SpoofConvNet Based Enhanced Signal Quality Monitoring for GNSS Spoofing Detection in Consumer Electronics

Xiaoqin Jin, Xiaoyu Zhang, Wenwu Wang, *Senior Member*, *IEEE*, Zhanfeng Qi, and Shuaiyong Zheng

Abstract— Global navigation satellite system (GNSS) is indispensable for consumer electronics (e.g., smartphones) but faces severe spoofing threats that manipulate positioning/timing. However, traditional signal quality monitoring (SQM) methods rely on fixed multi-correlator fusion, which lacks adaptability to dynamic spoofing, leading to unstable detection. To address these limitations, we first define the spoofing signal-to-noise ratio (SSNR) to quantitatively evaluate theoretical detection probability of SQM metrics, providing a benchmark for metric selection. We then prove the suboptimality of linear fusion using Cauchy-Schwarz inequality, which cannot reach the theoretical SSNR upper bound, further confirming the need for nonlinear solutions. Building on this theoretical insight, we propose a dedicated spoofing convolution network (SpoofConvNet) tailored for consumer electronics. Adopting a three-stage framework (multi-correlator spatiotemporal feature input, end-to-end convolutional neural network processing, and spoofing state output), SpoofConvNet directly targets the flaws of traditional methods. Its shared encoder integrates spatiotemporal feature extraction and noise suppression, while 2-dimensional convolutions simultaneously capture spatial correlator anomalies and temporal frame trends. Its lightweight architecture aligns with the hardware constraints of consumer devices. Experiments validate SpoofConvNet outperforms both traditional SQM methods and mainstream neural networks, providing a practical anti-spoofing solution for GNSS-enabled consumer electronics.

***Index Terms*—Consumer electronics, global navigation satellite system (GNSS) spoofing detection, signal quality monitoring (SQM), SpoofConvNet, spoofing signal-to-noise ratio (SSNR)**

This work was supported by the Tianjin Research Innovation Project for Postgraduate Students, China (No. 2022BKYZ039). *(Corresponding authors: Xiaoyu Zhang; Zhanfeng Qi.)*

Xiaoqin Jin, Xiaoyu Zhang, and Zhanfeng Qi are with the College of Artificial Intelligence, Nankai University, Tianjin 300350, China (e-mail: xiaoqinjin@mail.nankai.edu.cn; zhangxiaoyu@nankai.edu.cn; qizhanfeng@nankai.edu.cn).

Wenwu Wang is with the Centre for Vision, Speech and Signal Processing, University of Surrey, GU2 7XH Guilford, U.K. (e-mail: w.wang@surrey.ac.uk).

Shuaiyong Zheng is with the School of Integrated Circuit Science and Engineering, Tianjin University of Technology, Tianjin 300384, China (e-mail: syzheng21@email.tjut.edu.cn).

I. INTRODUCTION

GLOBAL navigation satellite system (GNSS) has become an indispensable sensor in consumer electronics, as it underpins core functions of devices such as smartphones, virtual reality (VR) headsets and smart wearables [1]. These functions specifically include location-based services in ride-hailing apps and spatial positioning in VR games. However, the open signal structure and ultra-low received power of GNSS make it highly vulnerable to spoofing attacks, where counterfeit signals are injected to manipulate position or timing information [2]. A typical incident occurred near the Kremlin in Moscow in 2016, when GNSS spoofing caused smartphones of social media users to incorrectly locate at Vnukovo airport, which is 20 miles from downtown Moscow [3]. As consumer electronics increasingly rely on GNSS for safety-critical scenarios (e.g., pedestrian navigation) and experience-driven scenarios (e.g., VR), timely detection and isolation of spoofing attacks have become imperative to safeguard user trust and system integrity [4].

The mechanism of GNSS spoofing and its impact on receiver tracking loops can be summarized as follows: spoofing signals initially enter the receiver with a weak power advantage, gradually diverge from authentic signals (pull-off), and eventually manipulate the loop output to control navigation results [5]. During spoofing, the variation in the cross-correlation function (CCF) between the local replica and the received signal is illustrated in Fig. 1, where the green dashed line denotes the CCF between the authentic signal and the local replica, the red dashed line denotes the CCF between the spoofing signal and the local replica, while the black curve denotes the CCF between the hybrid signal (combining spoofing and authentic signals) and the local replica. The black dots indicate the positions of the early (E), prompt (P), and late (L) correlators within the tracking loop. After spoofing intrusion, the coexistence of authentic and spoofing signals (with relative delay) distorts the CCF. This distortion transforms the CCF from a symmetric shape to an asymmetric one, and this asymmetry serves as a critical indicator for spoofing detection via signal quality monitoring (SQM). SQM is widely adopted in consumer electronics due to its compatibility with existing receiver hardware. The basic principle of SQM is to construct detection metrics using correlator outputs and implement binary hypothesis testing (H_0: no spoofing; H_1: spoofing exists) for decision-making.

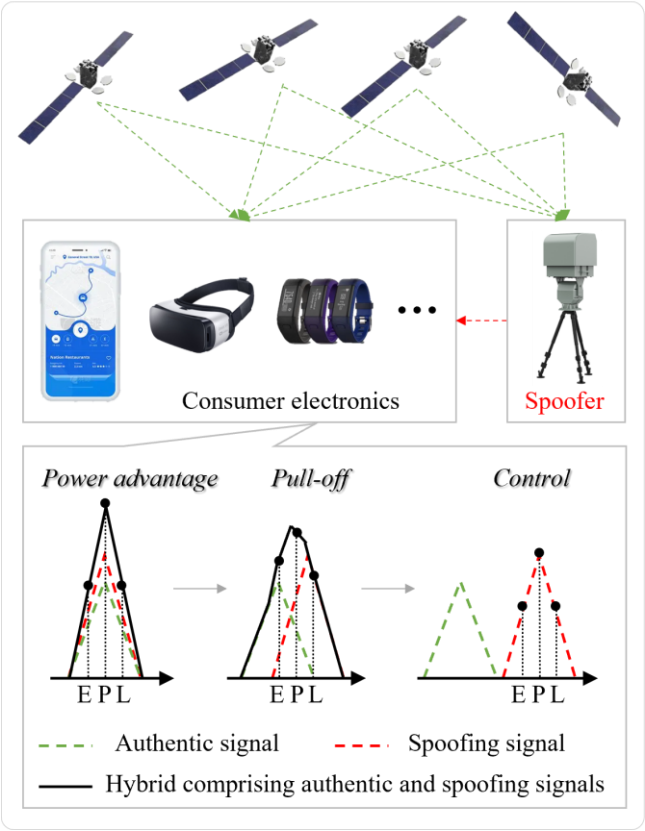

Fig. 1. Variations of the CCF in the GNSS receiver tracking loop during spoofing intrusion.

Traditional SQM methods for spoofing detection primarily focus on two directions. On one hand, classical detection metrics, including Delta, Ratio, Slope, and early-late phase (ELP), are built using outputs from a single pair of in-phase (I) correlators [6], [7]. To adapt to spoofing with time varying delays and phases (a scenario common in dynamic consumer scenarios like driving), subsequent studies have extended these metrics by fusing quadrature (Q) outputs and multi-correlator signals [8], [9], [10], [11]. They construct composite detection metrics via linear weighting to broaden the coverage of spoofing parameters [12], [13], [14], [15], [16], [17], [18], [19], [20]. On the other hand, noise suppression is critical for improving detection reliability in noisy consumer environments (e.g., urban canyons). Recent work has applied Kalman filtering to smooth raw correlator outputs, which effectively reduces noise interference on SQM metrics without adding excessive latency to consumer devices [21].

With the proliferation of artificial intelligence (AI) enabled consumer electronics (e.g., AI-optimized smartphones, intelligent wearables), intelligent SQM methods integrating machine learning (ML) and deep learning (DL) have emerged as a research focus [22], [23]. These methods aim to address the limitations of traditional methods based on linear models while aligning with the computational capabilities of modern consumer hardware [24]. Their core advantage lies in leveraging data-driven nonlinear modeling to enhance detection robustness in complex consumer scenarios, such as urban multipath and dynamic spoofing. Key advances in this field center on three directions: multi-feature fusion, which integrates SQM metrics, carrier-to-noise ratio (CNR), and positioning, navigation and timing (PVT) residuals to address the limitations of single-parameter detection [25], [26], [27], [28]; sequential dynamic modeling, which uses long short-term memory (LSTM) or convolutional neural network (CNN) to capture the slow time varying characteristics of spoofing signals and adapt to dynamic consumer scenarios like vehicle-mounted navigation [29], [30]; and unknown scenario adaptation, which adopts generative adversarial network or variational autoencoder to generalize to unseen spoofing types and address the uncertainty of real-world consumer attack patterns [31], [32], [33], [34]. Many of these methods have validated their effectiveness on the Texas spoofing test battery (TEXBAT) benchmark dataset, achieving high detection accuracy and low latency, which are key requirements for consumer devices [35], [36]. However, while intelligent SQM methods have made progress, they still lack a systematic connection with the theoretical bottlenecks of traditional methods. Most studies focus on performance optimization through empirical model design, without clarifying why nonlinear models outperform linear weighting. Additionally, they rarely customize features or network structures for the unique characteristics of GNSS signals and the hardware constraints of consumer electronics.

Current research on GNSS spoofing detection in consumer electronics faces three major gaps. First, the absence of quantitative assessments regarding the theoretical detection performance of different SQM metrics hinders resource-constrained consumer devices from selecting optimal indicators. Second, the limitations of traditional methods and theoretical basis for introducing intelligent approaches remain unresolved, impeding the generalization of intelligent SQM across diverse consumer scenarios. Third, the features and network architectures required for spoofing detection urgently require customization. Existing approaches often employ generic deep learning architectures, failing to fully leverage GNSS signal characteristics while also struggling to accommodate the hardware constraints of consumer devices.

