electronics

MDPI

Article

Resilient Cooperative Localisation for EVs Using V2X Sidelink Measurements Under Hybrid Cyber-Attacks: A Deep Learning-Based Physical-Layer Security Framework

Ahmed M. A. A. Elngar [1,*], Mohammed J. Abdulaal [1,2] and Mohammed Ahmed Salem [3]

[1] Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia; mjabdulaal@kau.edu.sa
[2] Centre of Excellence in Intelligent Engineering System (CEIES), King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3] Faculty of Electronics and Computer Technology and Engineering, Universiti Teknikal Malaysia Melaka, Melaka 76100, Malaysia; binghooth@utem.edu.my
* Correspondence: ahmedelngar02@gmail.com

Abstract

In this work, we explore resilient cooperative localisation for electric vehicles subject to the hybrid attack of gradual global navigation satellite system (GNSS) drag-off spoofing along with received signal strength indicator (RSSI) jamming. In order to mitigate such attacks, a deep learning-based physical-layer security approach is presented. The presented approach includes a long short-term memory (LSTM) detector for attack detection, a regression-based RSSI signal purifier, and a cooperative fusion scheme, which decreases the dependence on the GNSS branch in case of attack detection. The proposed approach is validated via the Berlin Vehicle-to-Everything (V2X) dataset with respect to six scenarios, including benign GNSS-only and cooperative localisation, attacked localisation without defence, and attacked localisation with physical-layer security support. According to the experimental evaluation results, the considered hybrid attack significantly impacts the localisation accuracy, leading to an increase in the GNSS-only localisation error to root mean square error (RMSE) = 149.93 m, mean absolute error (MAE) = 129.81 m, and maximum error = 259.62 m. At the same time, the proposed cooperative localisation with physical-layer security decreases the attacked cooperative localisation error to RMSE = 4.00 m, MAE = 3.51 m, and maximum error = 12.01 m.

Keywords: V2X communication; physical-layer security (PLS); deep learning (DL); GNSS spoofing; cooperative localisation; RSSI jamming; signal purification

Academic Editors: Lintao Li, Qihao Lv, Hua Li and Yuanyuan Dong

Received: 26 April 2026
Revised: 27 May 2026
Accepted: 30 May 2026
Published: 3 June 2026

1. Introduction

The high rate of electrification and automation in the automobile sector has made electric vehicles (EVs) a key component of connected and autonomous transport systems. In order to attain high autonomy, electric vehicles make extensive use of cooperative intelligent transport systems (C-ITS) [1], where the global navigation satellite system (GNSS) signal is used along with Vehicle-to-Everything (V2X) communication to exchange kinematic information with the surroundings to ensure safe operation [2–4]. As shown in Figure 1, the major drawback associated with the operation of EVs is the fact that the accuracy of the location information is dependent on unauthenticated wireless signals.

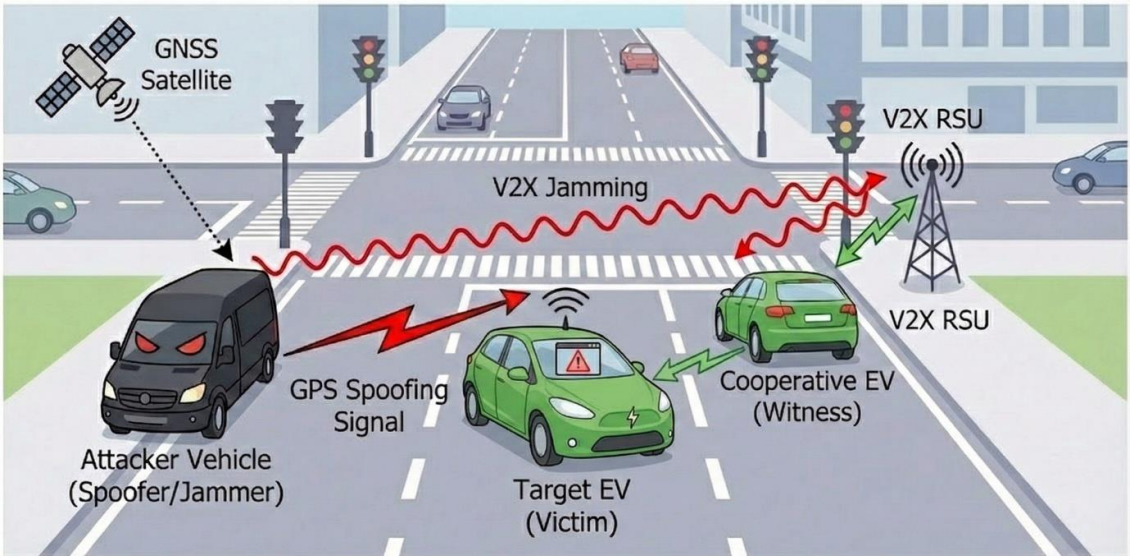

Figure 1. Scenario: Coordinated GNSS spoofing and V2X jamming attack on electric vehicles.

Vehicular localisation is highly vulnerable to physical-layer attacks [5,6]. An attacker can gradually bias the GNSS solution through spoofing [7–9], while simultaneously degrading the cooperative verification channel through received signal strength indicator (RSSI) jamming [10–12]. Even though a lot of research has been dedicated to using upper-layer cryptography for secure data, this cannot be achieved with physical signals [13]. In addition, most countermeasures are based on static thresholds or standard Kalman filtering, which are not capable of differentiating between a coordinated attack, referred to as drag-off, and natural channel fading [14,15]. Although prior studies have investigated GNSS anti-spoofing, V2X misbehaviour detection, and deep learning-based RSSI processing separately, the protection of cooperative EV localisation against coordinated GNSS drag-off spoofing and RSSI jamming remains insufficiently addressed.

To address this important problem, a physical-layer security (PLS)-assisted cooperative localisation framework based on cooperative localisation is proposed in this research. Instead of discarding the noisy data, a deep learning (DL) method is utilised to characterise and filter the interference of the signal. The deep learning module acts as a defensive physical-layer processing stage and corrects the vehicle trajectory based on the reliability of the V2X ranging information. The key contributions of this paper are summarised as follows:

i Modelling of Hybrid Cyber-Attacks: We formulate a hybrid attack model combining gradual GNSS drag-off spoofing with high-variance RSSI jamming for cooperative EV localisation.

ii Deep Learning-Based PLS Architecture: We design a dual-stage deep learning architecture comprising a long short-term memory (LSTM) network for real-time attack detection and a regression-based autoencoder for signal purification within the localisation loop.

iii Resilient Cooperative Fusion: We demonstrate that the proposed PLS-assisted cooperative fusion framework can substantially reduce the localisation error under the considered hybrid attack scenario, lowering the RMSE from 149.93 m to 4.00 m in the attacked cooperative case.

The rest of this paper is organised as follows. In Section 2, the related work on GNSS spoofing, V2X misbehaviour detection, DL-based localisation, and PLS is discussed. In Section 3, the PLS-based cooperative localisation system is introduced, including the system

model, threat model, deep learning-based PLS system, and simulation settings. In Section 4, the quantitative results are provided, including detector performance, signal purification behaviour, and localisation performance under the six considered scenarios. Finally, the conclusions are provided in Section 5.

2. Related Work

In this section, the main research lines regarding this work are briefly described: Section 2.1 GNSS spoofing and jamming in connected and autonomous vehicles, Section 2.2 misbehaviour and intrusion detection in V2X networks, and Section 2.3 deep learning techniques for RSSI-based localisation and PLS. The purpose is to point out the gap remaining in the protection of platooning EVs against hybrid drag-off and jamming attacks using physical-layer machine learning.

2.1. GNSS Spoofing and Jamming in Vehicular Localisation

The susceptibility of GNSS systems to spoofing and jamming attacks has been widely discussed. Previous studies on detecting GNSS spoofing attacks in vehicle navigation systems have primarily relied on detecting sudden position jumps or inconsistencies in pseudorange residuals using simple thresholding, receiver autonomous integrity monitoring (RAIM), or Kalman filter innovation methods [16–19]. Although these methods perform well against simple drag-off attacks, they perform poorly when confronted with more sophisticated attacks where the position bias is gradually applied to avoid triggering a static detector. More recent studies have also focused on sophisticated spoofing techniques for connected and autonomous vehicles, such as drag-off attacks that maintain a nominal error envelope for a long period of time [7,20]. Some studies have also proposed infrastructure-aided verification or even multiple-antenna-based angle-of-arrival detection methods [21–23]. However, these methods are not always feasible in a mixed-traffic environments due to a lack of infrastructure. In parallel, GNSS jamming has been investigated as Denial-of-Service attacks with wideband interference to saturate the front-end and degrade the carrier-to-noise ratio [24]. Conventional mitigation techniques rely on adaptive notch filtering and/or array processing at the radio-frequency (RF) front-end, which again requires special hardware and does not address the question of how the navigation engine should react if both GNSS and cooperative ranging become unreliable [25]. Moreover, these methods mainly protect the GNSS branch itself and do not explain how localisation should be recovered when the cooperative V2X ranging channel is simultaneously degraded.

