AoA-aided Kalman Filter to Mitigate False Data Injections Attacks in Vehicular Scenarios

Luis Javier Puente Lam*†, Pedro M. Santos*
*Cister Research Centre, Instituto Superior de Engenharia do Porto (ISEP)
†Faculdade de Engenharia da Universidade do Porto (FEUP)
Porto, Portugal
{javie,pss}@isep.ipp.pt

2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall) | 979-8-3315-1778-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/VTC2024-Fall63153.2024.10757691

***Abstract*—In Autonomous Driving (AD), precise positioning is crucial for safe, efficient and cost-effective transportation. However, malicious cyber threats such as false data injection (FDI) attacks via Vehicle-to-Everything (V2X) links can significantly undermine these goals. FDI involves the insertion of incorrect data into the ego-vehicle or information system (IS), at specific points in time (Impulse FDI) or over specific intervals (Pulse FDI). To combat the specific threat of incorrect position data being shared by a Vehicle-of-Interest, our approach leverages collaboration between a set of trusted participants to perform positioning by exchanging Angle-of-Arrival (AoA) measurements over sidelinks paired with a Kalman Filter. Our method reduces localization errors caused by Impulse FDI to below $10m$ in 60% of cases, and the errors caused by Pulse FDI in 66.39% of cases.**

***Index Terms*—V2X, False Data Injection, Kalman Filter, Cooperative Wireless Positioning, Angle-of-Arrival, MUSIC**

I. Introduction

Autonomous driving (AD) relies heavily on accurate perception of the surrounding world, to ensure safe and efficient transportation. However, physical limitations (e.g., resolution and detection range) of onboard sensors such as cameras, radar, and Lidar constrain its effectiveness. Vehicle-to-Everything (V2X) links, including to-vehicle (V2V), or *sidelinks*, and to-network (V2N), i.e., links between user equipment and base station, can expand the knowledge horizon of vehicles by enabling Cooperative Perception (CP) services. A simple example is vehicles wirelessly advertising their position (obtained e.g. from GPS) and kinematic information (speed and direction). However, reporting faulty, inaccurate, or incorrect positions can lead to serious accidents. Position mis-reports can occur due to multiple reasons, such as GPS malfunction (e.g. in an urban canyon); or if the vehicle is compromised by a cyber-attack, i.e., it suffered an intrusion that makes it intentionally mis-report position data in the V2X messages. The later situation is known as a **False Data Injection (FDI)** attack [1]. FDI can happen at one point in time (e.g., to falsely indicate a vehicle stopped at a crosswalk) – **Impulse FDI** –, or over intervals of time (e.g., to hide route deviations) – **Pulse FDI**.

This work was supported by national funds through the FCT/MCTES, Portuguese Foundation for Science and Technology, within the CISTER, ISEP/IPP Research Unit (UIDP/UIDB/04234/2020), and also by project Route 25 (ref. TRB/2022/00061 - C645463824-00000063), funded by the EU/Next Generation, within call N.º 02/C05-i01/2022 of the Recovery and Resilience Plan (RRP).

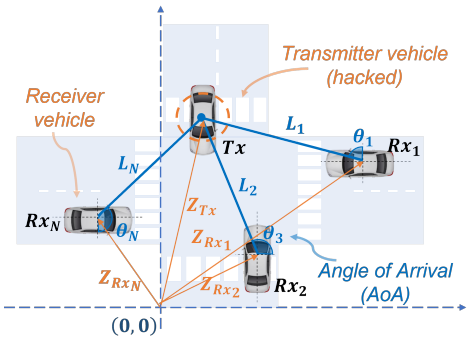


Fig. 1: Scenario showing a Vehicle-of-Interest (VoI) Tx that has been hacked using FDI, and a set of n cooperating vehicles Rx_1,..., Rx_n, that measure AoA of Tx's transmissions using antenna arrays and compute intersections to estimate the Tx's location.

The same V2X wireless communication infrastructure can be explored to verify the correctness of positions reported by a given vehicle, refered to as **Vehicle-of-Interest (VoI)** independently, therefore mitigating the effect of FDI cyber-attacks. Wireless Positioning (WP) leverages physical layer mechanisms such as **Angle-of-Arrival (AoA)** to compute the angle of a transmitter relative to the receiver. A set of receiver vehicles (trusted parties) interested in verifying the reported position can exchange AoAs to estimate the VoI's location independently. This is shown in Fig. 1.