To address these gaps, we propose a GNSS spoofing detection method based on a dedicated spoofing convolution network (SpoofConvNet), which is tailored for consumer electronics. The method adopts a three-stage framework: multi-correlator temporal-spatial feature input, end-to-end convolutional neural network processing, and spoofing state output. This framework enables accurate detection of dynamic spoofing while balancing performance and resource efficiency. The key contributions of this study are as follows:

1) We first provide a quantitative definition of the spoofing signal-to-noise ratio (SSNR) for SQM metrics. A higher SSNR indicates a higher theoretical detection probability, and this definition lays a theoretical foundation for metric selection in consumer devices.
2) Using the Cauchy-Schwarz inequality, we theoretically prove that any linearly weighted multi-correlator SQM

method cannot reach the theoretical SSNR upper bound. This confirms the inherent suboptimality of linear methods and justifies the need for nonlinear models.

3) We design a shared encoder structure that extracts temporal-spatial features from multi-correlators while suppressing noise. By replacing traditional linear weighting with the local feature extraction and nonlinear mapping of CNNs, we fundamentally resolve the theoretical suboptimality of linear methods. Meanwhile, the architecture of SpoofConvNet is lightweight, making it suitable for consumer electronics.

Experimental results on self-constructed datasets (covering time and position spoofing) and the TEXBAT dataset validate the effectiveness of the proposed method, demonstrating its potential for integration into smartphones, VR headsets, and other consumer devices.

The remainder of this paper is organized as follows. Section II analyzes the spoofing process and SQM metrics, clarifying the limitations of traditional methods. Section III details the design of SpoofConvNet. Section IV presents experimental validation, comparing the performance of the proposed method with traditional and other intelligent methods. Section V discusses the results and concludes the paper.

II. Spoofing Process and Metric Analysis

This section first establishes a signal model under spoofing attacks. It clarifies the statistical characteristics of multi-correlator outputs for both authentic and spoofing signals. It then analyzes the principles and performance bottlenecks of classical SQM metrics, and further discusses the constraints of linear weighted multi-correlator fusion methods. All analyses focus on optimizing signal processing approaches that align with consumer electronics' hardware capabilities, improving detection performance for real-world user scenarios, and resolving practical security challenges in GNSS-enabled consumer applications.

A. Classical SQM Metrics and Their Performance Limitations

The output expressions of correlators with code spacing d for I and Q channels of the tracking loop are [21]

$$\begin{cases} I(d) = R(\Delta\tau + d)\cos(\Delta\varphi) + \alpha_s R(d) + n_{\mathrm{I}} \\ Q(d) = R(\Delta\tau + d)\sin(\Delta\varphi) + n_{\mathrm{Q}} \end{cases} \tag{1}$$

where $\Delta\tau$, $\Delta\varphi$, and α_s denote the relative delay, phase, and amplitude of the spoofing signal to the authentic signal. n_{I} and n_{Q} are zero-mean Gaussian white noise components. $R(\bullet)$ is the CCF of the pseudorange random noise (PRN) code, satisfying

$$R(d) = \begin{cases} 1 - |d|, & |d| < 1 \text{ chip} \\ 0, & |d| \geq 1 \text{ chip} \end{cases}. \tag{2}$$

From (1) and (2), after spoofing intrusion and before the onset of pull-off (a process where spoofing signals gradually diverge from authentic ones), $\Delta\tau = 0$ and the I-channel CCF exhibits symmetric, even characteristics. Once pull-off starts, $\Delta\tau$ deviates from 0, and the CCF no longer maintains symmetry. This change in CCF symmetry before and after pull-off serves as the core basis for spoofing detection via SQM, which is widely adopted in consumer electronics due to its compatibility with existing GNSS receiver hardware (e.g., multi-correlator architectures in smartphone chipsets).

SQM implements detection through binary hypothesis testing: the null hypothesis H_0 indicates no spoofing, and the alternative hypothesis H_1 indicates spoofing presence. Detection metrics are constructed using correlator outputs to quantify CCF asymmetry. Two typical SQM metrics are Delta and Ratio.

1) Delta metric

The Delta metric quantifies CCF asymmetry using the normalized difference between the outputs of E and L correlators. For the I-channel, its expression is

$$M_{\mathrm{DI}} = \frac{I(-d) - I(d)}{I(0)}. \tag{3}$$

M_{DI} follows a Gaussian distribution with a noise variance of

$$\sigma_{\mathrm{DI}}^2(d) = \frac{1}{C/N_0 \cdot T_{coh}}\left[1 - R(2d)\right] \tag{4}$$

where C/N_0 is the CNR, and T_{coh} is the coherent integration time. From (1), the mean of M_{DI} can be derived as

$$\mu_{\mathrm{DI}}(d) = \frac{R(\Delta\tau - d) - R(\Delta\tau + d)}{R(\Delta\tau)\cos(\Delta\varphi) + \alpha_s}\cos(\Delta\varphi). \tag{5}$$

From (5), under H_0 (no spoofing), $\Delta\tau = 0$ and $\mu_{\mathrm{DI}}(d) = 0$; under H_1 (spoofing presence), $\Delta\tau \neq 0$ and $\mu_{\mathrm{DI}}(d) \neq 0$.

2) Ratio metric

The Ratio metric quantifies CCF asymmetry using the normalized sum of E and L correlator outputs. For the I-channel, its expression is

$$M_{\mathrm{RI}} = \frac{I(-d) + I(d)}{I(0)} - \mu_{\mathrm{R}}(d). \tag{6}$$

M_{RI} follows a Gaussian distribution with a direct current (DC) component $\mu_{\mathrm{R}}(d)$ and a noise variance of

$$\sigma_{\mathrm{RI}}^2(d) = \frac{1}{C/N_0 \cdot T_{coh}}\left[1 + R(2d) - 2R^2(d)\right]. \tag{7}$$

From (1), the mean of M_{RI} can be derived as

$$\mu_{\mathrm{RI}}(d) = \frac{\left[R(\Delta\tau - d) + R(\Delta\tau + d)\right]\cos(\Delta\varphi) + 2\alpha_s R(d)}{R(\Delta\tau)\cos(\Delta\varphi) + \alpha_s} - \mu_{\mathrm{R}}(d). \tag{8}$$

To ensure the mean of M_{RI} is 0 under H_0, the DC component of M_{RI} is obtained from (8) as

$$\mu_{\mathrm{R}}(d) = 2R(d). \tag{9}$$

Further, the mean of M_{RI} under $\mathrm{H_1}$ is

$$\mu_{\mathrm{RI}}(d) = \frac{R(\Delta\tau - d) + R(\Delta\tau + d) - 2R(d)R(\Delta\tau)}{R(\Delta\tau)\cos(\Delta\varphi) + \alpha_s}\cos(\Delta\varphi). \quad (10)$$

As indicated by the above analysis, both Delta and Ratio metrics are Gaussian variables with a mean of 0 under $\mathrm{H_0}$. For a specific Gaussian variable M_x with standard deviation σ_x and mean 0 under $\mathrm{H_0}$, the detection threshold T_x corresponding to a given false alarm rate (FAR) $\mathrm{P_F}$ is calculated by

$$\mathrm{P_F} = 1 - \int_{-T_x}^{T_x} \frac{1}{\sqrt{2\pi}\sigma_x} e^{-\frac{x^2}{2\sigma_x^2}} dx = erfc\left(\frac{T_x}{\sqrt{2}\sigma_x}\right). \quad (11)$$

In subsequent experiments, $\mathrm{P_F}$ was set to 10^{-5} for calculations of T_x. Correspondingly, the theoretical detection probability when the mean of M_x is μ_x under $\mathrm{H_1}$ is

$$\mathrm{P_D} = \int_{T_x}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_x} e^{-\frac{(x-|\mu_x|)^2}{2\sigma_x^2}} dx = \frac{1}{2} erfc\left(erfc^{-1}(\mathrm{P_F}) - \frac{|\mu_x|}{\sqrt{2}\sigma_x}\right). \quad (12)$$

Based on the derived (4), (5), (7), (10), (11), and (12), the theoretical detection probabilities of Delta and Ratio can be numerically calculated for different values of relative delay and phase between spoofing and authentic signals. In these calculations, the amplitude gain of the spoofing signal is set to 0.4 dB, C/N_0 is 45 dB·Hz, and T_{coh} is 1 ms. Since spoofing signals with a relative delay exceeding 2 chip cannot interfere with the receiver tracking loop, the relative delay range is limited to 0~2 chip. Fig. 2 shows the theoretical detection probabilities of Delta and Ratio when $\Delta\varphi = 0$, $\Delta\tau$ varies from 0 to 2 chip at 0.1 chip intervals, and d varies from 0 to 2 chip at 0.1 chip intervals. The highest theoretical detection probability is achieved when $d = \Delta\tau$. This highlights the limitation of classical single-correlator SQM metrics in consumer scenarios, where spoofing delays are often time varying.

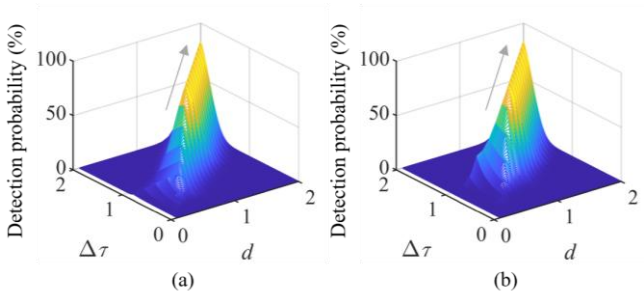

Fig. 2. Theoretical detection probabilities of (a) Delta and (b) Ratio under different relative delays and correlator spacings.