2.2. Misbehaviour and Intrusion Detection in V2X Networks

At the V2X level, a significant body of work is dedicated to misbehaviour detection and intrusion detection systems (IDSs) for vehicular networks [26]. Most of these methods are based on network- and application-layer approaches that monitor the content of messages and their conformity to the road topology and vehicle dynamics in order to identify unrealistic cooperative awareness messages (CAMs) and basic safety messages (BSMs) [27–29]. Such methods are particularly useful for identifying fake information and Sybil attacks [30]. However, most of these methods depend on the reliability of the underlying physical information [31,32]. Recently, machine learning-based IDS approaches have been proposed for V2X communication, which utilise the advantages of the packet time, message sequence, and flow statistics [33,34]. Hybrid models using convolutional neural network (CNN) and LSTM techniques have been proposed to effectively identify complex attacks in intelligent transport systems operating at 5.9 GHz (ITS-G5) and Cellular Vehicle-to-Everything (C-V2X) networks [35]. However, these approaches primarily concentrate on the security of the higher layers of the protocols, such as Denial-of-Service

(DoS), flooding, and replay attacks, rather than physical-layer attacks like RSSI jamming and GNSS spoofing [36]. They do not address the integrity of the lane-level localisation measurements. Consequently, although such methods are useful for detecting higher-layer vehicular misbehaviour, they do not directly resolve the corruption of the physical measurements used by the localisation engine.

2.3. Deep Learning for RSSI-Based Localisation and Physical-Layer Security

Deep learning has also been employed in improving wireless localisation and PLS techniques [37]. For wireless localisation in indoor and urban environments, several works have employed feed-forward networks, CNNs, LSTMs, and autoencoders in improving localisation estimates based on RSSI fingerprints, moving beyond traditional log-distance path loss models [38–42]. These works prove the effectiveness of neural networks in learning complex relationships from noisy data using temporal convolutional network (TCN) RSSI time-series data and in improving localisation estimates significantly compared to traditional path loss models [43]. In the framework of PLS, deep learning techniques have been considered for PLS channel authentication, the detection of eavesdroppers, and the detection of jamming attacks in 5G and beyond-5G systems [44–47]. The most popular approaches rely on CNNs and recurrent neural networks (RNNs) for the detection of malicious links based on channel state information (CSI), RSSI-based distributions, and constellation diagrams [48,49]. Although these studies prove the effectiveness of PLS by significantly enhancing it via AI-based classifiers, the decision process is not completed by a feedback loop to correct the trajectory based on clean measurements. Moreover, most of these studies treat localisation enhancement, signal denoising, or physical-layer attack detection separately, rather than integrating detection, purification, and defensive fusion within one cooperative localisation pipeline.

2.4. Gap Analysis and Distinction of This Work

The existing GNSS anti-spoofing and anti-jamming techniques have mainly focused on GNSS-based detection or additional RF-based techniques. Studies on the detection of misbehaviour and IDSs in V2X have considered message integrity in higher layers, while those on deep learning-based localisation and PLS have considered security and localisation separately, as shown in Table 1. To the best of the authors' knowledge, three main gaps are not fully addressed. These gaps are summarised as follows:

i A hybrid drag-off + jamming attack specifically targeting lane-level localisation in autonomous EV platoons;
ii A dual-stage deep learning-based PLS framework that both detects and denoises physical-layer measurements (via an LSTM sentinel and a regression-based cleaner);
iii A cooperative fusion engine that dynamically reweights GNSS and V2X ranging based on the PLS decision, explicitly aiming to prevent the off-road divergence of the EV trajectory on real V2X measurement data (Berlin V2X) [50].

The presented framework integrates deep learning components into a closed-loop physical-layer defence pipeline for cooperative localisation. As per Section 3.2, the attack detection occurs in the PLS layer using the LSTM-based sentinel, followed by the purification of the jammed sidelink RSSI using the regression autoencoder. The purified RSSI feeds the cooperative fusion layer, which down-weights the (possibly spoofed) GNSS layer under attack at the same time. The novelty of the present work does not lie in proposing a new standalone learning model but in the integration of detection, RSSI purification, and cooperative fusion against a coordinated GNSS drag-off spoofing and RSSI jamming threat. LSTM classifiers for anomaly detection in time-series, autoencoder-style regression for the denoising of input data, and weighted GNSS-V2X fusion are all known techniques.

However, the novelty is in the closed-loop integration of these building blocks against a particular type of joint drag-off + jamming threat at the physical layer for autonomous EV platoons, which has been previously overlooked, to the best of our knowledge.

Table 1. Comparative positioning of the proposed framework against representative prior work.

Reference	Work	Attack Model	Defence Stage	Cooperative Fusion?	Reported Outcome
[19]	RAIM	GNSS spoofing (jump)	GNSS only	No	Detection only
[16]	Kalman filter-based global positioning system (GPS)/INS	GPS spoofing	GPS/INS Kalman filter	Yes (filter)	Few-metre horizontal error
[18]	Particle filter localisation	GNSS spoofing	Particle filter	Yes	Few-metre error
[33,39]	CNN-LSTM V2X IDS	DoS/replay (upper layer)	Upper-layer IDS	No	High F1, no localisation error
[43]	TCN RSSI localisation	Indoor noise	RSSI localisation	Single link	≈metre-level (indoor)
[47]	DL RSSI denoising	Indoor noise	RSSI denoising	Single link	≈metre-level (indoor)
[46]	PLS channel authentication	PLS spoofing	Channel level	No	Detection only
	This work (proposed)	Hybrid drag-off + RSSI jamming	PLS (LSTM + autoencoder)	Yes (GNSS + V2X)	RMSE 4.00 m under attack

Finally, the empirical evaluation on the publicly available Berlin V2X dataset shows that the proposed closed-loop defence substantially reduces the localisation error under the considered hybrid attack scenario, while remaining within the same order of magnitude as the benign cooperative baseline.

3. PLS-Assisted Cooperative Localisation Framework

This framework was formulated for analysing the impact of deep learning physical-layer protection mechanisms on electric vehicle localisation under coordinated spoofing and jamming attacks. In the process, the target vehicle is assumed to receive the GNSS position estimation and V2X sidelink signal, which include the RSSI and signal-to-noise ratio (SNR) measurements. Under normal circumstances, both sensors will be exploited in localising the target vehicle. However, under adversarial conditions, the GNSS sensor is spoofed and the V2X sensor is jammed. As such, the aim of the proposed framework is to detect the attack and cleanse the RSSI measurement of any contamination. To achieve this objective, a deep learning-based physical-layer security module is introduced, as illustrated in Figure 2.

3.1. System and Threat Model

Let the true horizontal position of the target vehicle at discrete time step t be denoted by

$$\boldsymbol{p}_{true}(t) = \begin{bmatrix} \phi_{true}(t) \\ \lambda_{true}(t) \end{bmatrix} \tag{1}$$

where $\phi_{\text{true}}(t)$ and $\lambda_{\text{true}}(t)$ are the true latitude and longitude, respectively.

Under spoofing, the GNSS observation is gradually displaced from the true position according to

$$\mathbf{p}_{\mathbf{gps}}(t) = \mathbf{p}_{\text{true}}(t) + t \begin{bmatrix} \delta_\phi \\ \delta_\lambda \end{bmatrix} \tag{2}$$

where $\mathbf{p}_{\text{gps}}(t)$ is the spoofed GNSS position, δ_ϕ is the latitude drift rate, and δ_λ is the longitude drift rate introduced by the attacker. This formulation represents a drag-off attack in which the position error grows progressively rather than appearing as an abrupt jump. In benign operation, the GNSS observation is instead written as

$$\mathbf{p_{gps}}(t) = \mathbf{p}_{\text{true}}(t) + \mathbf{n}_{\text{gps}}(t) \tag{3}$$

where $\mathbf{n}_{\text{gps}}(t)$ is the nominal GNSS perturbation.

Let $\text{RSSI}_{\text{raw}}(t)$ denote the clean sidelink RSSI measurement at time step t. Under jamming, the observed RSSI becomes

$$\text{RSSI}_{\text{obs}}(t) = \text{RSSI}_{\text{raw}}(t) + n_{\text{jam}}(t) \tag{4}$$

where $\text{RSSI}_{\text{obs}}(t)$ is the jammed observation and $n_{\text{jam}}(t)$ is the injected jamming term. In benign operation, the observation is represented as

$$\text{RSSI}_{\text{obs}}(t) = \text{RSSI}_{\text{raw}}(t) + n_{\text{benign}}(t) \tag{5}$$

where $n_{\text{benign}}(t)$ denotes ordinary measurement noise. The purpose of the PLS stage is therefore to distinguish between nominal RSSI variation and hostile RSSI corruption before the corrupted measurements are used in localisation.

For the RF-based ranging model, let P_{TX} denote the transmit power, n denote the path loss exponent (PLE), and $\hat{d}_{\text{rf}}(t)$ denote the range estimate inferred from the purified RSSI. The log-distance inversion used in the code is

$$\hat{d}_{\text{rf}}(t) = 10^{\frac{P_{\text{TX}} - \text{RSSI}_{\text{clean}}(t)}{10n}} \tag{6}$$

where $\text{RSSI}_{\text{clean}}(t)$ is the reconstructed RSSI after purification. Although the RF-only branch is part of the wider simulation code, the present manuscript focuses only on the six scenarios associated with GNSS-only, cooperative, and PLS-assisted cooperative localisation.

