and LSTM can mitigate Type II TSA. The proposed LSTM method is with the best TSA mitigation performance.

The proposed LSTM method improves the RMSE by an amount of 0.33 compared with MLP method under type II attack. This improvement can improve timing accuracy by 0.33 microseconds. Assuming PDOP value is 3, the algorithm proposed in this article can improve positioning accuracy by nearly 296.79 m. The proposed algorithm significantly improved the positioning accuracy and timing accuracy under type II attack, which is significant for high-precision positioning and timing.

The processing time of the employed methods under Type II TSA is shown in Table 8. The computational complexity of employed methods under Type II TSA is similar to that of Type I TSA. For LSTM, this algorithm achieves higher TSA mitigation precision at the cost of higher computational complexity.

Table 7 RMSE under Type II TSA

Method	WLS	EKF	LBG	RE	TSARM	MLP	LSTM
RMSE	132.24	134.96	135.74	42.79	89.15	1.32	0.99

Table 8 Processing time of the employed methods under Type II TSA

Method	WLS	EKF	LBG	RE	TSARM	MLP	LSTM
Time/s	2.68	2.90	2.73	3.07	54.82	17.87	26.70

Conclusions

This study focuses on TSA detection and mitigation. The TSA detection and mitigation algorithm based on LSTM is proposed, and the performance of the proposed algorithm is verified. Experiments and results show that the proposed algorithm can detect and mitigate two well-known types of TSA. In Type I TSA case, the RMSE is improved by 56.41, 89.14 and 0.01 compared with RE, TSARM and MLP, respectively. In Type II TSA case, the RMSE is improved by 41.80, 88.16 and 0.33 compared with RE, TSARM and MLP, respectively. This indicates that the proposed algorithm has better TSA detection and mitigation capabilities than the existing three algorithms. A further research direction of this study will test the TSA detection and mitigation performance of the algorithm in the real TSA environment.

Acknowledgements Not applicable.

Author contributions All authors contributed to the study conception and design. XZ and BX presented the basic idea of the paper and revised the paper. YL performed the experiment and wrote the paper. ZC, DS and ZZ contributed to the discussion about the content and provided comments on the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding This work was supported by the National Key Research and Development Program of China (Grant No. 2021YFA0716500), the National Natural Science Foundation of China (Grant Nos. 61973328, 91938301) and Shenzhen Science and Technology Plan Project (Grant No. ZDSYS20210623091807023).

Data availability The GNSS datasets can be provided to readers by contacting the corresponding author on reasonable request.

Declarations

Conflict of interest The authors declare no conflict of interest.

Ethical approval and consent to participate Not applicable.

Consent for publication All authors read and approved the final manuscript to be published.

References

Borio D, Gioia C (2021) Interference mitigation: impact on GNSS timing. GPS Solut. https://doi.org/10.1007/s10291-020-01075-x

Chauhan SVS, Gao GX (2021a) Synchrophasor data under Gps spoofing: attack detection and mitigation using residuals. IEEE Trans Smart Grid 12(4):3415–3424

Chauhan SVS, Gao GX (2021b) Spoofing resilient state estimation for the power grid using an extended kalman filter. IEEE Trans Smart Grid 12(4):3404–3414

Gao Y, Li G (2022) Three time spoofing algorithms for GNSS timing receivers and performance evaluation. GPS Solut. https://doi.org/10.1007/s10291-022-01275-7

Google (2020) Raw GNSS measurements. https://developer.android.google.cn/guide/topics/sensors/gnss.

Hochreiter S, Schmidhuber J (1997) Long short-term memory. Neural Comput 9(8):1735–1780

Huang B, Ji Z, Zhai R, Xiao C, Yang F (2021) Clock bias prediction algorithm for navigation satellites based on a supervised learning long short-term memory neural network. GPS Solut. https://doi.org/10.1007/s10291-021-01115-0

Jaduszliwer B, Camparo J (2021) Past, present and future of atomic clocks for GNSS. GPS Solut. https://doi.org/10.1007/s10291-020-01059-x

Jiang X, Zhang J, Harding BJ, Makela JJ, Dominguez-Garc´ıa A D, (2013) Spoofing GPS receiver clock offset of phasor measurement units. IEEE Trans Power Syst 28(3):3253–3262

Khalajmehrabadi A, Gatsis N, Akopian D, Taha AF (2018) Realtime rejection and mitigation of TSA on the global positioning system. IEEE Trans Ind Electron 65(8):6425–6435

Lee J, Taha AF, Gatsis N, Akopian D (2020) Tuning-free, low memory robust estimator to mitigate GPS spoofing attacks. IEEE Contr Syst Lett 4(1):145–150

Liang G, Zhao J, Luo F, Weller SR, Dong Z (2017) A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid 8(4):1630–1638