Fig. 3 further shows the theoretical detection probabilities of Delta and Ratio when $\Delta\tau$ =0.9 chip and $\Delta\varphi$ takes values of 0, 0.2π, 0.25π, and 0.5π rad. First, for any $\Delta\varphi$, the detection probability peaks when d = 0.9 chip (i.e., $d = \Delta\tau$), and Delta and Ratio exhibit similar performance (with Delta slightly outperforming Ratio). This indicates that improving detection probability depends more on matching correlator spacing to spoofing delay than on metric type. However, in real consumer scenarios, spoofing delays are dynamic, making it challenging to maintain reliable detection with a single pair of correlators. Second, as $\Delta\varphi$ increases from 0 to 0.5π rad, signal energy gradually shifts from the I-channel to the Q-channel. This causes the detection probabilities of Delta and Ratio (calculated using only I-channel outputs) to decrease significantly, even dropping to nearly 0 when $\Delta\varphi$ = 0.5π rad. This underscores the necessity of fusing I/Q channel data to ensure robust detection across varying phase conditions.

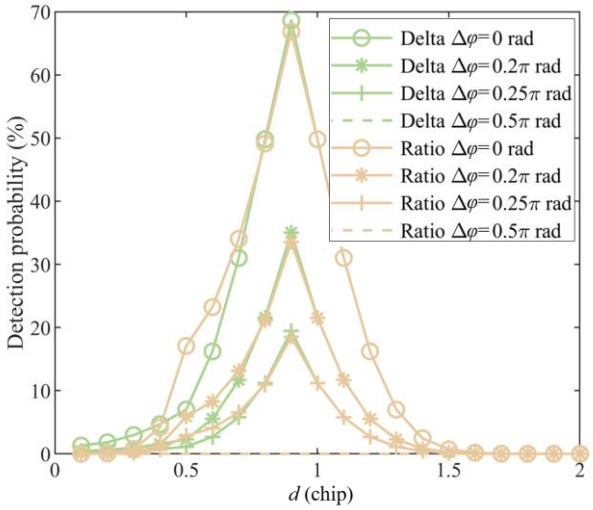

Fig. 3. Theoretical detection probabilities of Delta and Ratio under different relative phases and correlator spacings.

B. Linear Weighted Multi-Correlator SQM and Its Constraints

To address the limitations of single-correlator SQM metrics, multi-correlator fusion methods have been proposed. These methods use multiple pairs of E/L correlators with different spacings to cover a wider range of $\Delta\tau$, which is critical for adapting to time varying spoofing delays. This subsection analyzes the most common fusion method based on linear weighting and proves its theoretical suboptimality using the Cauchy-Schwarz inequality, providing a rationale for adopting nonlinear approaches in consumer electronics.

From the analysis in Section II.A, Delta exhibits slightly higher theoretical detection probability than Ratio under the same spoofing parameters. Thus, Delta is selected as the base metric. A metric group is constructed by configuring N pairs of I/Q complex correlators, where the N pairs are evenly spaced. d_n denotes the spacing of the n-th correlator pair (n = 1, 2, ..., N). The Delta metrics computed from the outputs of the I-channel and Q-channel correlators are abbreviated as DeltaI and DeltaQ respectively. When the correlator interval is d_n, they are denoted as $D_{\mathrm{I}}(d_n)$ and $D_{\mathrm{Q}}(d_n)$

$$\begin{cases} D_{\mathrm{I}}(d_n) = \dfrac{I(-d_n) - I(d_n)}{I(0)} \\ D_{\mathrm{Q}}(d_n) = \dfrac{Q(-d_n) - Q(d_n)}{I(0)} \end{cases}. \quad (13)$$

$D_I(d_n)$ and $D_Q(d_n)$ share the same noise variance, given by

$$\sigma_D^2(d_n) = \frac{1}{C/N_0 \cdot T_{coh}}\left[1 - R(2d_n)\right]. \tag{14}$$

For fusing the metric group, the linearly weighted summation is typically used

$$\begin{cases} C_I = \sum_{n=1}^{N} \beta_n D_I(d_n) \\ C_Q = \sum_{n=1}^{N} \beta_n D_Q(d_n) \end{cases} \tag{15}$$

where $\beta_n \geq 0$ is the weight coefficient. To minimize output noise, weights are generally determined by the reciprocal of the noise standard deviation. The noise variance of the summed metric is [21]

$$\sigma_C^2 = \frac{1}{C/N_0 \cdot T_{coh}} \sum_{m=1}^{N} \beta_m \left(\sum_{n=1}^{N} \beta_n \left[R(d_n - d_m) - R(d_n + d_m) \right] \right). \tag{16}$$

Since $D_I(d_n)$ and $D_Q(d_n)$ have the same noise variance and the I/Q channels are orthogonal, the complete detection metric is obtained via non-coherent accumulation of the two channels

$$C_{IQ} = (C_I)^2 + (C_Q)^2. \tag{17}$$

From (12), when the detection metric follows a Gaussian distribution, the detection probability for a given false alarm rate depends only on the ratio of the mean to the standard deviation (μ_x/σ_x). Fig. 4 presents the theoretical detection probability corresponding to μ_x/σ_x values ranging from 0 to 10. A higher μ_x/σ_x indicates a higher detection probability. For comparing the performance of different detection metrics, the square of this ratio (i.e., the ratio of the mean squared to the variance) is used. This ratio reflects the relative energy of spoofing versus noise; a larger value means stronger spoofing characteristics relative to noise and better detection performance. For clarity, this ratio is defined as the SSNR.

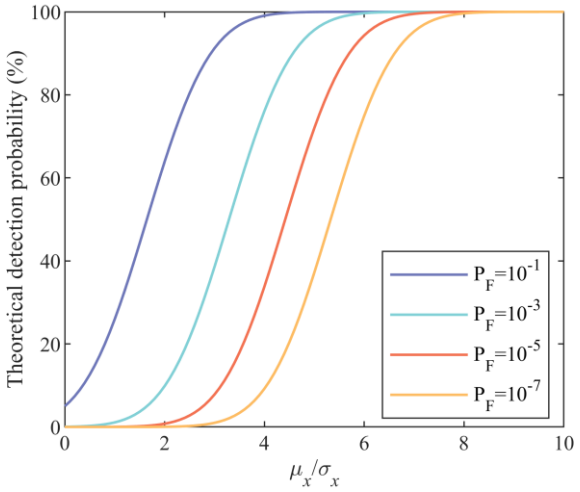

Fig. 4. Theoretical detection probability as a function of the μ_x/σ_x ratio under different false alarm rates.

Taking $D_I(d_n)$ as an example, consider N detection metrics $D_I(d_1)$, $D_I(d_2)$, ⋯, $D_I(d_N)$. From the analysis in Section II.A, the theoretical detection probability is maximized when $\Delta\tau = d_n$. Thus, at any given moment during a spoofing, only one of the N metrics output the maximum SSNR, denoted as M

$$M = SSNR_{\max} = \max_{1 \leq n \leq N} \frac{\left[\mu_{DI}(d_n)\right]^2}{\sigma_D^2(d_n)} \tag{18}$$

where $\mu_{DI}(d_n)$ is the mean of $D_I(d_n)$. Let j be the index of the metric with the maximum SSNR; then M can be expressed as

$$M = SSNR_{\max} = \frac{\left[\mu_{DI}(d_j)\right]^2}{\sigma_D^2(d_j)}. \tag{19}$$

The mean of the weighted sum C_I is

$$E[C_I] = \sum_{n=1}^{N} \beta_n E\left[D_I(d_n)\right] = \sum_{n=1}^{N} \beta_n \mu_{DI}(d_n). \tag{20}$$

Since the correlator spacings satisfy $d_n \geq 0$ and $d_m \geq 0$, it follows that $|d_n - d_m| \leq |d_n + d_m|$. From (2), we obtain $R(d_n - d_m) \geq R(d_n + d_m)$. Consequently, by (16), the covariance between $D_I(d_n)$ and $D_I(d_m)$ is non-negative

$$\begin{aligned} &\mathrm{Cov}\left(D_I(d_n),\ D_I(d_m)\right) \\ &= \frac{1}{C/N_0 \cdot T_{coh}}\left[R(d_n - d_m) - R(d_n + d_m)\right] \geq 0 \end{aligned}. \tag{21}$$

From (21), the noise variance of the weighted sum C_I satisfies

$$\sigma_C^2 \geq \frac{1}{C/N_0 \cdot T_{coh}} \sum_{n=1}^{N} \beta_n^2 \left[1 - R(2d_n)\right] = \sum_{n=1}^{N} \beta_n^2 \sigma_D^2(d_n). \tag{22}$$

Using (20), (22), and Cauchy-Schwarz inequality, the SSNR of the weighted sum C_I satisfies the following inequality

$$\begin{aligned} R_{SSNR} &= \frac{\left(E[C_I]\right)^2}{\sigma_C^2} \leq \frac{\left(\sum_{n=1}^{N} \beta_n \mu_{DI}(d_n)\right)^2}{\sum_{n=1}^{N} \beta_n^2 \sigma_D^2(d_n)} \\ &\leq \frac{\left(\sum_{n=1}^{N} \beta_n^2\right)\left(\sum_{n=1}^{N} \left(\mu_{DI}(d_n)\right)^2\right)}{\sum_{n=1}^{N} \beta_n^2 \sigma_D^2(d_n)} \leq \frac{\left(\sum_{n=1}^{N} \beta_n^2\right)\left(\sum_{n=1}^{N} M \sigma_D^2(d_n)\right)}{\sum_{n=1}^{N} \beta_n^2 \sigma_D^2(d_n)} \\ &= M \frac{\left(\sum_{n=1}^{N} \beta_n^2\right)\left(\sum_{n=1}^{N} \sigma_D^2(d_n)\right)}{\sum_{n=1}^{N} \beta_n^2 \sigma_D^2(d_n)} \leq M \frac{\sum_{n=1}^{N} \beta_n^2 \sigma_D^2(d_n)}{\sum_{n=1}^{N} \beta_n^2 \sigma_D^2(d_n)} = M \end{aligned}. \tag{23}$$

Inequality (23) indicates the SSNR of the weighted sum does not exceed the maximum SSNR M among the original N metrics. The equality in the Cauchy-Schwarz inequality holds only if $\beta_n/\mu_{DI}(d_n)$ is constant for all n. However, in real consumer scenarios, spoofing signal parameters (e.g., $\Delta\tau$, $\Delta\varphi$) are unknown and time varying, which means $\mu_{DI}(d_n)$ is also

unknown and time varying. A fixed weighting scheme cannot achieve the maximum SSNR output, so the detection probability cannot reach the upper bound of a single metric.