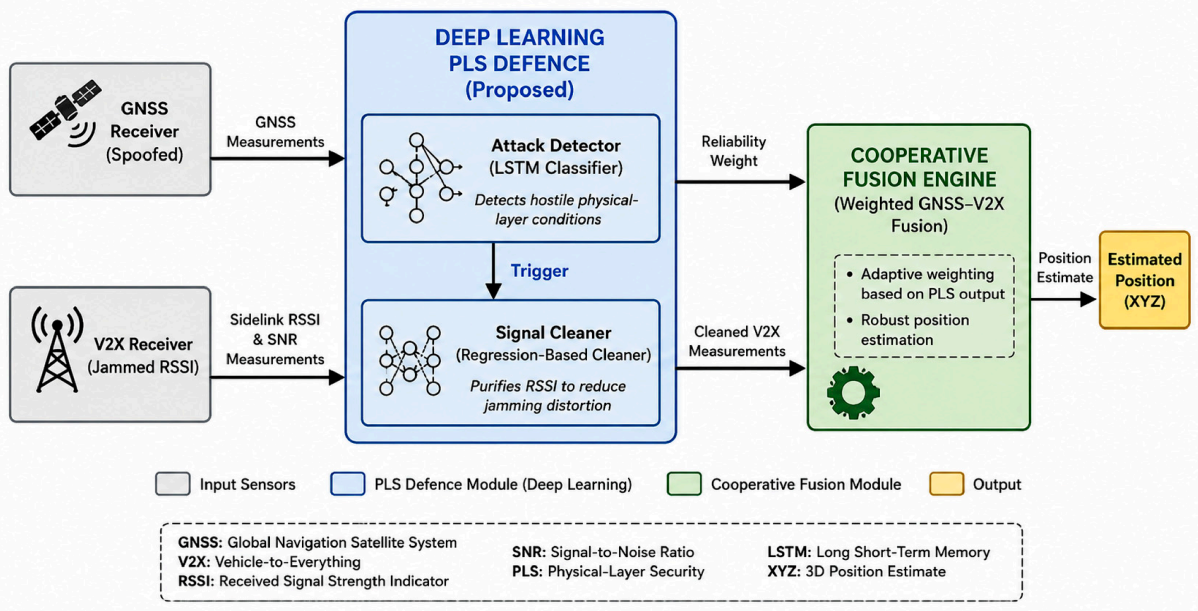

Figure 2. PLS-assisted cooperative localisation architecture.

3.2. Deep Learning-Based Physical-Layer Security Layer

The PLS layer processes physical-layer measurements as short temporal sequences. At each time step t, the detector input feature vector is defined as

$$\mathbf{x}(t) = \begin{bmatrix} SNR(t) \\ \mathrm{RSSI}_{\mathrm{obs}}(t) \end{bmatrix} \tag{7}$$

where $\mathrm{SNR}(t)$ is the SNR and $\mathrm{RSSI}_{\mathrm{obs}}(t)$ is the potentially jammed RSSI. The corresponding temporal input sequence is

$$\mathbf{X}(t) = [\mathbf{x}(t-L+1), \mathbf{x}(t-L+2), \ldots, \mathbf{x}(t)] \tag{8}$$

where L is the detector sequence length. This sequence is supplied to the LSTM detector, which produces a binary decision

$$\hat{a}(t) = f_{\mathrm{LSTM}}(\mathbf{X}(t)) \tag{9}$$

where $f_{\mathrm{LSTM}}(\cdot)$ denotes the detector mapping and $\hat{a}(t) \in \{0, 1\}$ is the estimated attack label. A value of $\hat{a}(t) = 1$ indicates that the current sidelink condition is classified as attacked.

The detector is trained on synthetically labelled data. Let $a_i \in \{0, 1\}$ denote the label assigned to the i-th training sample, where $a_i = 0$ indicates a safe sample and $a_i = 1$ indicates a jammed sample. The attacked training RSSI is formed as

$$\mathrm{RSSI}_i^{\mathrm{atk}} = \mathrm{RSSI}_i + n_i \tag{10}$$

where RSSI_i is the clean RSSI and n_i is the injected jamming perturbation. The corresponding training sequence label is then taken from the terminal element of each temporal window,

$$y_k = a_{k+L-1} \tag{11}$$

Thus, the detector learns to classify short temporal segments as safe or attacked based on the joint behaviour of the SNR and RSSI. The exact architectural and optimisation settings are summarised later in the implementation table.

Once an attack is indicated, the observed RSSI is purified by a regression-based cleaner. Let $g_{\mathrm{reg}}(\cdot)$ denote the cleaner mapping. The reconstructed signal is

$$\mathrm{RSSI}_{\mathrm{clean}}(t) = g_{\mathrm{reg}}(\mathrm{RSSI}_{\mathrm{obs}}(t)) \tag{12}$$

If no attack is detected, the measurement is left unchanged and

$$\mathrm{RSSI}_{\mathrm{clean}}(t) = \mathrm{RSSI}_{\mathrm{obs}}(t) \tag{13}$$

The cleaner is trained using jammed–clean RSSI pairs, where the corrupted RSSI serves as input and the corresponding clean RSSI serves as the target. In this way, the LSTM and the regression network perform complementary roles: the detector identifies the presence of hostile channel activity, whereas the cleaner reconstructs a more usable sidelink signal for localisation.

In the present implementation, the detector output is latched. Once an attack has been detected, the system remains in the attacked state for the remainder of the run. This can be written as

$$a_{\mathrm{latched}}(t) = \max_{1 \le \tau \le t} \hat{a}(\tau) \tag{14}$$

where $a_{\text{latched}}(t)$ is the persistent attack state. This rule prevents repeated switching between attack and non-attack modes during contested operation.

3.3. Cooperative Localisation and Fusion Logic

The GNSS branch is directly represented by the current GNSS observation,

$$\hat{\mathbf{p}}_{\text{gps}}(t) = \mathbf{p}_{\text{gps}}(t) \tag{15}$$

The cooperative branch utilises the purified RSSI measurements obtained from the PLS cleaner in order to support localisation under degraded GNSS conditions. The reconstructed RSSI is first converted into cooperative ranging information using the log-distance path loss model defined in Equation (6). The resulting ranging measurements are then incorporated into the cooperative localisation branch to generate a bounded cooperative position estimate. The cooperative estimate is modelled in the current six-scenario implementation as

$$\hat{\mathbf{p}}_{\text{coop}}(t) = \mathbf{p}_{\text{true}}(t) + \mathbf{n}_{\text{coop}}(t) \tag{16}$$

where $\hat{\mathbf{p}}_{\text{coop}}(t)$ denotes the cooperative position estimate and $\mathbf{n}_{\text{coop}}(t)$ represents the residual cooperative ranging uncertainty after RSSI purification. This simplified representation was retained in the present scenario study in order to isolate the effect of the PLS-assisted detection and fusion strategy. The final position estimate is obtained through the weighted fusion of the GNSS and cooperative branches

$$\hat{\mathbf{p}}(t) = \alpha(t)\hat{\mathbf{p}}_{\text{gps}}(t) + (1 - \alpha(t))\hat{\mathbf{p}}_{\text{coop}}(t) \tag{17}$$

where $\hat{\mathbf{p}}(t)$ is the fused position estimate and $\alpha(t)$ is the GNSS trust weight. In the current implementation, $\alpha(t)$ is scenario-dependent. Under nominal cooperative operation, the GNSS and cooperative branches are equally weighted. Under attacked cooperative operation without defence, the GNSS branch remains strongly trusted, so the spoofed position dominates the estimate.

Under attacked cooperative operation with PLS enabled, the GNSS trust weight is represented by the fixed reduced value $\alpha_{\text{def}} = 0.01$, corresponding to an almost complete reliance on the cooperative branch after attack detection. In the current six-scenario implementation, the fusion weights are predefined on a per-scenario basis rather than dynamically adapted over time. Thus, the PLS layer affects localisation not by directly estimating the position but by purifying the sidelink signal and by modifying the fusion logic in response to detected attack conditions.

For clarity, three representative cooperative fusion scenarios are explicitly defined in this study. Scenario S4 corresponds to benign cooperative localisation, Scenario S1 represents attacked cooperative localisation without defence, and Scenario S6 represents attacked cooperative localisation with the proposed PLS-assisted defence.

$$\begin{aligned}
\hat{\mathbf{p}}_{S4}(t) &= \alpha_{\text{nom}}\hat{\mathbf{p}}_{\text{gps}}(t) + (1 - \alpha_{\text{nom}})\hat{\mathbf{p}}_{\text{coop}}(t) \\
\hat{\mathbf{p}}_{S1}(t) &= \alpha_{\text{undef}}\hat{\mathbf{p}}_{\text{gps}}(t) + (1 - \alpha_{\text{undef}})\hat{\mathbf{p}}_{\text{coop}}(t) \\
\hat{\mathbf{p}}_{S6}(t) &= \alpha_{\text{def}}\hat{\mathbf{p}}_{\text{gps}}(t) + (1 - \alpha_{\text{def}})\hat{\mathbf{p}}_{\text{coop}}(t)
\end{aligned} \tag{18}$$

where α_{nom} is the nominal cooperative fusion weight, α_{undef} is the attacked but undefended weight, and α_{def} is the attacked defended weight. Their exact numerical values are reported in the parameter table at the end of this section.

3.4. Operational Workflow of the Proposed Framework

The complete operation of the proposed framework follows the processing chain illustrated in Figure 2. At each time step t, the target EV first acquires a GNSS-based position observation and a V2X sidelink measurement characterised by the RSSI and SNR. The GNSS branch may be affected by spoofing, whereas the V2X branch may be affected by RSSI jamming. The received physical-layer features are then processed by the LSTM-based attack detector using the temporal input sequence defined in Equation (8). The detector output in Equation (9) determines whether the current sidelink condition is regarded as safe or attacked. If the condition is classified as attacked, the signal cleaner is triggered and reconstructs the purified RSSI according to Equation (12). Otherwise, the original observed RSSI is retained according to Equation (13). The purified RSSI is then forwarded to the cooperative localisation branch, while the GNSS branch is weighted according to the fusion logic defined in Equation (17). In this way, the framework performs detection, signal purification, and defensive fusion within one closed-loop localisation pipeline.