The detection and mitigation of FDI attacks has motivated various approaches. Machine Learning (ML) algorithms are able to analyze normal behavior patterns and alert in case of anomalies [2]. In [3], an SVM-based classifier was implemented to recognize *malicious* or *trustworthy* data packets from other vehicles. In [4], the authors propose a local-global fuzzy clustering method for detecting FDI based on Deep-Learning. In [5], seven representative classification algorithms for detecting common injection attacks on in-vehicle networks were discussed. However, ML approaches require accurate historical data and a high-speed system for classification. To

remove reliance from historical data, **Kalman Filter (KF)** have been applied to FDI detection and mitigation [6]. In [7], a robust KF for the Automated Guided Vehicle state estimation in FDI attacks using Huber loss function was discussed. However, it uses solely local information.

In this paper, we use a **Kalman Filter to mitigate the impact of FDIs in position data reported by the VoI**, thereby producing an position estimate of the VoI that is more accurate. The KF is complemented with a cooperative positioning mechanism in which a set of receiver vehicles (trusted) share among themselves their AoA to the VoI (measured when a V2X message is received from the VoI), therefore producing an independent position estimate that can be compared with the reported one. The KF seamlessly integrates both position data (reported and estimated through cooperation) to produce a position estimate that is accurate and resilient to FDIs. The KF obviates the need for extensive historical datasets and can exhibit lower computational demands compared to ML-based methods. Our proposed approach is capable of estimating the position of the VoI with a mean error of $8.60m$ and a standard deviation of $4.21m$ in the presence of Impulse FDI. Against Pulse FDI, it achieves a mean error of $9.01m$ and a standard deviation of $6.75m$.

The rest of this paper is organized as follows. Section II presents the FDI mitigation mechanism. In section III, we report the main results. Section IV contains the concluding remarks.

II. KF Using AoA for FDI Mitigation

We first introduce the FDI attack model that we consider (Section II-A). We then explain the details of our approach, observing the following sequence.

1. **AoA computation** Receiver vehicles estimate AoA to VoI from phase difference measurements (Section II-B).
2. **Cooperative Positioning.** Vehicles share their position, and observed AoA; at each vehicle, position (cooperative) of VoI is computed by projection intersection (Section II-C).
3. **Kalman Filter to mitigate FDI.** Individual vehicles employ a Kalman Filter to reduce position errors caused by FDI and AoA measurements (Section II-D).

A. FDI Attack Model

An FDI attack is a type of cyberattack in which the intruder injects false data into the real data stream of a system. According to [8], two of the most common forms of FDI are:

- **Impulse FDI:** Data is injected instantaneously, i.e. at specific points (randomly) in time.
- **Pulse FDI:** Data is fed over a certain period of time.

We consider z_{pos} as the position of the VoI according to its kinematic model, and also as its exact localization. For simplicity, we assume that the vehicle moves at a constant speed, then $x = \frac{v}{t}$. More sophisticated kinematic models will be addressed in future works. The FDI attacks are launched at time t_{FDI}. The position that the vehicle reports to the BS at each time t is z_{rep}. Then, the impulse FDI and the pulse FDI can be modeled by Eq. 4a and Eq. 4b, respectively:

$$\mathrm{z}_{rep} = \begin{cases} \mathrm{z}_{pos} + \vec{\mathrm{n}}_{pos} & \text{if } t_{FDI} \\ \mathrm{z}_{pos} & \text{otherwise} \end{cases} \tag{1a}$$

$$\mathrm{z}_{rep} = \begin{cases} \mathrm{z}_{pos} + \vec{\mathrm{n}}_{pos} & \text{if } t_{FDIstart} \leq t_{FDI} \leq t_{FDIend} \\ \mathrm{z}_{pos} & \text{otherwise} \end{cases} \tag{1b}$$

where $\vec{\mathrm{n}}_{pos}$ represents a translation in the reported position due to tampering. The translation $\vec{\mathrm{n}}_{pos}$ can be of different nature, depending on the attacker's intention. For example, a random vector can be assigned to $\vec{\mathrm{n}}_{pos}$ if the goal is just to obfuscate one's location (as considered in this work). Or the attacker may wish to simulate that the VoI is in a parallel lane/street; in that case, $\vec{\mathrm{n}}_{pos}$ would be set at a systematic offset w.r.t. to the VoI's position (e.g., 5 meters to the right). When no false data was fed, we assume that the VoI reported position is exact and not impacted by any sources of noise (e.g., GPS error).