An alternative approach to multi-correlator fusion is "OR-gate decision-making," where spoofing is declared if any metric exceeds the threshold [18]. However, this method requires distributing the total false alarm rate across multiple metrics. From (12), reducing the false alarm rate for individual metrics leads to a decrease in detection probability.

C. Nonlinear Advantages of Neural Networks

Classical SQM metrics are limited by their reliance on single correlator pairs, making them unable to adapt to time varying spoofing. Linearly weighted multi-correlator fusion methods expand feature coverage but are constrained by the Cauchy-Schwarz inequality, preventing them from reaching the theoretical SSNR upper bound. OR-gate decision-making reduces detection probability due to false alarm rate distribution. Thus, introducing nonlinear fusion mechanisms is critical to overcoming these limitations and improving spoofing detection performance, and neural networks provide both theoretical support and technical pathways for this goal.

From a theoretical perspective, the universal approximation theorem states that a feedforward neural network with hidden layers (equipped with nonlinear activation functions) can approximate any continuous nonlinear function defined on a compact set to arbitrary precision [37]. This is vital for fusing multi-correlator features to detect spoofing, as complex non-linear relationships are present between multi-correlator outputs (e.g., Delta metrics from I/Q channels with different spacings) and spoofing states (relative delay, phase, amplitude). Moreover, the universal approximation theorem provides flexibility in network design without necessitating the prior construction of mathematical models. Data-driven learning enables the generation of feature fusion. This generality is essential for deploying SQM in diverse GNSS-enabled consumer devices.

From the perspective of practical detection requirements, the dynamic characteristics of spoofing signals further demand that detection models possess temporal dependency modeling capabilities, which is another key advantage of neural networks. Spoofing signals exhibit slow time varying behavior. Relative delay gradually changes across frames, and relative phase shifts due to environmental propagation effects or spoofing device instability. Linear weighting and single-time-step feature extraction methods only focus on multi-correlator outputs at the current frame. They cannot use historical frame information to distinguish between random noise interference and sustained dynamic changes in spoofing signals, leading to missed detections or false alarms. Neural networks, especially those with temporal modeling capabilities, such as 2-dimensional (2D) CNNs, effectively address this issue. By treating continuous frames of multi-correlator outputs as temporal inputs, the network can automatically learn the dynamic evolution rules of spoofing. Meanwhile, temporal modeling enhances noise robustness. By smoothing and correlating features across frames, transient noise-induced anomalies are suppressed, and the network can focus on the sustained dynamic features of spoofing signals.

III. SpoofConvNet Based Detection Scheme

To address the limitations of traditional SQM methods, this section proposes a GNSS spoofing detection scheme based on a dedicated convolution network (named SpoofConvNet). This scheme is tailored for consumer electronics, as it breaks through the bottlenecks of linear modeling, adapts to the spatiotemporal characteristics of GNSS signals, and enables efficient detection of both static and dynamic spoofing scenarios through end-to-end feature learning.

A. Overall Architecture

From the preceding analysis, classical SQM metrics, relying on single correlator pairs, fail to continuously capture dynamic spoofing features, while linearly weighted multi-correlator fusion methods cannot reach the theoretical SSNR upper bound. To address these issues, this scheme adopts a three-stage detection framework: multi-correlator spatiotemporal feature input → end-to-end convolutional neural network processing → spoofing state output, as shown in Fig. 5. Each module works synergistically to achieve integrated functions of feature extraction, noise suppression, and classification decision-making. The core goal is to break the limitations of linear methods through nonlinear modeling while enhancing detection robustness in complex consumer scenarios.

The scheme's key innovations align with the hardware capabilities and application demands of consumer electronics. First, it replaces traditional linear weighting with the local feature extraction and nonlinear mapping of CNNs. This fundamentally resolves the theoretical suboptimality of linear methods proven in Section II. Through multi-layer nonlinear transformations, the network adaptively explores the deep coupling relationships between multi-correlator features and spoofing states. It does not require pre-defined fixed weights, allowing it to adapt to time varying spoofing parameters. Second, it integrates GNSS signal physical characteristics with convolutional network technology by designing a shared encoder structure. This structure extracts spatiotemporal features from multi-correlators while suppressing noise, eliminating the need for additional filtering modules. This simplifies the detection process and avoids increased latency from multi-module cascading, which is essential for consumer devices that demand low-latency responses (e.g., real-time positioning in ride-hailing apps). Third, the network structure is deeply adapted to the 2D spatiotemporal characteristics of GNSS signals. Spoofing interference manifests in two ways: spatial anomalies (e.g., pseudorange offsets) and temporal anomalies (e.g., gradual delay shifts). The scheme uses 2D convolutions to capture both types of features simultaneously, addressing the limitation of traditional static models (e.g., multilayer perceptron (MLP)) that only process global statistical information. This enables accurate detection of

dynamic spoofing scenarios common in consumer applications.

B. Signal Input Layer Design

The core function of the input layer is to convert the raw outputs of multi-correlators in GNSS receivers into a spatiotemporal feature format suitable for network modeling. Its dimensional design strictly follows the physical characteristics of GNSS signals and the spoofing detection requirements of consumer electronics, ensuring compatibility with the hardware constraints of devices like smartphones and smart wearables. Specifically, the input data is defined as a 3-dimensional (3D) tensor (H, W, C), where each dimension's value and meaning are determined based on the spoofing detection needs.

For the spatial dimension (H = 20), it corresponds to the distribution range of Delta metric groups. Since spoofing signals require a relative delay of 0~2 chip to interfere with the tracking loop, 20 pairs of correlators are spaced at 0.1 chip intervals. Each correlator output includes amplitude and correlation peak energy information from both I and Q channels. This design ensures full coverage of potential delay offsets of spoofing signals, which is critical for adapting to dynamic delay changes.

For the temporal dimension (W = 100), it corresponds to the temporal observation window of GNSS signals. Combined with the 10 Hz update rate of consumer-grade GNSS receivers, the tracking loop update at 1000 Hz under T_{coh} = 1 ms, with 100 consecutive frames corresponding to a 0.1 s observation window. This duration is sufficient to capture the slow time varying characteristics of dynamic spoofing signals, preventing the loss of dynamic features due to an overly short window.

For the channel dimension (C = 2), it corresponds to the I and Q channels of GNSS receivers. As analyzed in Section II, signal energy gradually shifts from the I-channel to the Q-channel as the relative phase $\Delta\varphi$ increases from 0 to 0.5π rad. Relying on a single channel can significantly reduce detection probability. By inputting data from both I and Q channels, the network fully utilizes the complete energy information of signals, enhancing detection robustness under phase offset conditions common in urban consumer environments (e.g., signal reflections in canyons).

C. Feature Processing Layer Design

The feature processing layer is the core of SpoofConvNet, as it realizes the integrated functions of noise suppression, feature extraction, and classification decision-making. It adopts an integrated structure of "shared encoder + classifier". The shared encoder is responsible for spatiotemporal feature extraction and noise suppression, while the classifier determines the spoofing state based on the extracted features. The overall design balances detection performance and engineering practicality, with a focus on meeting the lightweight requirements of consumer electronics.

1) Shared Encoder (with Temporal Denoising Capability)

The shared encoder adopts a feature extraction architecture based on 2D convolutions to capture the spatiotemporal joint features of multi-correlator outputs while suppressing random noise. The first layer is a 2D convolution with a 3×3 kernel, 64 filters, and "same" padding. The 3×3 kernel can simultaneously cover a local window of "3 adjacent correlators (spatial dimension) + 3 consecutive observation frames (temporal dimension)". This design is suited to the local anomaly characteristics of GNSS spoofing signals, such as output offsets of specific correlators over a short time period. The 64 filters are used to extract different types of local spatiotemporal features, including spatial distribution anomalies and temporal gradual changes. A batch normalization layer and rectified linear unit (ReLU) activation function follow the convolution layer. Batch normalization accelerates network training convergence and alleviates overfitting. The ReLU activation function introduces nonlinearity into the network, enabling it to model complex relationships between features and spoofing states. The second layer is a 2D convolution symmetric to the first, but with the number of filters reduced to 32. This design retains key features while reducing the network parameter scale, avoiding excessive computational overhead that hinders deployment on resource-constrained consumer devices (e.g., smartwatches with limited processing power). It also uses batch normalization and ReLU activation to further enhance feature extraction and noise suppression.

In terms of functionality, the shared encoder offers the advantage of integrated feature extraction and noise suppression. The local receptive field of 2D convolutions focuses on local anomaly regions of spoofing signals (e.g., 3–5 frames when spoofing begins), effectively filtering out global random noise interference. The batch normalization layer further weakens the impact of noise on feature distribution. Unlike traditional methods that require additional filtering modules, this integrated design reduces latency and hardware complexity, making it more suitable for integration into consumer GNSS receiver chips.

2) Classifier (Directly Connected to the Encoder)

The classifier is designed based on a combination of convolution, pooling, global fusion, and fully connected layers. Its core goal is to convert the high-dimensional spatiotemporal features extracted by the shared encoder into binary classification results (no spoofing/spoofing present). It also adopts lightweight design strategies to meet the real-time requirements of consumer applications. Its structural design is detailed as follows.

First, a 2D convolution layer with a 3×3 kernel, 64 filters, and "same" padding is used. It is paired with a batch normalization layer and ReLU activation function to further refine the features output by the encoder. This step enhances the distinguishability between spoofing features and normal signal features, which is critical for reducing false alarms.