The processing sequence can therefore be summarised as

$$\begin{aligned}\text{GNSS/V2X acquisition} &\rightarrow \text{attack detection} \rightarrow \text{RSSI purification} \\ &\rightarrow \text{cooperative localisation} \rightarrow \text{weighted fusion} \\ &\rightarrow \text{final position estimate}\end{aligned}$$

where each stage corresponds directly to one of the functional modules shown in Figure 2. The main role of the PLS layer is not only to indicate the presence of a hostile condition but also to influence the final position estimate by improving the sidelink signal quality and by reducing the influence of the spoofed GNSS branch when required.

3.5. Evaluation Metrics

Let $\mathbf{p}_{\text{true}}(t)$ denote the ground-truth horizontal position of the target EV at time step t, and let $\hat{\mathbf{p}}(t)$ denote the corresponding fused position estimate. The instantaneous localisation error is defined as

$$e(t) = \| \hat{\mathbf{p}}(t) - \mathbf{p}_{\text{true}}(t) \|_2 \tag{19}$$

where $e(t)$ is the horizontal localisation error at time step t, and $\| \cdot \|_2$ denotes the Euclidean norm.

Over a simulation horizon of T_{sim} time steps, the root mean square error (RMSE) is defined as

$$RMSE = \sqrt{\frac{1}{T_{\text{sim}}} \sum_{t=1}^{T_{\text{sim}}} e^2(t)} \tag{20}$$

where RMSE measures the overall localisation accuracy over the whole trajectory.

The mean absolute error (MAE) is given by

$$\text{MAE} = \frac{1}{T_{\text{sim}}} \sum_{t=1}^{T_{\text{sim}}} e(t) \tag{21}$$

where MAE represents the average magnitude of the localisation error.

The maximum error is defined as

$$\text{MaxErr} = \max_{1 \le t \le T_{\text{sim}}} e(t) \tag{22}$$

where MaxErr captures the worst-case localisation deviation over the whole simulation horizon. These three metrics are used to compare the six localisation scenarios considered in this work.

In addition to the trajectory-level metrics, the LSTM detector is evaluated using standard binary classification measures. Let TP, TN, FP, and FN denote the true-positive, true-negative, false-positive, and false-negative counts, respectively. The classification accuracy is

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{23}$$

where Accuracy indicates the proportion of correctly classified attacked and safe samples.

The detector precision is defined as

$$\text{Precision} = \frac{TP}{TP + FP} \tag{24}$$

where Precision quantifies the fraction of predicted attacks that are truly attacks.

The detector recall is

$$\text{Recall} = \frac{TP}{TP + FN} \tag{25}$$

where Recall measures the fraction of actual attacks that are successfully detected.

The F1-score is computed as

$$\text{F1} = \frac{2\text{Precision Recall}}{\text{Precision} + \text{Recall}} \tag{26}$$

where F1 provides a balanced measure of detection performance by combining precision and recall. In addition, the receiver operating characteristic–area under the curve (ROC-AUC) is reported in the Results section in order to characterise the separability of attacked and safe conditions.

The signal cleaner is evaluated independently by comparing the reconstructed RSSI against the clean RSSI target. Let r_i^{clean} denote the clean RSSI target for sample i, let r_i^{jam} denote the jammed RSSI input, and let $\hat{r}_i$ denote the reconstructed RSSI. The cleaner RMSE is defined as

$$\text{RMSE}_{\text{clean}} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(\hat{r}_i - r_i^{\text{clean}}\right)^2} \tag{27}$$

where N is the number of cleaner evaluation samples.

The cleaner MAE is

$$\text{MAE}_{\text{clean}} = \frac{1}{N}\sum_{i=1}^{N} \mid \hat{r}_i - r_i^{\text{clean}} \mid \tag{28}$$

where $\text{MAE}_{\text{clean}}$ measures the average absolute reconstruction error.

To further quantify the reconstruction quality, the coefficient of determination is defined as

$$R^2 = 1 - \frac{\sum_{i=1}^{N}\left(\hat{r}_i - r_i^{\text{clean}}\right)^2}{\sum_{i=1}^{N}\left(r_i^{\text{clean}} - \bar{r}^{\text{clean}}\right)^2} \tag{29}$$

where $\bar{r}^{\text{clean}}$ is the sample mean of the clean RSSI targets. In addition, the percentage reduction in residual error variance is defined as

$$\text{VR}_{\%} = 100 \times \frac{\text{Var}\left(r^{\text{jam}} - r^{\text{clean}}\right) - \text{Var}\left(\hat{r} - r^{\text{clean}}\right)}{\text{Var}\left(r^{\text{jam}} - r^{\text{clean}}\right)} \tag{30}$$

where $VR_{\%}$ denotes the percentage reduction in reconstruction error variance after signal cleaning. These measures allow the denoising stage to be assessed independently of the final localisation output.

3.6. Simulation Configuration

The full set of implementation settings used for this experiment is listed in Table 2 below. These include the dataset splitting strategy, simulation time frame, length of detector sequence, attack injection rule, GNSS spoofing parameters, RSSI jamming parameters, detector network architecture, cleaner network architecture, training hyperparameters, and fusion weights for each of the six selected scenarios. The use of a single table in order to present all of these quantities allows the discussion of the methodology to remain tightly focused.

Table 2. Simulation and model parameters.

Parameter	Value	Description
T_{sim}	1000 steps	Simulation duration
Data split	70%/30%	Chronological training/testing partition
ID_{victim}	2	Vehicle selected for tracking
η	0.5	Proportion of training samples synthetically jammed
P_{TX}	−10 dBm	Transmit power of the sidelink beacons
n	2.5	Average urban PLE
σ_{jam}	12.0 dB	Standard deviation of jamming noise
σ_{RSSI}	1.0 dB	Standard deviation of benign RSSI perturbation
σ_{GNSS}	10^{-5} deg	Standard deviation of benign GNSS perturbation
δ_{drift}	2×10^{-5} deg/s	GNSS spoofing drift rate
L	5	LSTM temporal window length
Detector input dimension	2	SNR and RSSI
Detector architecture	1 LSTM layer + fully connected (FC) + Softmax	LSTM classifier structure
LSTM hidden units	50	Hidden units in detector
Detector optimiser	Adam	Detector training algorithm
Detector learning rate	0.01	Detector initial learning rate
Detector mini-batch size	256	Detector batch size
Detector epochs	5	Detector training epochs
Cleaner architecture	FC–Rectified Linear Unit (ReLU)–FC–FC regression network	RSSI cleaner structure
Cleaner hidden-layer sizes	20, 10	Hidden units in cleaner
Cleaner optimiser	Adam	Cleaner training algorithm
Cleaner learning rate	0.01	Cleaner initial learning rate
Cleaner mini-batch size	128	Cleaner batch size
Cleaner epochs	20	Cleaner training epochs
α_{nom}	0.50	GNSS weight in nominal cooperative fusion
α_{undef}	0.90	GNSS weight in attacked cooperative fusion without defence
α_{def}	0.01	GNSS weight in attacked cooperative fusion with PLS

4. Results and Discussion

The proposed PLS layer was tested using the test portion of the Berlin V2X dataset [50], where the localisation performance was assessed under six different scenarios, which included a benign scenario, an attacked scenario without any defence, and an attacked scenario with the proposed PLS support. The evaluation process can be divided into three phases. Firstly, the deep learning modules within the proposed PLS layer will be validated independently. Secondly, the performance of the localisation under the six selected scenarios will be quantitatively investigated. Finally, the time-varying and location-varying effects of the proposed defence will be demonstrated by error evolution and trajectory plots.

4.1. Validation of Deep Learning-Based PLS Layer

Prior to analysing the localisation accuracy, the two deep learning modules that constitute the proposed PLS layer need to be verified, as the success of the whole scheme relies on not only attack detection but also signal cleaning. The former module is tasked with differentiating between attacked and unattacked physical-layer environments, while the latter is tasked with rebuilding an improved RSSI signal upon detecting attacks. Thus, in this section, we first investigate the statistical separability utilised by the detector, followed by the detector performance and cleaner evaluation.

4.1.1. Statistical Separation of Clean and Jammed RSSI

Figure 3 presents the empirical RSSI distributions under clean and synthetically jammed conditions. The red bars and red fitted curve represent the jammed RSSI used during detector training, showing a wider distribution and higher variance due to the injected attack. The green fitted curve represents the genuine clean sidelink RSSI, while the green histogram is mostly seen as the darker red or brownish region beneath the semi-transparent red attack distribution. This overlap indicates that some clean and jammed RSSI samples share similar values, so the two classes are not perfectly separable from RSSI alone. However, the wider spread and shifted behaviour of the jammed distribution provide useful statistical features for the LSTM detector to distinguish benign from hostile channel conditions.