B. Angle-of-Arrival Estimation at Individual Vehicle

Consider $\mathbf{n}$ vehicles: one transmitter Tx (the VoI), and $\mathbf{n-1}$ receivers Rx. The transmitter emits signals isotropically. The receiving vehicles are equipped with a Uniform Circular (antenna) Array (UCA) with radius r, consisting of M antennas (in our scenario, we use $M = 4$) spaced at distance d_{ant}. The wavelength of narrowband is denoted as λ with $\lambda = \frac{c}{f}$, and $d_{\mathrm{ant}} < \lambda$.

The incident signals from the D transmitters, along with their amplitude and phase, are represented by complex quantities $s_1, s_2, ..., s_D$, from directions $\theta_1, \theta_2, ..., \theta_D$. For simplicity, we set $D=1$. Incoming signals vary over time, and therefore we take k samples over time of the incoming signal.

The incident signals are represented by the steering vector $\vec{\mathbf{a}} = a(\theta_i)$, where the first column, $a(\theta_1)$, corresponds to the steering vector for the first user, and so on.

$$a(\theta_1) = \begin{bmatrix} G_0 e^{j\beta p_0} \\ G_1 e^{j\beta p_1} \\ \vdots \\ G_{M-1} e^{j\beta p_{M-1}} \end{bmatrix}$$

with $\beta = \frac{2\pi}{\lambda}$, and $p_m = r \cdot cos\left(\frac{2\pi m}{M} - \theta_1\right)$, $m = 0, ..., M-1$. G_m represents the antenna gain in the direction θ. As we assume isotropic antennas, $G_m = 1$.

Then, the received signal $\vec{\mathbf{x}}$ is expressed as:

$$\vec{\mathbf{x}} = \vec{\mathbf{a}} s + \vec{\mathbf{n}}_{\mathrm{AoA}} \tag{2}$$

$$\vec{\mathbf{x}} = \begin{bmatrix} a(\theta_1) & ... & a(\theta_D) \end{bmatrix} \begin{bmatrix} s_1(k) \\ s_2(k) \\ \vdots \\ s_D(k) \end{bmatrix} + \vec{\mathbf{n}}_{\mathrm{AoA}}(k) \tag{3}$$

where $\vec{\mathbf{n}}_{\mathrm{AoA}}$ identifies noise components affecting the signals received at each antenna independently, such as shadowing, fading, and multipath. In this paper, we do not address these propagation phenomena, i.e. we consider all vehicles under Line-of-Sight (LoS) conditions. However, we recognize their

importance and will consider them in future work. Instead, we focus on a proof-of-concept for cooperative WP and the application of KF to improve positioning accuracy in FDI attacks. Hence, for simplicity, we assume that $\vec{\mathbf{n}}_{\mathrm{AoA}}$ follows a white Gaussian noise model: $\vec{\mathbf{n}}_{\mathrm{AoA}}(k) \sim \mathcal{N}(\mu_{\mathrm{n_{AoA}}}, \sigma_{\mathrm{n_{AoA}}})$ for each k. In this signal model, the MUSIC algorithm (MUltiple SIgnal Classification) can estimate the direction of the incoming signal. MUSIC decomposes the signal correlation matrix into two orthogonal matrices: the signal subspace and the noise subspace. Direction can be estimated from either subspace, assuming uncorrelated noise in each channel.

C. Cooperative Position Determination using SVD

The receiving vehicles (engaged in positioning the VoI) share their positions and measured AoAs to the VoI θ_i between themselves. Using that information, each vehicle can internally represent signal trajectories as lines on the world map L_i, as shown in Fig.1. The arrival angles θ_i measured by the cooperating vehicles must be mapped to a common (world) reference system, which leads to $\theta_{i,(CR)}$. By defining the orientation of a receiver vehicle in the common reference system as $\alpha_{\mathrm{i,(CR)}}$, we use $\alpha_{\mathrm{i,(CR)}}$ as an Euclidean rotation operator via the expression $\theta_{i,(CR)} = \theta_i + \alpha_{\mathrm{i,(CR)}}$. When θ_i is mentioned in the following, this refers to $\theta_{i,(CR)}$.