Next, a 2×2 max-pooling layer is added. This layer reduces the dimension of feature maps through subsampling, lowering the computational load of subsequent layers while retaining

key information. This lightweight design is essential for deploying the network on consumer devices with limited battery life and computing power.

After pooling, a global average pooling (GAP) layer compresses the 2D feature maps into a 1-dimensional (1D) vector. By calculating the global mean of each feature channel, the GAP layer eliminates interference from local redundant information and avoids the parameter explosion issue caused by directly flattening features.

Finally, two fully connected layers are included with 128 dimensions (for feature dimension conversion and nonlinear mapping), and 2 dimensions (corresponding to the two classes of "no spoofing" and "spoofing present"). A Softmax function outputs the probability distribution of the two classes. If the probability of "spoofing present" is ≥0.5, the current observation window is determined to contain a spoofing; otherwise, it is determined to have no spoofing.

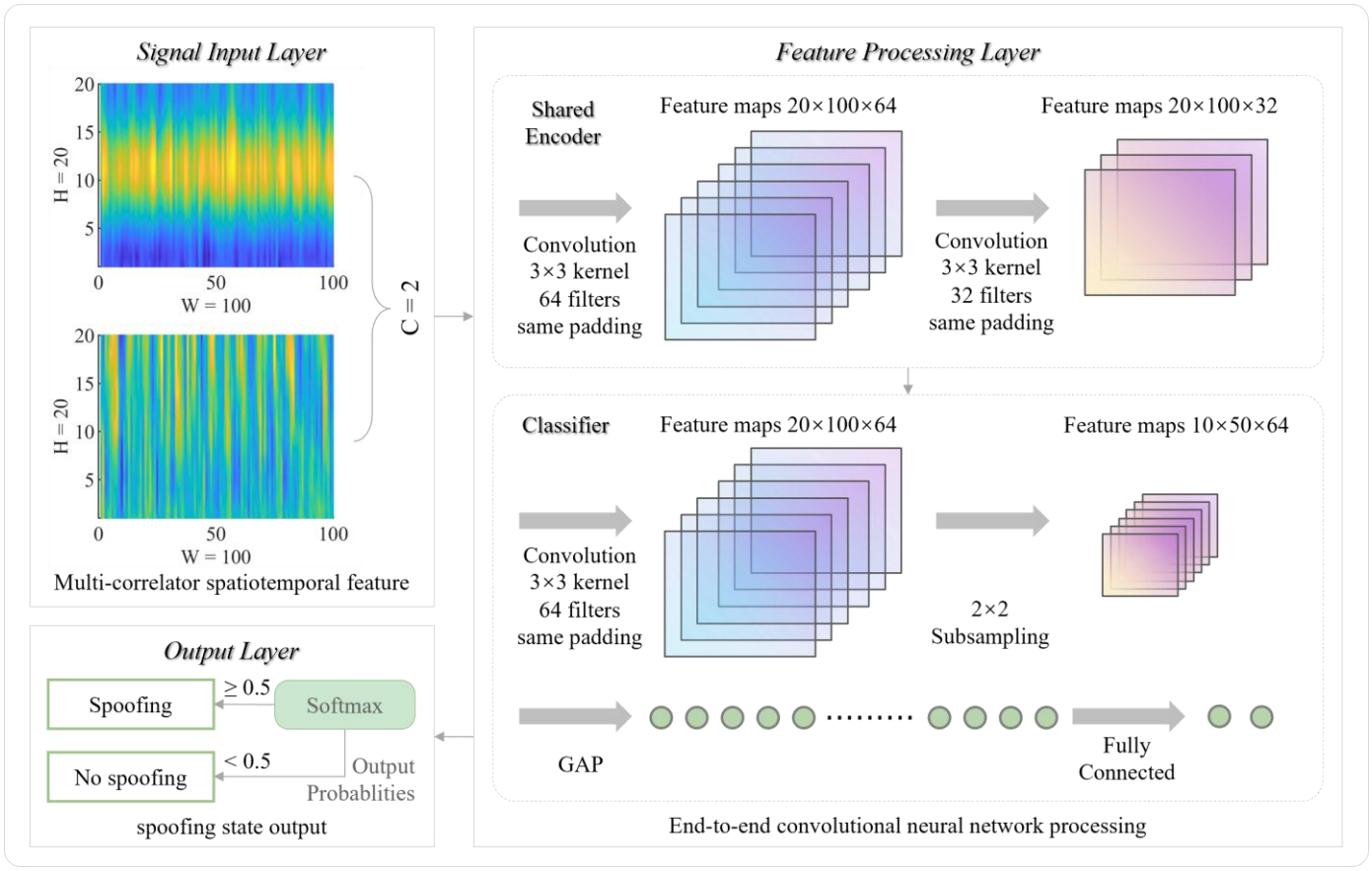

Fig. 5. Proposed SpoofConvNet-based spoofing detection framework.

IV. Experimental Validation

In this section, the effectiveness of the proposed SpoofConvNet for consumer-centric GNSS spoofing detection is validated through multi-dimensional experiments in both static (time/position) and dynamic (time/position) spoofing cases. A quantitative analysis is conducted to indicate the advantages of SpoofConvNet in enhancing detection, adapting to resource-constrained consumer devices, and maintaining strong generalization across unseen scenarios.

A. Experimental Setup and Dataset Configuration

The experiment was conducted on Nankai University's campus (Tianjin, China), a hybrid urban-suburban environment with semi-occluded (building-lined paths) and open (plazas) areas, which is typical of consumer GNSS use cases, as shown in Fig. 6. Two key systems were deployed: a reference receiver system for collecting authentic GNSS data, and a spoofing-transceiver system for simulating controlled attacks. The reference system used a consumer-grade multi-constellation GNSS receiver (u-blox NEO-M8T) with a patch antenna, mounted on the rooftop of the unmanned aerial vehicle to collect authentic data. This included static position and dynamic trajectory data. The spoofing-transceiver system, designed for low cost and consumer compatibility, used a HackRF One to produce hybrid signals (authentic + spoofing). Spoofing parameters (amplitude gain: 6 dB, time delay: 0~2 chip, position offset: 0~600 m) simulated real-world attacks, while a compact smartphone-sized antenna and software receiver replicated signal processing.

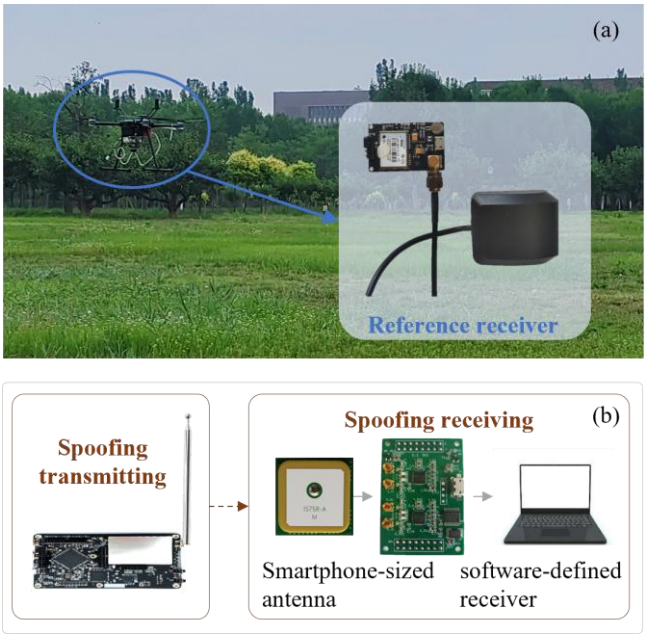

Fig. 6. Experimental scenario and setup. (a) Reference receiver deployment in a semi-occluded campus environment; (b) Configuration of the spoofing-transceiver system.

The signal workflow followed a consumer-relevant pipeline: authentic baseband signals were generated using reference receiver data and ephemeris, while spoofing signals targeted four common consumer scenarios (static time/position spoofing, dynamic time/position spoofing). Hybrid signals were up-converted to the 1575.42 MHz and transmitted, then received by the software receiver, down-converted to intermediate frequency, and recorded for analysis.

The test dataset included 16,000 samples, with 2,000 "no spoofing" and 2,000 "spoofing" samples per scenario, covering a CNR range of 40~50 dB·Hz (reflecting noisy urban to open consumer environments). Samples were formatted as 3D tensors [H=20, W=100, C=2] to match SpoofConvNet's input design. Training used a consumer-grade processor with an Adam optimizer (initial learning rate 0.001), batch size 64, 50 epochs (with early stopping), and L2 regularization.

B. Comparison with Traditional Methods

Fig. 7 shows the detection rate of DeltaI under static time spoofing, with varying spoofing delays (0~2 chip) and correlator spacings (0~2 chip) across different CNR levels. As CNR decreases from 50 to 40 dB·Hz, the overall detection rate declines. For any given CNR, the highest detection rate occurs when the correlator spacing matches the spoofing delay, which aligns with the theoretical analysis in Section II. Furthermore, Fig. 8 presents the complementary performance of DeltaI and DeltaQ when the correlator spacing is fixed at 1.4 chip. Both metrics achieve high detection rates when the spoofing delay is near 1.4 chip, but their performance diverges in two intervals: in Interval A, DeltaI outperforms DeltaQ; in Interval B, DeltaQ is superior. This validates the necessity of fusing I/Q channel data.