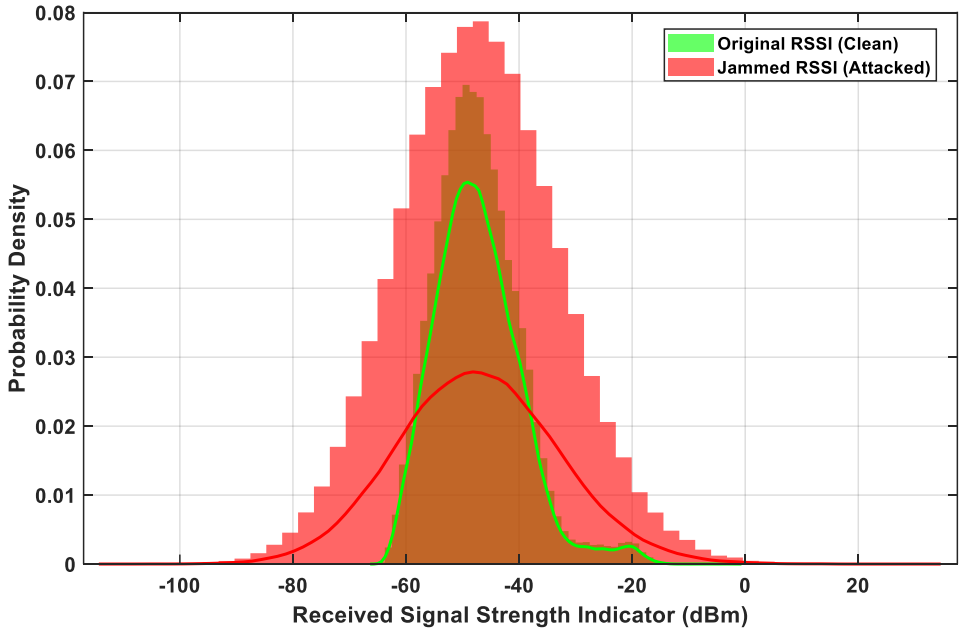

Figure 3. RSSI feature distribution under clean vs. jammed conditions.

4.1.2. Quantitative Performance of the LSTM Detector

It is necessary to evaluate the performance of the detector quantitatively as well. In terms of test sequences, the LSTM detector showed accuracy of 0.7056, precision of 0.7248, recall of 0.6636, an F1-score of 0.6928, and an ROC-AUC of 0.7462. The confusion matrix numbers included $TP = 1659, TN = 1866, FP = 630$, and $FN = 841$. The results indicate that the detector provides reasonable discrimination capabilities between benign and attacked physical-layer conditions. However, some attack instances remain undetected, while certain benign conditions are incorrectly classified as attacks. Table 3 shows their significance in analysing the localisation results.

Table 3. LSTM detector performance metrics.

Metric	Value
Accuracy	0.7056
Precision	0.7248
Recall	0.6636
F1-Score	0.6928
ROC-AUC	0.7462
True Positives (TP)	1659
True Negatives (TN)	1866
False Positives (FP)	630
False Negatives (FN)	841

4.1.3. Qualitative Signal Reconstruction by the Cleaner

Having detected the attack, the cleaner tries to produce a more accurate RSSI signal for the cooperative localisation path. Figure 4 presents an example of a segment, where the red line represents the jammed input, the green line represents the clean RSSI target, and the blue dotted line represents the produced output. It can be observed that the clean signal correlates well with the clean one and reduces a considerable share of the highly volatile noise added by the jammer. This means that the cleaner increases the usefulness of the sidelink measurement.

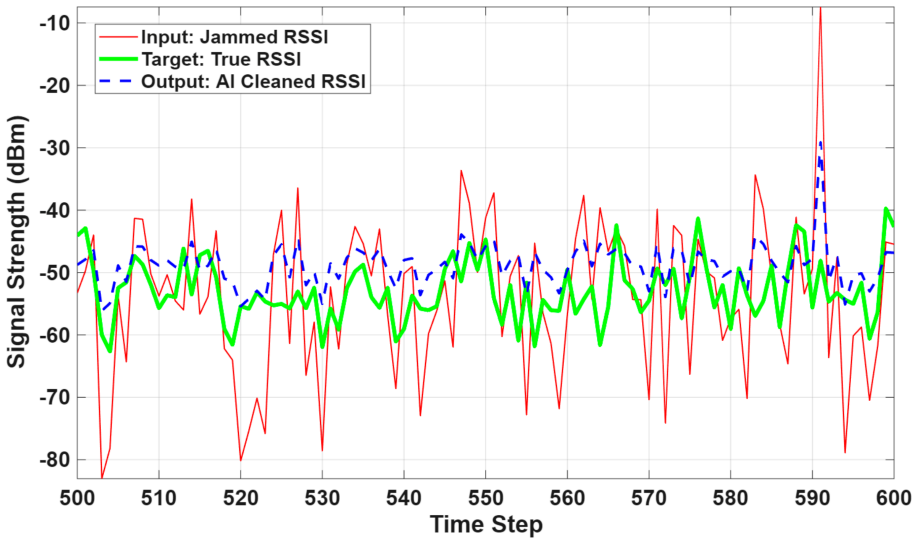

Figure 4. Signal denoising performance of the regression-based cleaner on a test segment.

4.1.4. Quantitative Performance of the RSSI Cleaner

The denoising phase should also be evaluated using quantitative methods. Prior to denoising, the jammed signal had an RMSE of 11.959 dB and MAE of 9.5156 dB compared to the target RSSI signal. After denoising, these metrics were decreased to RMSE = 5.5249 dB and MAE = 4.4303 dB. Moreover, after denoising, the signal obtained an R2 value of 0.1100 and a residual error variance decrease of 79.856%; this is summarised in Table 4. This shows that the cleaner is not able to restore the original signal completely; however, it decreases the RSSI distortion from the jammer considerably and therefore ensures that it is a significantly improved input for the cooperative localisation engine branch.

Table 4. RSSI cleaner performance metrics.

Metric	Value
RMSE before cleaning (dB)	11.959
RMSE after cleaning (dB)	5.5249
MAE before cleaning (dB)	9.5156
MAE after cleaning (dB)	4.4303
R^2 after cleaning	0.1100
Residual error variance reduction (%)	79.856

Taken together, the detector and cleaner results confirm that the proposed PLS layer performs the two required physical-layer defence tasks: identifying suspicious channel conditions and reconstructing a substantially less distorted sidelink signal. However, the practical value of these improvements must still be evaluated in the full localisation loop. The next subsection therefore examines the localisation behaviour under the six retained scenarios.

4.2. Localisation Performance Under the Six Considered Scenarios

The localisation performance of the proposed framework was assessed on the basis of six scenarios, as mentioned in Section 3. The six scenarios consist of a benign GNSS-only and cooperative baseline, attacked GNSS-only and cooperative localisation without defence, and attacked GNSS-only and cooperative localisation with defence using the proposed PLS layer. The corresponding RMSE, MAE, and MaxErr are provided in Table 5 below.

Table 5. Performance comparison.

Scenario ID	Scenario Description	Attack?	Detection/Defence?	RMSE (m)	MAE (m)	MaxErr (m)
S1	Attack + Cooperative	Yes	No	134.94	116.84	233.42
S2	Attack + GNSS Only	Yes	No	149.93	129.81	259.62
S3	Baseline (GNSS Only)	No	-	1.31	1.14	3.75
S4	Baseline (Cooperative)	No	-	2.07	1.81	6.33
S5	Attack + GNSS + PLS	Yes	Yes	149.93	129.81	259.62
S6	Proposed (Coop + PLS)	Yes	Yes	4.00	3.51	12.01

The six scenarios also enable a component-level interpretation of the proposed framework. Scenario S2 shows the effect of the hybrid attack on GNSS-only localisation, while Scenario S1 shows that cooperative localisation without the PLS layer remains strongly affected by the spoofed GNSS and jammed sidelink measurements. Scenario S5 isolates the use of the PLS layer without cooperative fusion and shows that signal purification alone

does not improve localisation when the final estimate remains GNSS-dominated. Scenario S6 therefore represents the full closed-loop configuration, where attack detection, RSSI purification, and cooperative fusion operate together. This comparison indicates that the main gain is not produced by a single module in isolation but by the interaction between the detector, cleaner, and fusion rule.

For benign conditions, the GNSS-only baseline in Scenario S3 attains an RMSE of 1.31 m, MAE of 1.14 m, and MaxErr of 3.75 m. The cooperative baseline in Scenario S4 attains an RMSE of 2.07 m, MAE of 1.81 m, and MaxErr of 6.33 m. This implies that the cooperative baseline is less accurate compared to the pure GNSS baseline when there is no attack. This type of behaviour is expected in the current scenario since the nominal cooperative baseline is constructed using the fusion of the highly accurate GNSS baseline with another branch whose accuracy level is lower due to RSSI errors. In other words, cooperation is included in this case mainly for robustness against attacks rather than improving the nominal GNSS baseline under benign conditions.

As soon as the joint spoofing and jamming attack is launched, the performance of the unguarded localisation algorithms deteriorates significantly. For Scenario S2, in which the localisation component depends entirely on the attacked GNSS component, the RMSE increases to 149.93 m, the MAE increases to 129.81 m, and the MaxErr becomes equal to 259.62 m. The situation is only marginally improved in Scenario S1, in which the cooperation takes place but without implementing the suggested PLS mitigation measure, as the RMSE in this scenario amounts to 134.94 m, the MAE equals 116.84 m, and the MaxErr is 233.42 m. It can be observed that mere cooperation is insufficient in combating the hybrid attack, as the fusion stage is affected by the spoofed GNSS position and the jammed sidelink observation.

An especially interesting finding is obtained based on the results of Scenario S5. Here, the PLS filter is used, but the localisation engine is solely GNSS-based. As a consequence, the values of the RMSE, MAE, and MaxErr are exactly the same as in Scenario S2. Hence, we can conclude that denoising alone does not have any effect on the accuracy of localisation, provided that the final estimate of the location is computed based on the GNSS spoofing branch alone. Consequently, the signal cleaner cannot be considered as an independent module. It is valuable only in combination with the cooperative localisation approach, since its output affects the logic of fusing data streams. This is a crucial finding for the research, because the gain is not achieved through denoising alone but through the closed-loop interaction of all three stages.