In [9], the authors propose that the relationship between each receiving vehicle Rx_i located at position $\mathrm{z_{Rx_i}} = [x_i, y_i]^{\mathrm{T}}$, and the transmitting vehicle Tx located at $\mathrm{z_{Tx}} = [x, y]^{\mathrm{T}}$ as:

$$\mathrm{z_{Tx}} = \mathrm{z_{Rx}}i + d_{\mathrm{Tx-Rx_i}} \cdot \mathrm{v_{Rx}}i \tag{4}$$

where $\mathrm{v_{Rx}}i = [\cos\theta_i, \sin\theta_i]^{\mathrm{T}}$ is the unit vector in the L_i direction, and $d_{\mathrm{Tx-Rx_i}}$ is the distance between each receiving vehicle and the transmitter (which we assume is unknown). Then, Eq. 4 can be rewritten as:

$$-x_i \sin\theta_i + y_i \cos\theta_i = -x \sin\theta_i + y \cos\theta_i \tag{5}$$

In the case of n receiving vehicles, the following system of equations is derived:

$$\begin{bmatrix} -x_1 \sin\theta_1 + y_1 \cos\theta_1 \\ \vdots \\ -x_n \sin\theta_n + y_n \cos\theta_n \end{bmatrix} \approx \begin{bmatrix} -\sin\theta_1 & \cos\theta_1 \\ \vdots & \vdots \\ -\sin\theta_n & \cos\theta_1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \tag{6}$$

In simplified matrix notation, $b(\theta) \approx A(\theta) \cdot \mathrm{z_{TX}}$.

The above system of equations can be solved using the Singular Value Decomposition (SVD) of the matrix $A(\theta)$:

$$A(\theta) = U \Sigma V^T$$

where U is a unitary (orthogonal) matrix of size $n \times n$, then $U^T = U^{-1}$. Σ is a diagonal matrix with non-negative singular values. V^T is a unitary (orthogonal) matrix of size 2×2. Substituting the SVD into the system of equations:

$$U^T b(\theta) = \Sigma V^T \mathrm{z_{TX}}$$

Let $\mathbf{z} = V^T \mathrm{z_{TX}}$, then $\mathbf{z} = \Sigma^{-1} U^T b(\theta)$, and Tx's position (cooperative position) is calculated by $\mathrm{z_{TX}}$ = Vz.

D. Kalman Filter

1) Overview: The Kalman Filter (KF) is an iterative mathematical process that uses successive data inputs with a series of equations. The stochastic model defines the noise characteristics, while the dynamic model shows the behavior of the state variables. These are the most important factors that influence the performance of KF. The KF consists of two steps, as follows:

- **Predict Step:** The state transition matrix $\mathbf{F}$ facilitates the prediction of the future state of the system, while the process noise covariance matrix $\mathbf{Q}$ accounts for the uncertainties in this prediction process.

$$\mathrm{x}_{k|k-1} = \mathrm{F}\mathrm{x}_{k-1|k-1} \tag{7a}$$

$$\mathrm{P}_{k|k-1} = \mathrm{F}\mathrm{P}_{k-1|k-1}\mathrm{F}^T + \mathrm{Q} \tag{7b}$$

- **Update Step:** The observation matrix $\mathbf{H}$ is used to calculate the residual $\mathbf{y}$, which captures the difference between predicted and observed values. This residual is described by the residual covariance matrix $\mathbf{S}$. Adjustments to the state estimate are determined by the Kalman gain matrix $\mathbf{K}$, which compensates for the effects of prediction errors and observation uncertainties. The state error covariance matrix $\mathbf{P}$ is then updated to improve the accuracy of the state estimation process. $\mathbf{I}$ is the identity matrix.

$$\mathrm{y}_k = \mathrm{z}_k - \mathrm{H}\mathrm{x}_{k|k-1} \tag{8a}$$

$$\mathrm{S}_k = \mathrm{H}\mathrm{P}_{k|k-1}\mathrm{H}^T + \mathrm{R} \tag{8b}$$

$$\mathrm{K}_k = \mathrm{P}_{k|k-1}\mathrm{H}^T\mathrm{S}_k^{-1} \tag{8c}$$

$$\mathrm{x}_{k|k} = \mathrm{x}_{k|k-1} + \mathrm{K}_k\mathrm{y}_k \tag{8d}$$

$$\mathrm{P}_{k|k} = (\mathrm{I} - \mathrm{K}_k\mathrm{H})\mathrm{P}_{k|k-1} \tag{8e}$$

2) Application: To reduce the position error caused by FDI attacks, we consider two mechanisms: a KF that uses solely the positions reported over V2X by the VoI, and a KF that uses the cooperative position estimate. Accordingly, two Kalman filters were modeled by using Eq. 7 and Eq. 8:

- **KF-Reported.** A KF for reported positions. We use the positions obtained from the vehicle kinematic model $\mathrm{z}_{pos,t}$ and the positions reported to the BS $\mathrm{z}_{rep,t+1}$, to estimate the position in the next state $\mathrm{z}_{pos,t+1}$ (Fig. 2).
- **KF-Cooperative.** KF for cooperative positions based on AoA. Similar to KF-Reported, we use the positions reported by the VoI $\mathrm{z}_{rep,t}$ and the positions estimated from the cooperative positioning based on AoA measurements $\mathrm{z}_{CoopAoA,t}$ to improve the position estimate of the Tx at time $t+1$ (Fig. 3).

The vector $\mathrm{x} = [x, \dot{x}, y, \dot{y}]^{\mathrm{T}}$ represents the state of the system, which includes the position and velocity in two dimensions. We assume that the VoI moves at a constant speed

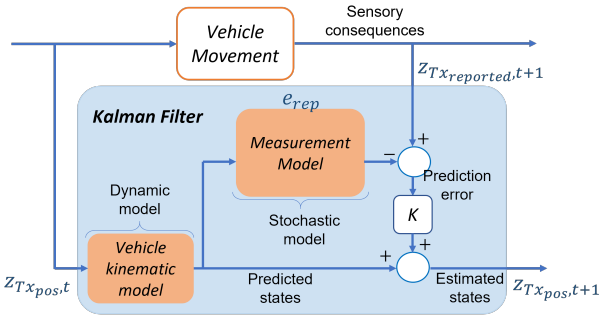


Fig. 2: Local Kalman Filter (KF-Reported)

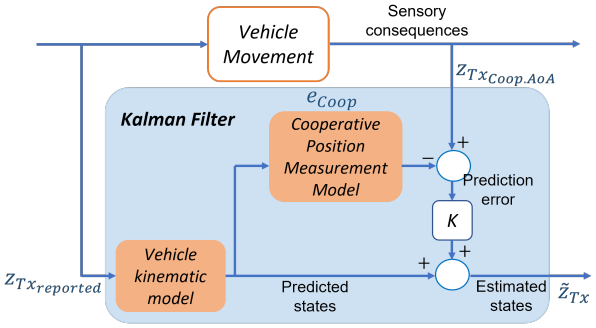


Fig. 3: Cooperative Kalmen Filter (KF-Cooperative)

(i.e. no acceleration), and therefore the state transition model F must reflect that the speed does not change over time:

$$\mathbf{F} = \begin{bmatrix} 1 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

where $\Delta t = 1s$. We initialize the covariance matrix $\mathbf{P}_{4\times4} = 10^3 \cdot \mathbf{I}_{4\times4}$ with a high value (i.e. high uncertainty in the initial system estimate). The covariance matrix of the process noise was set as $\mathbf{Q}_{4\times4} = 10^{-3} \cdot \mathbf{I}_{4\times4}$, since we consider that the kinematic model provides exact positions of the system. The Observation matrix $\mathbf{H}$ means that only the positions x and y are directly observed.

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The covariance matrix of the measurement noise $\mathbf{R}_{2\times2}$ represents the uncertainty of the observations. The observation vector $\mathrm{z} = [\mathrm{z}_x, \mathrm{z}_y]^{\mathrm{T}}$ represents the measured positions. In the case of KF for reported positions, the state and observation vectors are $\mathrm{x} = [x_{\mathrm{z}_{Pos}}, \dot{x}_{\mathrm{z}_{Pos}}, y_{\mathrm{z}_{Pos}}, \dot{y}_{\mathrm{z}_{Pos}}]^{\mathrm{T}}$ and $\mathrm{z} = [\mathrm{x}_{Rep}, \mathrm{y}_{Rep}]^{\mathrm{T}}$, respectively. For AoA-based cooperative positions, KF was initialized with $\mathrm{x} = [x_{\mathrm{z}_{Rep}}, \dot{x}_{\mathrm{z}_{Rep}}, y_{\mathrm{z}_{Rep}}, \dot{y}_{\mathrm{z}_{Rep}}]^{\mathrm{T}}$ and $\mathrm{z} = [\mathrm{x}_{Coop}, \mathrm{y}_{Coop}]^{\mathrm{T}}$.

III. Experimental Evaluation

We report performance results of our technique in a simulated scenario.