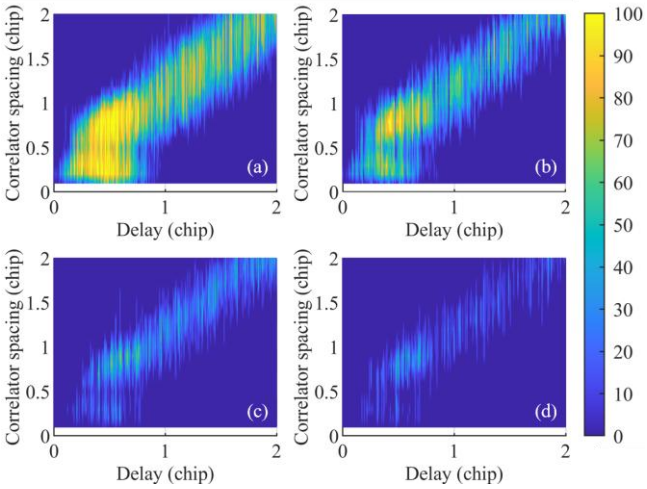

Fig. 7. Detection rates of DeltaI under static time spoofing for different spoofing delays and correlator spacings under (a) CNR = 50 dB·Hz, (b) CNR = 48 dB·Hz, (c) CNR = 45 dB·Hz, and (d) CNR = 40 dB·Hz.

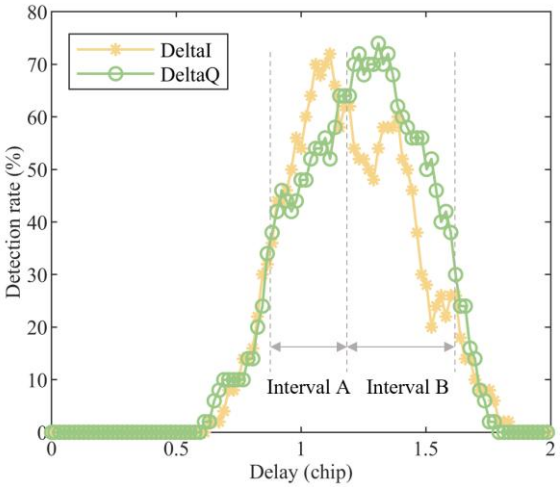

Fig. 8. Detection rates of DeltaI and DeltaQ for varying spoofing delays (correlator spacing = 1.4 chip).

To validate SpoofConvNet's superiority over traditional multi-correlator fusion methods, we compare its performance with two classical linear methods: Kalman-filtered linear weighted SQM (Kalman + Weight) and Kalman-filtered OR-gate SQM (Kalman + Or gate). Both traditional methods use Kalman filtering to smooth raw metrics but differ in fusion logic. Fig. 9 shows the real-time detection rates of the two traditional methods and SpoofConvNet under static time spoofing across different CNR levels. SpoofConvNet reaches a 100% detection rate faster than both traditional methods in all CNR scenarios. This low latency is critical for consumer applications, where delayed spoofing alerts can disrupt user experience.

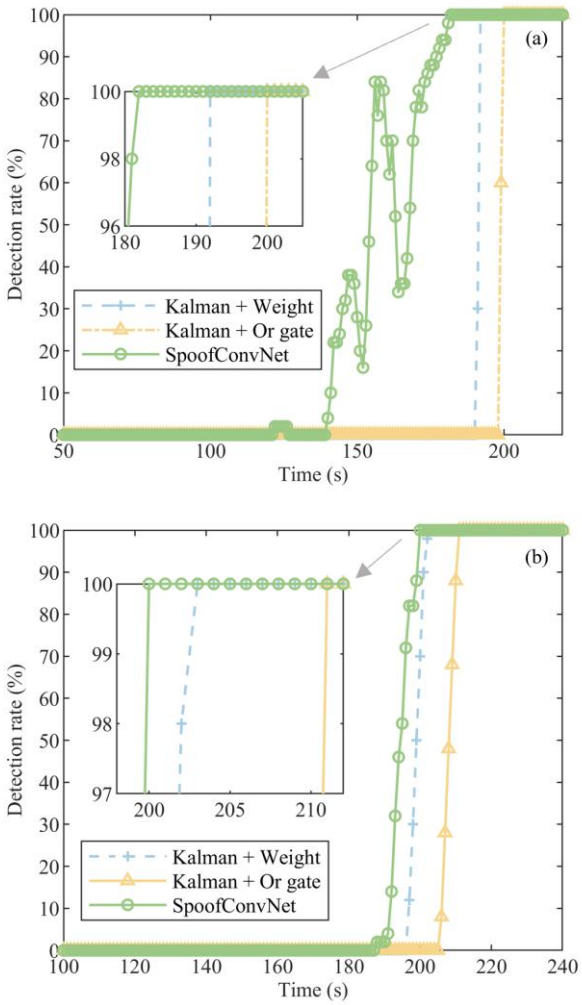

Fig. 9. Real-time detection rates under static time spoofing under (a) CNR = 50 dB·Hz, and (b) CNR = 45 dB·Hz.

To quantify performance across all scenarios, Fig. 10 presents the average detection rates of the three methods during spoofing pull-off. Traditional methods show significant performance variation. Kalman + Weight reaches 88.41% in static time spoofing but drops to 70.49% in static position spoofing, while Kalman + Or gate falls to 55.99% in static position spoofing. In contrast, SpoofConvNet maintains an average detection rate exceeding 90% across all four scenarios, demonstrating stable performance.

C. Comparison with Other Neural Network Architectures

To further highlight SpoofConvNet's advantages, we compare it with three mainstream neural networks (MLP, bidirectional LSTM (BiLSTM), and Transformer), configured with the same input dimension [20, 100, 2] and trained under identical conditions. Fig. 11 shows the receiver operating characteristic (ROC) curves of all four networks across the four spoofing scenarios. SpoofConvNet's ROC curve is consistently closest to the top-left corner, indicating the best balance between detection rate and false alarm rate. This advantage is most pronounced in time spoofing scenarios (Figs. 11(a) and (c)).

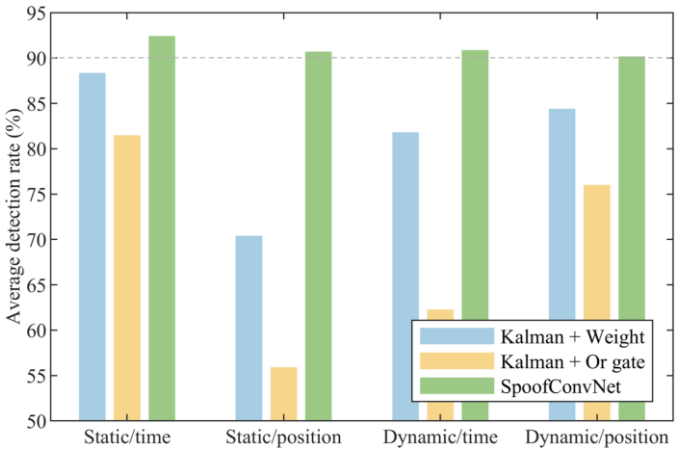

Fig. 10. Average detection rates across four scenarios.

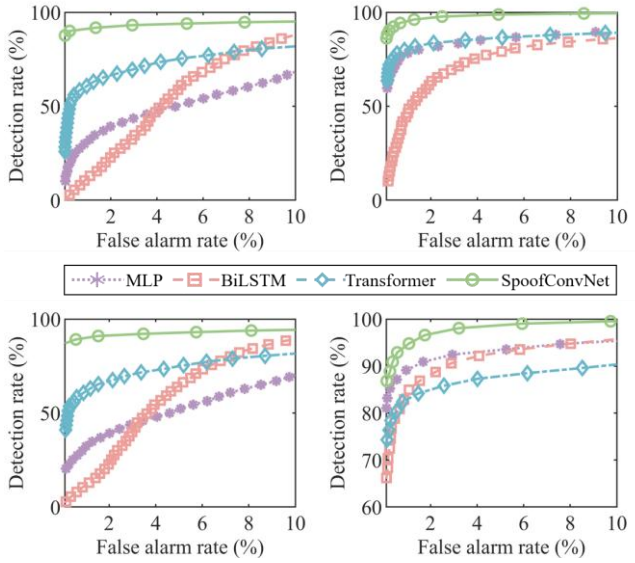

Fig. 11. ROC curves of different networks across four spoofing scenarios with (a) static time spoofing, (b) static position spoofing, (c) dynamic time spoofing, and (d) dynamic position spoofing.

Figs. 12 and 13 present detection rates and false alarm rates versus CNR (40~50 dB·Hz). As CNR increases, all networks show higher detection rates and lower false alarm rates. Regarding detection rate, BiLSTM and SpoofConvNet outperform MLP and Transformer at all CNR levels. Specially, at 48 dB·Hz, SpoofConvNet reaches peak detection rates of 99.49% (static time) and 99.28% (dynamic time), which is the highest among all networks. Regarding the false alarm rate, SpoofConvNet achieves the lowest overall level among all compared models, and nearly all its results across CNR levels are below 10%. The isolated outlier in Fig. 13(c) that slightly exceeds 10% is statistically negligible and does not reflect the model's general performance. BiLSTM, by comparison, shows a distinctly higher false alarm rate across the board.

Table I summarizes performance across all scenarios and CNR levels. SpoofConvNet achieves the highest area under curve (AUC) (0.9840), a detection rate (92.68%) comparable to BiLSTM (93.95%), and the lowest false alarm rate (1.75%).

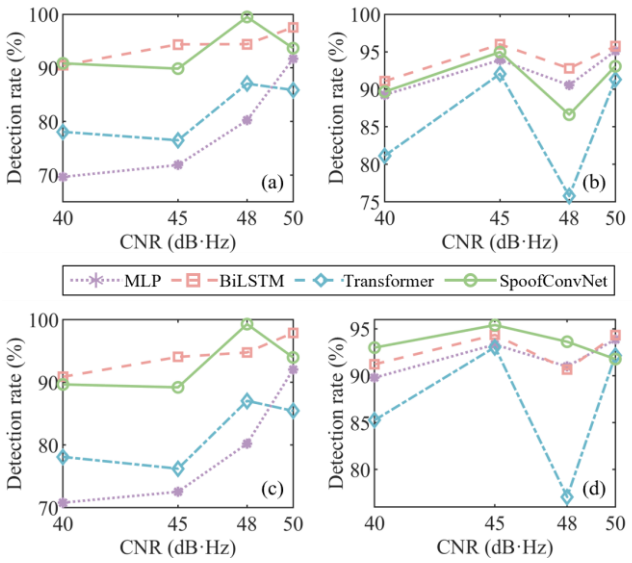

Fig. 12. Detection rates vs. CNR under (a) static time spoofing, (b) static position spoofing, (c) dynamic time spoofing, and (d) dynamic position spoofing.