The efficiency of the suggested approach is confirmed by Scenario S6, when both the PLS layer and the cooperative fusion engine operate. As for the second scenario, the RMSE metric takes the value of 4.00 m, the MAE value amounts to 3.51 m, while the MaxErr metric is equal to 12.01 m. Compared to the attacked GNSS-only scenario of Scenario S2, this results in a reduction in the RMSE and MAE metrics of 97.3% and 97.2%, respectively. When comparing the suggested approach to the attacked and undefended cooperative case of Scenario S1, the RMSE and MAE metrics are reduced by more than 96%. This proves that the suggested approach allows the system to overcome the negative impact of the coordinated attack on the localisation process and keeps the error rate close to that in the case of benign cooperation. Nevertheless, the non-zero value of MaxErr shows that localisation failures can occur, although the suggested approach is highly resilient to the threat model in question.

From the above results in Table 5, we can deduce four major observations. First, localisation using the GNSS system only is precise in good environments but very susceptible in the case of coordinated spoofing attacks. Second, a cooperative strategy without any defensive measures cannot guarantee resilience. Third, when the GNSS channel dominates,

there will be no improvement in localisation using the signal purification based on PLS. Finally, our proposed strategy, which combines physical-layer attack detection, RSSI purification, and cooperative fusion, offers the highest robustness in localisation under the current hybrid attack.

4.3. Trajectory-Level Analysis and Discussion

The scenario-based metrics given in Table 5 indicate the level of localisation error in each operating condition; however, they do not completely capture how the error is evolving over time and how the attack is shaping the vehicle trajectory in space. This is why, in addition to the numerical results, a temporal error evolution study and a spatial trajectory analysis are included herein. These two approaches provide insight into how the proposed cooperative approach based on the use of PLS mitigates the hybrid drag-off attack.

4.3.1. Localisation Error Evolution Under Attack

Figure 5 depicts the cumulative distribution function (CDF) plot for the localisation errors of the safe baseline, the attacked GNSS-only solution, and the proposed defended cooperative solution. Here, the green curve depicts the safe baseline, while the red dashed curve depicts the case of the attack. The blue curve depicts the proposed defence method. From Figure 5, it is clear that the safe baseline has a high cumulative probability value for smaller errors, which means that the majority of the benign estimates are near the ground truth trajectory. However, the attacked GNSS-only solution is highly biased towards higher errors, indicating the negative impact of the hybrid spoofing and jamming attack on the performance of the system. Finally, it can be seen from Figure 5 that the proposed defence is somewhere in between these two extremes and closer to the safe baseline, suggesting that the number of estimates having low to moderate errors is far greater than that for the GNSS-only solution. This can also be seen from the horizontal line at the 90% confidence level, where high-confidence localisation is achieved with low error values.

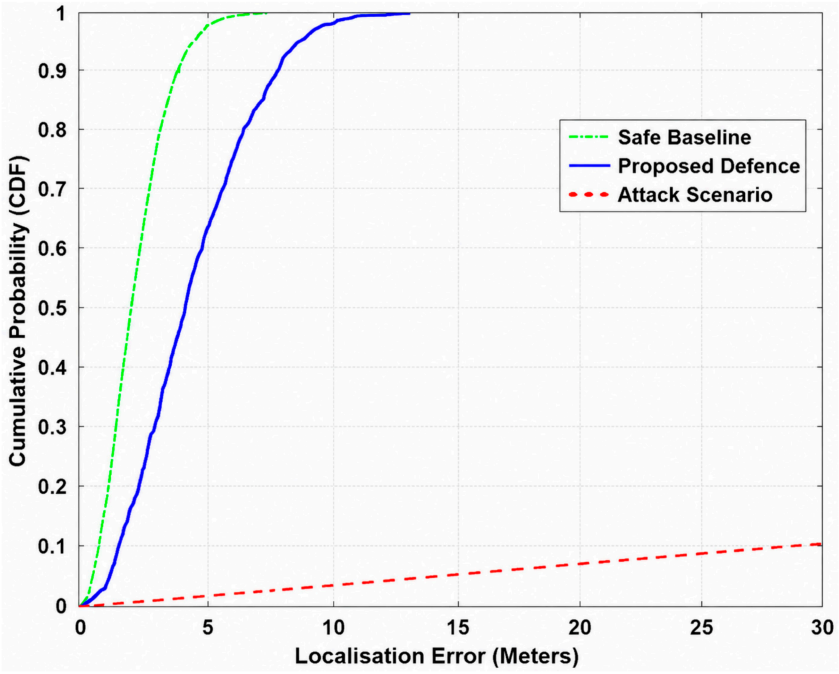

Figure 5. Cumulative distribution function of localisation error for the safe baseline, the attack scenario, and the proposed defence.

While Figure 5 presents the localisation accuracy in terms of its distribution, Figure 6 shows how the localisation error changes with time when an attack takes place. The red

dotted line shows the attacked case without any protection, while the blue line shows the proposed localisation architecture using the PLS layer. This temporal performance is consistent with what can be seen in Table 5. In the unprotected case, the localisation error increases gradually since the GNSS branch is persistently pulled towards the spoofing attack, while the sidelink branch is constantly suffering from jamming interference.

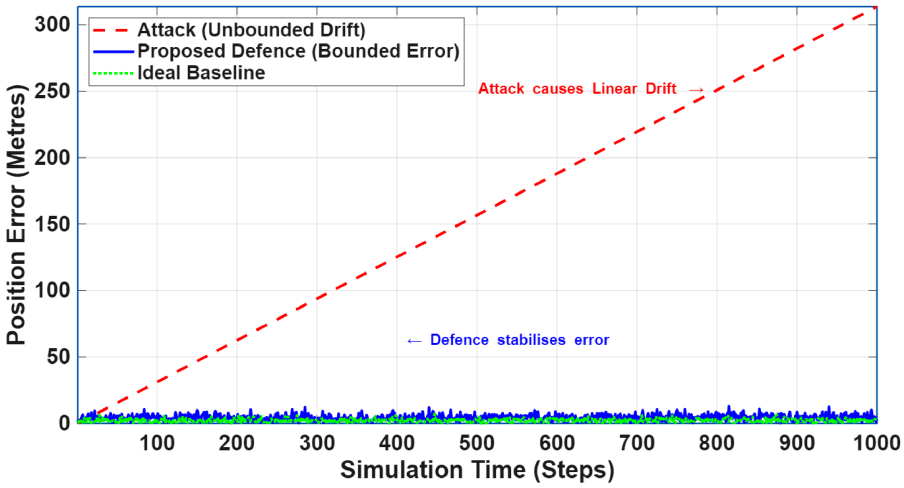

Figure 6. Localisation error evolution.

In contrast, once the proposed PLS-based cooperative approach is activated, the growth of the localisation error is significantly reduced. The threat situation is detected by the LSTM detector, the cleaner provides a more accurate RSSI signal, and the cooperative approach shows an advantage over the fused approach. Thus, the blue curve is restricted within rather small boundaries of the error. This proves that the proposed approach not only reduces the average error but also prevents further growth of the localisation error under threat conditions. However, this does not mean that the error is completely eliminated, since some deviation exists even under defended conditions because of competition as well as the inaccuracy of the detector and cleaner. Thus, the conclusion is that the proposed approach should be considered as providing an appreciable improvement in the localisation error under threat conditions.

4.3.2. Trajectory Correction Under Attack

Figure 7 illustrates the spatial impact of the proposed defence on the vehicle trajectory. The ground-truth path is shown in green, the attacked and undefended GNSS-dominated trajectory is shown in red, and the defended cooperative trajectory is shown in blue. In the undefended case, the estimated path drifts far from the ground-truth trajectory, which is consistent with the large RMSE, MAE, and MaxErr values reported for Scenarios S1 and S2. This spatial divergence demonstrates the practical effect of the drag-off spoofing attack: even if the deviation develops gradually, it eventually drives the localisation estimate away from the intended road corridor.

In contrast, the trajectory corresponding to the proposed defended case remains much closer to the ground-truth path. Although some residual offset and fluctuation remain, the defended trajectory follows the true route in a qualitatively consistent manner and avoids the large spatial drift observed in the undefended baselines. This visual behaviour supports the substantial reductions in the RMSE and MAE reported for Scenario S6. It also confirms the main conclusion of the paper: the benefit of the proposed framework arises from the joint action of attack detection, RSSI purification, and cooperative fusion, rather than from signal cleaning in isolation.

Because the defended trajectory still exhibits a non-zero residual deviation, the result should not be interpreted as complete recovery to the benign GNSS-only case. Instead, it shows that the proposed framework is able to preserve a practically usable localisation track under the simulated hybrid attack, while greatly reducing the off-path behaviour seen in the undefended scenarios. This interpretation is more consistent with the reported MaxErr and avoids overstating the safety guarantee of the present single-scenario study.

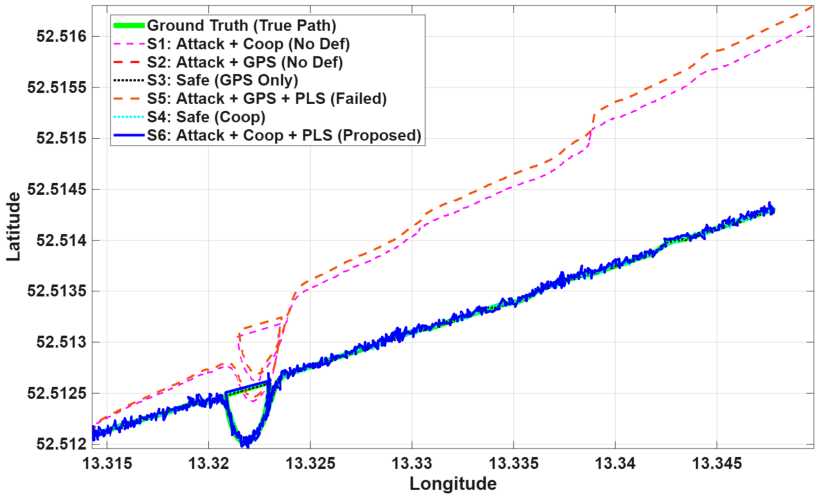

Figure 7. Trajectory-level comparison of the ground-truth path, benign baselines, attacked localisation cases, and the proposed PLS-assisted cooperative defence.