Luenberger D (1966) Observers for multivariable systems. IEEE Trans Autom Control 11(2):190–197

Ma J, Liu H, Peng C, Qiu T (2020) Unauthorized broadcasting identification: a deep LSTM recurrent learning approach. IEEE Trans Instrum Meas 69(9):5981–5983

Matsakis, D (2007) The timing group delay (TGD) correction and GPS timing biases. In: Proceedings of the 63rd Annual Meeting of The Institute of Navigation pp 49–54

Mosavi MR, Tabatabaei A, Zandi MJ (2016) Positioning improvement by combining GPS and GLONASS based on Kalman filter and its application in GPS spoofing situations. Gyroscop Navig 7(4):318–325

Orouji N, Mosavi MR (2021) A multi-layer perceptron neural network to mitigate the interference of time synchronization attacks in stationary GPS receivers. GPS Solut. https://doi.org/10.1007/s10291-021-01124-z

Risbud P, Gatsis N, Taha A (2019) Vulnerability analysis of smart grids to GPS spoofing. IEEE Trans Smart Grid 10(4):3535–3548

Schmidt E, Lee J, Gatsis N, Akopian D (2021) Rejection of smooth GPS time synchronization attacks via sparse techniques. IEEE Sensors J 21(1):776–789

Shereen E, Delcourt M, Barreto S, Dan G, Boudec J-YL, Paolone M (2020) Feasibility of time-synchronization attacks against PMU based state estimation. IEEE Trans Instrum Meas 69(6):3412–3427

Wang Y (2018) Distributed estimation of power system oscillation modes under attacks on GPS clocks. IEEE Trans Instrum Meas 67(7):1626–1637

Wang C, Kong L, Jiang J, Lai Y (2021) Machine learning-based approach to GPS antijamming. GPS Solut. https://doi.org/10.1007/s10291-021-01154-7

Wang Y, Kou Y, Zhao Y, Huang Z (2022) Detection of synchronous spoofing on a GNSS receiver using weighed double ratio metrics. GPS Solut. https://doi.org/10.1007/s10291-022-01268-6

Yao J, Yoon S, Stressler B, Hilla S, Schenewerk M (2021) GPS satellite clock estimation using global atomic clock network. GPS Solut. https://doi.org/10.1007/s10291-021-01145-8

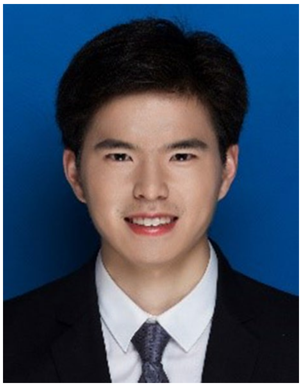
Yao J, Weiss M, Curry C, Levine J (2016) GPS Jamming and GPS Carrier-Phase Time Transfer. In: Proceedings of the 47th Annual Precise Time and Time Interval Systems and Applications Meeting, pp 80–85

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Yang Liu received the B.S. degree in communication engineering from XiDian University in 2017. He received the M.S. degree in information and communication engineering from National University of Defense Technology in 2019. He is currently pursuing the Ph.D. degree in Sun Yat-sen University. His current research interests include time synchronization and timescale algorithms.

Bo Xu is currently a professor/doctoral advisor in the School of Aeronautics and Astronautics, Sun Yat-sen University. His research interests are: aerospace dynamics and control, satellite navigation, deep space exploration. He published more than 70 papers, 30 of which were included in SCI.

Zhengkun Chen received a B.S. degree in surveying engineering from Central South University, Changsha, China, in 2013, an M.S. degree in electronics and communication engineering from the National University of Defense Technology, Changsha, China, in 2015 and his Doctoral degree in Communication and Information Systems from Sun Yat-sen University in Shenzhen, China in 2023. Currently, he is working as an Assistant Researcher at the Beijing Institute of Tracking and Telecommunications Technology in Beijing, China. His research interests include high-confidence, high-precision and high-integrity of comprehensive positioning, navigation, and timing (PNT).



Dan Shen received an M.S. degree in information and communication engineering from the National University of Defense Technology in 2018. He is currently pursuing a Ph.D. degree at Sun Yat-sen University. His current research interests include intelligent navigation.

Zhijian Zhou received a B.S. degree in communication engineering from Sun Yat-sen University in 2021. He is currently pursuing an M.S. degree at Sun Yat-sen University. His current research interests include safe navigation.

Xiangwei Zhu is a professor at the School of Electronics and Communication Engineering, Sun Yat-sen University. He mainly researches the BeiDou system and comprehensive positioning, navigation and timing (PNT), including intelligent and autonomous navigation, communication and navigation fusion, time synchronization, intelligent signal processing and instrument design.