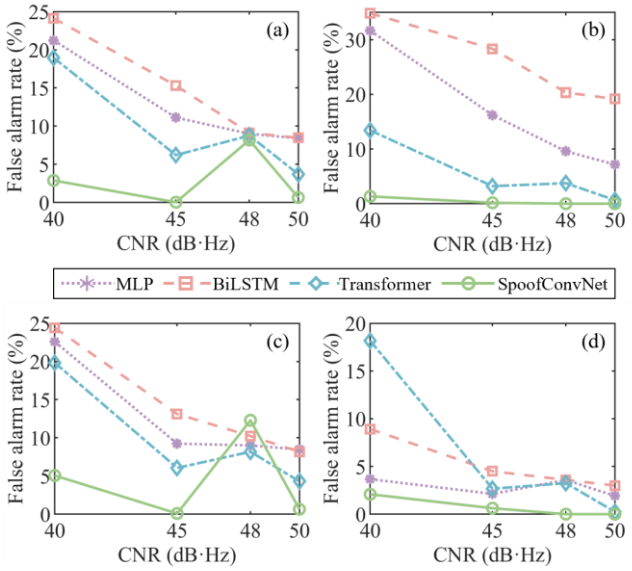

Fig. 13. False alarm rates vs. CNR under (a) static time spoofing, (b) static position spoofing, (c) dynamic time spoofing, and (d) dynamic position spoofing.

TABLE I
PERFORMANCE SUMMARY OF ALL NETWORKS

Network	AUC	P_D (%)	P_F (%)
MLP	0.9437	84.90	10.70
BiLSTM	0.9571	93.95	14.85
Transformer	0.9392	84.00	7.00
SpoofConvNet	**0.9840**	92.68	1.75

D. Ablation Studies

To verify the necessity of SpoofConvNet's core modules, including 2D convolution for spatiotemporal modeling and GAP for feature aggregation, two ablation models were tested under the same training and test conditions. The first ablation model, SpoofConvNet-1D, replaces all 3×3 2D convolutions with 3×1 1D convolutions, which only extract spatial features from correlator distributions without capturing temporal dependencies between consecutive frames. The second ablation model, SpoofConvNet-noGAP, removes the GAP layer from the classifier and directly flattens the 2D feature maps output by the max-pooling layer before feeding them into the fully connected layers.

Table II shows the performance of the ablation models with the original SpoofConvNet. SpoofConvNet-1D shows a 1.80% drop in AUC (to 0.9660) and a significant 10.05% increase in false alarm rate (to 11.80%), even as its detection rate only decreases slightly (to 92.28%). This confirms that 2D convolution is critical for distinguishing noise-induced random fluctuations from spoofing-induced temporal trends. For SpoofConvNet-noGAP, AUC decreases by 0.82% (to 0.9758) and false alarm rate rises by 5.05% (to 6.80%), while detection rate remains stable at 92.58%. This indicates that GAP suppresses interference from local noise by averaging feature values across each channel, which is essential for maintaining low false alarms. These results validate that 2D convolution and GAP are key to SpoofConvNet's superior performance, especially in the noise-prone, resource-constrained environments typical of consumer electronics.

TABLE II
PERFORMANCE OF ABLATION MODELS

Network	AUC	P_D (%)	P_F (%)
SpoofConvNet	0.9840	92.68	1.75
SpoofConvNet-1D	0.9660	92.28	11.80
SpoofConvNet-noGAP	0.9758	92.58	6.80

F. Generalization Performance on the TEXBAT Dataset

To further validate SpoofConvNet's adaptability to real-world consumer scenarios, cross-dataset testing was conducted on the TEXBAT, which is a public benchmark with real spoofing cases (Case 2~Case 8). No model fine-tuning was performed to simulate the practical deployment of SpoofConvNet on off-the-shelf consumer devices, where retraining or parameter adjustment is not feasible for end users.

Table III presents SpoofConvNet's performance on each

TEXBAT case. The model maintains high AUC values (>0.95) and detection rates (>88%), with an average AUC of 0.9786, only 0.54% lower than its performance on the self-constructed dataset, and an average detection rate of 90.84%. The false alarm rate remains below 10% for all cases. This consistent generalization across unseen data distributions confirms SpoofConvNet's practical value for consumer electronics.

TABLE III
SPOOFCONVNET'S PERFORMANCE ON TEXBAT DATASET

Case	AUC	P_D (%)	P_F (%)
2	0.9822	93.63	7.52
3	0.9695	88.84	0.43
4	0.9675	89.91	0.89
5	0.9543	90.92	3.96
6	0.9754	91.68	5.33
7	0.9919	90.31	0.49
8	0.9893	90.56	1.33

V. CONCLUSION AND DISCUSSION

We have presented a dedicated spoofing convolution network (SpoofConvNet) to address global navigation satellite system (GNSS) spoofing detection challenges in consumer electronics, where traditional methods suffer from linear suboptimality, poor dynamic adaptability, and hardware mismatches. Theoretically, this study defines the spoofing signal-to-noise ratio (SSNR) to quantify detection performance and uses the Cauchy-Schwarz inequality to prove that linear weighted multi-correlator fusion cannot reach the theoretical SSNR upper bound, providing a basis for adopting nonlinear models. Regarding architecture, SpoofConvNet's three-stage framework (multi-correlator spatiotemporal input, end-to-end convolutional neural network processing, and spoofing state output) is tailored for consumer devices. The shared encoder integrates spatiotemporal feature extraction and noise suppression, 2D convolutions capture both spatial correlator anomalies and temporal frame trends and the lightweight design fits mid-range consumer hardware constraints. Experiments validate that compared with traditional methods, SpoofConvNet maintains an average detection rate of 90%+. Versus mainstream neural networks, it achieves the highest area under curve (AUC) (0.9840). Cross-dataset testing on TEXBAT confirms generalization, with average AUC 0.9786 and detection rate 90.84%.

SpoofConvNet balances performance, efficiency, and hardware compatibility, offering a practical anti-spoofing solution for consumer GNSS devices. Future work will integrate low-power inertial data for weak-signal scenarios, expand to multi-constellation support, and compress the model for entry-level devices.

REFERENCES

[1] J. Wang, M. Xia, D. Zhang, W. Wen, W. Chen, and C. Shi, "Urban GNSS positioning for consumer electronics: 3D mapping and advanced signal processing," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 7059–7072, May 2025, doi: 10.1109/TCE.2025.3552892.

[2] M. Yuan, X. Tang, and G. Ou, "Authenticating GNSS civilian signals: A survey," *Satell. Navigat.*, vol. 4, no. 1, Feb. 2023, Art. no. 6.

[3] K. Rothrock, "The Kremlin eats GPS for breakfast," *The Moscow Times*, Oct. 21 2016. [Online]. Available: https://www.themoscowtimes.com/2016/10/21/the-kremlin-eats-gps-for-breakfast-a55823. [Accessed: Dec. 8 2025].

[4] J. Wang, L. Nie, Z. Gu, J. Wang, R. Tan, and S. Kumari, "Real-time GPS spoofing detection in consumer drones through multi-sensor data fusion and timesNet," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 5569–5583, May 2025, doi: 10.1109/TCE.2025.3560264.

[5] Y. Gao, Z. Lv, and L. Zhang, "Asynchronous lift-off spoofing on satellite navigation receivers in the signal tracking stage," *IEEE Sensors J.*, vol. 20, no. 15, pp. 8604–8613, Aug. 2020, doi: 10.1109/jsen.2020.2984525.

[6] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS signal authentication via power and distortion monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739–754, Apr. 2018.

[7] A. M. Khan, N. Iqbal, A. A. Khan, M. F. Khan, and A. Ahmad, "Detection of intermediate spoofing attack on global navigation satellite system receiver through slope based metrics," *J. Navigat.*, vol. 73, no. 5, pp. 1052–1068, 2020.

[8] C. Sun, J. W. Cheong, A. G. Dempster, H. Zhao, L. Bai, and W. Feng, "Robust spoofing detection for GNSS instrumentation using q-channel signal quality monitoring metric," *IEEE Trans. Instrum. Meas.*, vol. 70, Aug. 2021, Art. no. 8504115, doi: 10.1109/tim.2021.3102753.

[9] W. Wang, and Y. Hou, "GNSS induced spoofing detection based on dynamic 3-D correlation function," *IEEE Trans. Instrum. Meas.*, vol. 73, Nov. 2024, Art. no. 8507918, doi: 10.1109/TIM.2024.3472768.

[10] X. Shang, F. Sun, D. Wang, K. Xiao, S. Dou, X. Lu, and J. Sun, "GNSS spoofing detection based on multicorrelator distortion monitoring," *GPS Solutions*, vol. 27, no. 2, Apr. 2023, Art. no. 94.

[11] X. Shang, F. Sun, L. Zhang, J. Cui, and Y. Zhang, "Detection and mitigation of GNSS spoofing via the pseudorange difference between epochs in a multicorrelator receiver," *GPS Solutions*, vol. 26, no. 2, Apr. 2022, Art. no. 37, doi: 10.1007/s10291-022-01224-4.

[12] F. Rothmaier, Y.-H. Chen, S. Lo, and T. Walter, "A framework for GNSS spoofing detection through combinations of metrics," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 57, no. 6, pp. 3633–3647, Dec. 2021.