5. Conclusions

In this paper, an approach towards physical-layer security using deep learning algorithms was introduced to provide resilience to attacks on the cooperative localisation process in the form of a hybrid attack that combines GNSS spoofing via drag-off and RSSI jamming. In the design of the presented framework, two main functions have been included within the localisation process: an LSTM detector to detect the attacked physical-layer state and an RSSI cleaner to perform regression on the corrupted RSSI values. This combination of the two functions allows for the recovery of the clean sidelink signal prior to its usage for localisation purposes. The findings indicate that the discussed hybrid attack leads to significant localisation performance degradation without any countermeasure being employed. In the scenario where only the GNSS was attacked, the localisation error rose to an RMSE of 149.93 m, an MAE of 129.81 m, and a MaxErr of 259.62 m. Even the attacked cooperative scheme without any countermeasure still exhibited very poor performance, with the RMSE being equal to 134.94 m. In contrast, the RMSE of the defended cooperative localisation dropped to 4.00 m, with an MAE of 3.51 m and a MaxErr of 12.01 m. It is obvious that the advantage in the latter case did not result from the pure signal cleaning, since, in this instance, the attacked and the defended GNSS-only localisation schemes were the same. The reason for this positive effect lies in the cooperation of the above three techniques within a closed defence localisation scheme. The validity of deep learning was also used to demonstrate the efficiency of the proposed PLS module. Discrimination between the physical layers' attacked and safe states was successfully achieved by the LSTM detector, and a significant reconstruction error reduction for the jammed RSSI signal was attained through the regression-based cleaner method. In terms of computational time, the LSTM detector needed about 0.00109 s per sequence of input data and the cleaner needed about 0.00051 s per sample of RSSI data on a CPU processor. Accordingly, even in the case where the two modules operate simultaneously, the extra processing time of PLS amounts to approximately 1.6 ms per update, which is considerably shorter than the usual time interval

of 100 ms associated with a rate of 10 Hz for cooperative vehicular communications. Future lines of research include the extension of the proposed methodology to non-linear spoofing attacks, burst and adaptive RSSI jamming, complex geometric configurations with more than one vehicle, fusion weighting based on the confidence level, and the implementation of the method with hardware-in-the-loop testing on vehicular platforms. With such extensions, it will then be possible to assess how effective the proposed physical-layer security solution can be against many different types of attacks, while retaining the main idea from this paper, i.e., that robust localisation can be obtained by a unified loop process.

Author Contributions: Conceptualisation, A.M.A.A.E., M.J.A. and M.A.S.; methodology, A.M.A.A.E. and M.A.S.; software, A.M.A.A.E.; validation, A.M.A.A.E., M.J.A. and M.A.S.; formal analysis, A.M.A.A.E. and M.A.S.; investigation, A.M.A.A.E., M.J.A. and M.A.S.; resources, A.M.A.A.E., M.J.A. and M.A.S.; data curation, A.M.A.A.E.; writing—original draft preparation, A.M.A.A.E.; writing—review and editing, M.J.A. and M.A.S.; visualisation, A.M.A.A.E.; supervision, M.J.A.; project administration, A.M.A.A.E. and M.A.S.; funding acquisition, M.J.A. All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia (IPP: 1037-135-2025). The authors, therefore, acknowledge with thanks the DSR for the technical and financial support.

Data Availability Statement: The data analysed in this study are openly available in IEEE DataPort. The Berlin V2X dataset can be accessed at https://ieee-dataport.org/open-access/berlin-v2x, DOI: 10.21227/8cj7-q373, 8 December 2022.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Full Term
AI	Artificial Intelligence
BSM	Basic Safety Message
C-ITS	Cooperative Intelligent Transport System
CAM	Cooperative Awareness Message
CNN	Convolutional Neural Network
CSI	Channel State Information
C-V2X	Cellular Vehicle-to-Everything
DL	Deep Learning
DoS	Denial-of-Service
EV	Electric Vehicle
FC	Fully Connected
FN	False Negative
FP	False Positive
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IDS	Intrusion Detection System
ITS-G5	Intelligent Transport System Operating at 5.9 GHz
LSTM	Long Short-Term Memory
MAE	Mean Absolute Error
MaxErr	Maximum Error
PDF	Probability Density Function
PLE	Path Loss Exponent
PLS	Physical-Layer Security

RAIM	Receiver Autonomous Integrity Monitoring
ReLU	Rectified Linear Unit
RF	Radio Frequency
RMSE	Root Mean Square Error
RNN	Recurrent Neural Network
ROC-AUC	Receiver Operating Characteristic–Area Under the Curve
RSSI	Received Signal Strength Indicator
SNR	Signal-to-Noise Ratio
TCN	Temporal Convolutional Network
TN	True Negative
TP	True Positive
V2X	Vehicle-to-Everything
WLS	Weighted Least Squares

References

1. Walch, M.; Schirrer, A.; Neubauer, M. Impact Assessment of Cooperative Intelligent Transport Systems (C-ITS): A Structured Literature Review. *Eur. Transp. Res. Rev.* **2025**, *17*, 11. [CrossRef]
2. Noor-A-Rahim, M.; Liu, Z.; Lee, H.; Khyam, M.O.; He, J.; Pesch, D.; Moessner, K.; Saad, W.; Poor, H.V. 6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities. *Proc. IEEE* **2022**, *110*, 712–734. [CrossRef]
3. Niebisch, M.; Deinlein, T.; Pfaller, D.; German, R.; Djanatliev, A. Impact of the Communication Direction on the Reliability of Vehicle-to-Everything (V2X) Communications. In *Proceedings of the 2020 IEEE Vehicular Networking Conference (VNC)*; IEEE: New York, NY, USA, 2020; pp. 1–7.
4. Zheng, R.; Zheng, S.; Yu, S.; Ye, M.; Li, W. A V2X-Based Cooperative Positioning Method Through Enhanced KF and Transmission Delay Compensation in GNSS-Denied Scenarios. *Automot. Innov.* **2025**, *8*, 59–71. [CrossRef]
5. Focarelli, G.; Zanini, S.; Palamà, I.; Bianchi, G.; Bartoletti, S. Positioning Security in 5G and Beyond: Model and Detection of Physical Layer Threats. *IEEE Trans. Wirel. Commun.* **2026**, *25*, 1048–1061. [CrossRef]
6. Huang, P.; Gönültaş, E.; Arnold, M.; Srinath, K.P.; Hoydis, J.; Studer, C. Attacking and Defending Deep-Learning-Based Off-Device Wireless Positioning Systems. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 8883–8895. [CrossRef]
7. Meng, L.; Yang, L.; Yang, W.; Zhang, L. A Survey of GNSS Spoofing and Anti-Spoofing Technology. *Remote Sens.* **2022**, *14*, 4826. [CrossRef]
8. Michieletto, G.; Formaggio, F.; Cenedese, A.; Tomasin, S. Robust Localization for Secure Navigation of UAV Formations Under GNSS Spoofing Attack. *IEEE Trans. Autom. Sci. Eng.* **2023**, *20*, 2383–2396. [CrossRef]
9. Dasgupta, S.; Irfan, M.S.; Rahman, M.; Chowdhury, M. Detection and Mitigation of Spoofing Attacks In-Based Autonomous Ground Vehicle Navigation Systems. In *Data Analytics for Intelligent Transportation Systems*; Elsevier: Amsterdam, The Netherlands, 2025; pp. 403–427.
10. Radoš, K.; Brkić, M.; Begušić, D. Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors* **2024**, *24*, 4210. [CrossRef] [PubMed]
11. Abhishek, A.N.; Balaji, A.; Avinash, D.; Harish, D.; Santhameena, S. Evaluating GNSS Spoofing and Jamming Attacks on UAV Navigation: Implementation and Impact. In *Proceedings of the 2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 7–9 March 2025*; IEEE: New York, NY, USA, 2025; pp. 540–546.
12. Meheretu, S.E.; Nigussie, E.; Gebremeskel, G.B.; Hailesilassie, S.Y. A Systematic Literature Review on Spoofing and Jamming Approaches in Unmanned Aerial Vehicles Navigation. *J. Aerosp. Technol. Manag.* **2025**, *17*, e3425. [CrossRef]
13. Mitev, M.; Pham, T.M.; Chorti, A.; Barreto, A.N.; Fettweis, G. Physical Layer Security—From Theory to Practice. *IEEE BITS Inf. Theory Mag.* **2023**, *3*, 67–79. [CrossRef]
14. Zhang, P.; Xu, B. Research on Cooperative Collimating and Locating Model of Air Defense Based on Extended Kalman Filter. In *Proceedings of the International Symposium on Computer Applications and Information Systems (ISCAIS 2022)*; Sarfraz, M., Cen, M., Eds.; SPIE: Shenzhen, China, 2022; p. 41.
15. Xiao, Q.; Zhao, J.; Feng, S.; Li, G.; Hu, A. Securing NextG Networks with Physical-Layer Key Generation: A Survey. *Secur. Saf.* **2024**, *3*, 2023021. [CrossRef]
16. Jin, X.; Zhang, X.; Zheng, S. Indirect Kalman Filtering for Robust GNSS Spoofing Detection in Signal Quality Monitoring. *Signal Process.* **2026**, *239*, 110321. [CrossRef]
17. Liang, W.; Li, K.; Li, Q. Anti-Spoofing Kalman Filter for GPS/Rotational INS Integration. *Measurement* **2022**, *193*, 110962. [CrossRef]

18. Irfan, M.S.; Dasgupta, S.; Rahman, M. A Particle Filter Based Sensor Fusion Approach for GNSS Spoofing Detection Incorporating Autonomous Ground Vehicle Navigation Constraints. In *Proceedings of the 2025 IEEE/ION Position, Location and Navigation Symposium (PLANS), Salt Lake City, UT, USA, 28 April–1 May 2025*; IEEE: New York, NY, USA, 2025; pp. 105–111.
19. Pullen, S.; Joerger, M. GNSS Integrity and Receiver Autonomous Integrity Monitoring (RAIM). In *Position, Navigation, and Timing Technologies in the 21st Century*; Morton, Y.T.J., Diggelen, F., Spilker, J.J., Parkinson, B.W., Lo, S., Gao, G., Eds.; Wiley: Hoboken, NJ, USA, 2020; pp. 591–617.
20. Boo, J.; Kim, H. Threat of Unreliable GPS and Technical Needs for Advanced Air Mobility. *J. Aerosp. Inf. Syst.* **2026**, *23*, 214–222. [CrossRef]
21. Tong, H.; Feng, L.; Zhang, P.; Wu, P.; Zheng, Y.; Liu, W. GNSSMulti-Spoofing Detection and Angle-of-Arrival Estimation with a Rotating Dual-Antenna System. *IEEE Trans. Aerosp. Electron. Syst.* **2026**, *62*, 7822–7837. [CrossRef]
22. Chen, S.; Ni, S.; Lei, T.; Cheng, L.; Song, X. GNSS Spoofing Detection via the Intersection Angle between Two Directions of Arrival in a Single Rotating Antenna. *Sensors* **2024**, *24*, 1116. [CrossRef]
23. Jin, W.; Wu, S.; Zhang, G.; Si, R.; Teng, L.; Chen, W.; Ding, H.; Zhu, C. An Array Antenna-Based Attitude Determination Method for GNSS Spoofing Mitigation in Power System Timing Applications. *Appl. Sci.* **2026**, *16*, 3289. [CrossRef]
24. Wang, S.-Q.; Liu, J.; Cai, B.-G.; Wang, J.; Lu, D.-B. BOSVDD-Based GNSS Spoofing Detection for Rail Vehicle Positioning. *IEEE Trans. Instrum. Meas.* **2025**, *74*, 8500418. [CrossRef]
25. Arif, S. Adaptive Interference Mitigation in GPS Receivers. Doctoral Dissertation, University of Westminster, London, UK, 2022. [CrossRef]
26. Boualouache, A.; Engel, T. A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1128–1172. [CrossRef]
27. Lusvarghi, L.; Grazia, C.A.; Klapez, M.; Casoni, M.; Merani, M.L. Awareness Messages by Vulnerable Road Users and Vehicles: Field Tests via LTE-V2X. *IEEE Trans. Intell. Veh.* **2023**, *8*, 4418–4433. [CrossRef]
28. Zoghlami, C.; Kacimi, R.; Dhaou, R. Dynamics of Cooperative and Vulnerable Awareness Messages in V2X Safety Applications. In *Proceedings of the 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 30 May–3 June 2022*; IEEE: New York, NY, USA, 2022; pp. 853–858.
29. Alabdouli, H.; Hassan, M.S.; Abdelfatah, A. Enhancing Route Guidance with Integrated V2X Communication and Transportation Systems: A Review. *Smart Cities* **2025**, *8*, 24. [CrossRef]
30. Farsimadan, E.; Moradi, L.; Palmieri, F. A Review on Security Challenges in V2X Communications Technology for VANETs. *IEEE Access* **2025**, *13*, 31069–31094. [CrossRef]
31. Figueiredo, A.; Rito, P.; Luís, M.; Sargento, S. Mobility Sensing and V2X Communication for Emergency Services. *Mob. Netw. Appl.* **2023**, *28*, 1126–1141. [CrossRef]
32. Arikumar, K.S.; Prathiba, S.B.; Basheer, S.; Moorthy, R.S.; Dumka, A.; Rashid, M. V2X-Based Highly Reliable Warning System for Emergency Vehicles. *Appl. Sci.* **2023**, *13*, 1950. [CrossRef]
33. Venkatasamy, T.K.; Hossen, M.J.; Ramasamy, G.; Aziz, N.H.B.A. Intrusion Detection System for V2X Communication in VANET Networks Using Machine Learning-Based Cryptographic Protocols. *Sci. Rep.* **2024**, *14*, 31780. [CrossRef]
34. Abdel Hakeem, S.A.; Kim, H. Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 11137–11205. [CrossRef]
35. Alsaleh, A. Hybrid Deep Learning Approach for Secure Electric Vehicle Communications in Smart Urban Mobility. *Vehicles* **2025**, *7*, 112. [CrossRef]
36. Altaweel, A.; Mukkath, H.; Kamel, I. GPS Spoofing Attacks in FANETs: A Systematic Literature Review. *IEEE Access* **2023**, *11*, 55233–55280. [CrossRef]
37. Cappelli, I.; Carli, F.; Fort, A.; Intravaia, M.; Micheletti, F.; Peruzzi, G.; Vignoli, V. Enhanced Visible Light Localization Based on Machine Learning and Optimized Fingerprinting in Wireless Sensor Networks. *IEEE Trans. Instrum. Meas.* **2023**, *72*, 9503410. [CrossRef]
38. Kerdjidj, O.; Himeur, Y.; Sohail, S.S.; Amira, A.; Fadli, F.; Atalla, S.; Mansoor, W.; Copiaco, A.; Gawanmeh, A.; Miniaoui, S.; et al. Uncovering the Potential of Indoor Localization: Role of Deep and Transfer Learning. *IEEE Access* **2024**, *12*, 73980–74010. [CrossRef]
39. Liu, Y.-T.; Chen, J.-J.; Tseng, Y.-C.; Li, F.Y. An Auto-Encoder Multitask LSTM Model for Boundary Localization. *IEEE Sens. J.* **2022**, *22*, 10940–10953. [CrossRef]
40. Kordi, K.A.; Roslee, M.; Alias, M.Y.; Alhammadi, A.; Waseem, A.; Osman, A.F. Survey of Indoor Localization Based on Deep Learning. *Comput. Mater. Contin.* **2024**, *79*, 3261–3298. [CrossRef]
41. Rathnayake, R.M.M.R.; Maduranga, M.W.P.; Tilwari, V.; Dissanayake, M.B. RSSI and Machine Learning-Based Indoor Localization Systems for Smart Cities. *Eng* **2023**, *4*, 1468–1494. [CrossRef]
42. Nessa, A.; Adhikari, B.; Hussain, F.; Fernando, X.N. A Survey of Machine Learning for Indoor Positioning. *IEEE Access* **2020**, *8*, 214945–214965. [CrossRef]

43. Jia, B.; Liu, J.; Feng, T.; Huang, B.; Baker, T.; Tawfik, H. TTSL: An Indoor Localization Method Based on Temporal Convolutional Network Using Time-Series RSSI. *Comput. Commun.* **2022**, *193*, 293–301. [CrossRef]
44. Solaija, M.S.J.; Salman, H.; Arslan, H. Towards a Unified Framework for Physical Layer Security in 5G and Beyond Networks. *IEEE Open J. Veh. Technol.* **2022**, *3*, 321–343. [CrossRef]
45. Kazmi, S.H.A.; Hassan, R.; Qamar, F.; Nisar, K.; Ibrahim, A.A.A. Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions. *Symmetry* **2023**, *15*, 1147. [CrossRef]
46. Hoang, T.M.; Vahid, A.; Tuan, H.D.; Hanzo, L. Physical Layer Authentication and Security Design in the Machine Learning Era. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1830–1860. [CrossRef]
47. Ye, Q.; Fan, X.; Fang, G.; Bie, H. Exploiting Temporal Dependency of RSS Data with Deep Learning for IoT-Oriented Wireless Indoor Localization. *Internet Technol. Lett.* **2023**, *6*, e366. [CrossRef]
48. Yue, B.; Jiang, A.; Yang, C.; Lei, J.; Liu, H.; Zhang, Y. Deep Learning-Enhanced Human Sensing with Channel State Information: A Survey. *Comput. Mater. Contin.* **2026**, *86*, 1–28. [CrossRef]
49. Sai, S.; Sharma, D.; Peelam, M.S.; Chamola, V.; Guizani, M.; Niyato, D. Machine Learning Techniques for Wi-Fi CSI-Based Recognition and Sensing: A Comprehensive Review. *IEEE Internet Things J.* **2026**, *13*, 20190–20214. [CrossRef]
50. Hernangomez, R.H.; Geuer, P.G.; Palaios, A.P.; Schäufele, D.S.; Watermann, C.W.; Taleb-Bouhemadi, K.T.-B.; Parvini, M.P.; Krause, A.K.; Partani, S.P.; Vielhaus, C.V.; et al. Berlin V2X: A machine learning dataset from multiple vehicles and radio access technologies. In *Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 20–23 June 2023*; IEEE: New York, NY, USA, 2023.