[13] E. Schmidt, N. Gatsis, and D. Akopian, "A GPS spoofing detection and classification correlator-based technique using the LASSO," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 6, pp. 4224–4237, Dec. 2020.

[14] C. Sun *et al.*, "Moving variance-based signal quality monitoring method for spoofing detection," *GPS Solutions*, vol. 22, no. 3, Jul. 2018, Art. no. 83, doi: 10.1007/s10291-018-0745-7.

[15] W. Zhou, Z. Lv, G. Li, B. Jiao, and W. Wu., "Detection of spoofing attacks on global navigation satellite systems using Kolmogorov-Smirnov test-based signal quality monitoring method," *IEEE Sensors J.*, vol. 24, no. 7, pp. 10474–10490, Apr. 2024, doi: 10.1109/jsen.2024.3354110.

[16] J. Fang, J. Yue, B. Xu, and L.-T. Hsu, "A post-correlation graphical way for continuous GNSS spoofing detection," *Measurement*, vol. 216, Jul. 2023, Art. no. 112974, doi: 10.1016/j.measurement.2023.112974.

[17] M. R. Mosavi, Z. Nasrpooya, and M. Moazedi, "Advanced anti-spoofing methods in tracking loop," *J. Navigat.*, vol. 69, no. 4, pp. 883–904, Jul. 2016, doi: 10.1017/s0373463315001010.

[18] Y. Wang, Y. Kou, Y. Zhao, and Z. Huang, "Detection of synchronous spoofing on a GNSS receiver using weighed double ratio metrics," *GPS Solutions*, vol. 26, no. 3, Jul. 2022, Art. no. 91.

[19] W. Zhou, Z. Lv, X. Deng, and Y. Ke, "A new induced GNSS spoofing detection method based on weighted second-order central moment," *IEEE Sensors J.*, vol. 22, no. 12, pp. 12064–12078, Jun. 2022.

[20] X. Jin, X. Zhang, S. Li, Z. Hu, S. Zheng, and R. Ma, "GNSS anti-spoofing: A sliding composite delta metric using maximum likelihood estimation," *IEEE Sensors J.*, vol. 23, no. 20, pp. 24885–24894, Oct. 2023.

[21] X. Jin, X. Zhang, and S. Zheng, "Indirect Kalman filtering for robust GNSS spoofing detection in signal quality monitoring," *Signal Processing*, vol. 239, Feb. 2026, Art. no. 110321.

[22] E. Shafiee, M. R. Mosavi, and M. Moazedi, "Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers," *J. Navigat.*, vol. 71, no. 1, pp. 169–188, 2018.

[23]B. Pardhasaradhi, R. R. Yakkati, and L. R. Cenkeramaddi, "Machine learning-based screening and measurement to measurement association for navigation in GNSS spoofing environment," *IEEE Sensors J.*, vol. 22, no. 23, pp. 23423–23435, Dec. 2022, doi: 10.1109/jsen.2022.3214349.
[24]Q. Wu, Y. Zhang, Z. Yang, and M. R. Shikh-Bahaei, "Deep learning for secure UAV swarm communication under malicious attacks," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 10, pp. 14879–14894, 2024.
[25]F. Choudhury, A. Ikhlef, W. Saad, and M. Debbah, "Deep learning for detection and identification of asynchronous pilot spoofing attacks in massive MIMO networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 11, pp. 17103–17114, Nov. 2024, doi: 10.1109/twc.2024.3450834.
[26]Z. Chen, J. Li, J. Li, X. Zhu, and C. Li, "GNSS multiparameter spoofing detection method based on support vector machine," *IEEE Sensors J.*, vol. 22, no. 18, pp. 17864–17874, Sep. 2022, doi: 10.1109/jsen.2022.3193388.
[27]M. Li, G. Huang, L. Wang, and W. Xie, "Comprehensive classification assessment of GNSS observation data quality by fusing k-means and KNN algorithms," *GPS Solutions*, vol. 28, no. 1, Jan. 2024, Art. no. 21.
[28]X. Zhang, Y. Huang, Y. Tian, M. Lin, and J. An, "Noise-like features-assisted GNSS spoofing detection based on convolutional autoencoder," *IEEE Sensors J.*, vol. 23, no. 20, pp. 25473–25486, Oct. 2023.
[29]W. Mao, J. Ren, and S. Ni, "Fast GNSS spoofing detection based on LSTM-detect model," *GPS Solutions*, vol. 29, no. 1, 2025, Art. no. 57.
[30]R. Jin *et al.*, "Small delay GNSS forwarding spoofing detection in a multipath environment based on convolutional neural network," *IEEE Sensors J.*, vol. 24, no. 15, pp. 24070–24085, Aug. 2024.
[31]L. Chen, X. Ouyang, F. Zeng, Z. Rui, and Y. Ming, "GNSS spoofing detection based on lightweight features and CGAN-ANN in unknown scenarios," *GPS Solutions*, vol. 29, no. 4, Jul. 2025, Art. no. 175.
[32]J. Li, X. Zhu, M. Ouyang, W. Li, Z. Chen, and Q. Fu, "GNSS spoofing jamming detection based on generative adversarial network," *IEEE Sensors J.*, vol. 21, no. 20, pp. 22823–22832, Oct. 2021.
[33]S. Q. Wang, J. Liu, B. G. Cai, J. Wang, and D. B. Lu, "Multidomain joint spoofing detection based on a semi-supervised detection network for GNSS-based train positioning," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 61, no. 2, pp. 3936–3949, Apr. 2025.
[34]A. Iqbal, M. N. Aman, and B. Sikdar, "Machine and representation learning-based GNSS spoofing detectors utilizing feature set from generic GNSS receivers," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 574–583, Feb. 2024.
[35]T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GNSS signal authentication techniques," in *Proc. ION GNSS*, Nashville, TN, USA, 2012, pp. 3569–3583.
[36]T. E. Humphreys. (Mar. 2016). *The University of Texas at Austin. TEXBAT Data Sets 7 and 8*. [Online]. Available: https://rnl-data.ae.utexas.edu/datastore/texbat/texbat_ds7_and_ds8.pdf.
[37]L. Lu, P. Jin, G. Pang, Z. Zhang, and G. E. Karniadakis, "Learning nonlinear operators via DeepONet based on the universal approximation theorem of operators," *Nat. Mach. Intell.*, vol. 3, pp. 218–229, 2021.

Xiaoqin Jin received the B.S. degree from the College of Information and Communication Engineering, Harbin Engineering University, Harbin, China, in 2017, and the M.S. degree from the School of Electronic and Information Engineering, Beihang University, Beijing, in 2020. She is pursuing the Ph.D. degree with the College of Artificial Intelligence, Nankai University.

Her current research primarily focuses on satellite navigation signal processing and anti-spoofing technology.

Xiaoyu Zhang received the Ph.D. degree from Harbin Engineering University, Harbin, China, in 2002.

He is currently a full professor in the Institute of Robotics and Automatic Information System, College of Artificial Intelligence, Nankai University, Tianjin, China. He is also an expert in the field of military equipment. His current research interests include navigation, guidance, control, and artificial intelligence.

Wenwu Wang (Senior Member, IEEE) received the Ph.D. degree from Harbin Engineering University, Harbin, China, in 2002. He was then with King's College London, Cardiff University, Tao Group Ltd. (now Antix Labs Ltd.), and Creative Labs, before joining University of Surrey, U.K. in 2007, where he is currently a Professor in Signal Processing and Machine Learning, and a Co-Director of the Machine Audition Lab within the Centre for Vision Speech and Signal Processing. He is also an AI Fellow within the Surrey Institute for People Centered Artificial Intelligence. He has coauthored over 300 publications in these areas. He is a coauthor or corecipient of over 15 awards including the 2022 IEEE SPS Young Author Best Paper Award, ICAUS 2021 Best Paper Award, DCASE 2020, 2023 and 2024 Judges' Award, DCASE 2019 and 2020 Reproducible System Award, and LVA/ICA 2018 Best Student Paper Award. He is an Associate Editor from 2020 to 2025 for IEEE/ACM TRANSACTIONS ON AUDIO SPEECH AND LANGUAGE PROCESSING, and an Associate Editor from 2024 to 2026 for IEEE TRANSACTIONS ON MULTIMEDIA. He was a Senior Area Editor from 2019 to 2023 and an Associate Editor from 2014 to 2018 for IEEE TRANSACTIONS ON SIGNAL PROCESSING. His research interests include blind signal processing, sparse signal processing, audio-visual signal processing, machine learning and perception, artificial intelligence, machine audition (listening), and statistical anomaly detection. He is the elected Chair from 2023 to 2024 of IEEE SPS Machine Learning for Signal Processing Technical Committee, elected Chair from 2025 to 2027 and Vice Chair from 2022 to 2024 of EURASIP Technical Area Committee on Acoustic Speech and Music Signal Processing, an elected Member from 2021 to 2026 of the IEEE Signal Processing Theory and Methods Technical Committee, and an elected Member from 2019 of the International Steering Committee of Latent Variable Analysis and Signal Separation. He was a member of the organization committee of IEEE ICASSP 2019 and 2024, INTERSPEECH 2022, IEEE MLSP 2013, 2024, and 2025, and a Technical/Program Committee Member of over 100 international conferences.

Zhanfeng Qi received the Ph.D. degree from Tianjin University, Tianjin, China, in 2022.

He is currently a professor in the Institute of Robotics and Automatic Information System, College of Artificial Intelligence, Nankai University, Tianjin, China. His current research interests include autonomous marine mobile platform, bionic robot, and mobile observation of the marine environment.

Shuaiyong Zheng received the Ph.D. degree from Beihang University, Beijing, China, in 2021.

He is currently working as a lecturer in Communication Engineering with School of Integrated Circuit Science and Engineering, Tianjin University of Technology. His research interests cover satellite-based augmentation systems, inertial navigation systems, and integrated navigation systems.