TABLE I: Simulation Parameters

Parameter	Value
k: Number of time snapshots	2000
c: Speed of light in a vacuum	3×10^8 m/s
f: Signal frequency	2.442×10^9 Hz
M: Number of antennas	4
D: Number of incoming signals	1
d_{ant}: Spacing between antennas	10^{-1} m

A. System Model

We use a 5×5 Manhattan mobility model, where the distances between intersections are fixed at $100m$. We consider $N_{\mathrm{TX}} = 1$ and $N_{\mathrm{RX}} = 3$. Both the start and end position of each vehicle are drawn arbitrarily from the list of grid corners, following an uniform distribution (u.d.). The vehicles move at constant speed along random paths: at each intersection, the simulator randomly selects the next intersection from the set of immediately neighbouring intersections (given the small size of the scenario, only a few loops occur). The speeds of the individual vehicles are also randomly selected (u.d.) from a range of speeds between 10 and $50km/h$ (maximum speed in urban areas). The simulation time step is 1s, and vehicles produce one AoA estimate per (simulated) second.

We performed 10 experimental runs. The length of traversed trajectories vary across runs due to the stochastic nature of the generation process. We obtained an average of 152 AoA samples per run with a standard deviation of 47.87 samples and a total of 1444 samples.

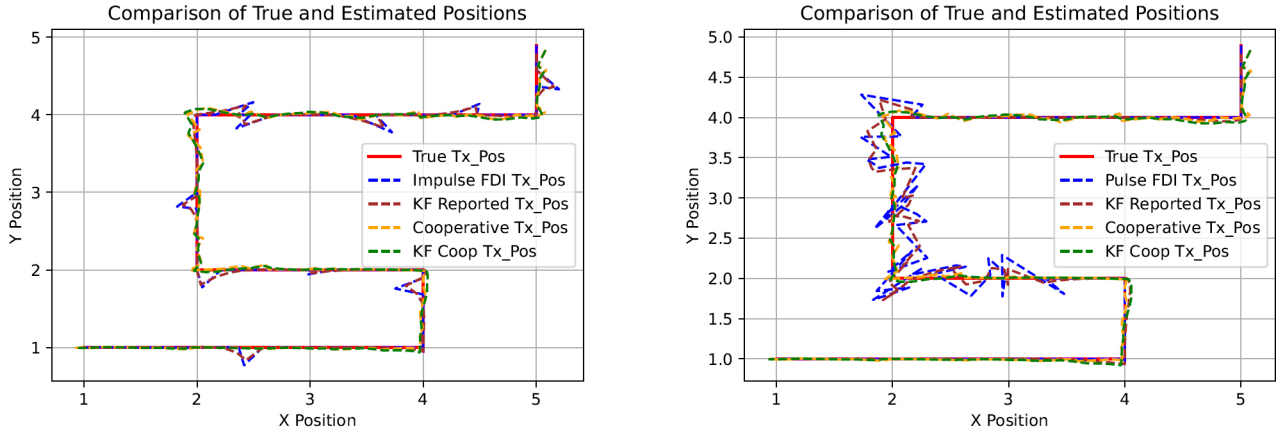
FDI were modeled according to Eq. 4a and Eq. 4b for the FDI impulse and the FDI pulse, respectively. A term $\vec{\mathbf{n}}_{\mathrm{pos}}(t_{FDI}) \sim \mathcal{U}(-30, 30)$, i.e. each component of the position vector z_{pos} at the specific instances t_{FDI} is randomly perturbed by the hacking event within the range $[-30m, 30m]$. The time instances for false data injection, in the case of the Impulse, were selected randomly (u.d.), with 10 hacks per run. For the FDI Pulses, we defined a time interval of $35s$ per run. The pulse is also triggered randomly (u.d.). Among of 1444 positions, 100 were hacked with impulse FDI and 350 with pulse FDI. All samples from uniform distributions were produced using Python's *random.choice()* function.

For the purpose of AoA estimation, the signal reception at multiple antennas is modelled according to Eq. 3. As explained in Sec. II-B, in our work, we model noise n_{AoA} as following a Gaussian distribution with parameter values $\mu_{\mathrm{AoA}} = 0$ and $\sigma^2_{\mathrm{n_{AoA}}} = 0.3$. Cooperative positions were calculated with the model described in Sec. II-C.

All the above details were implemented in a simulator for mobility and wireless channel, and paired with a code version of the MUSIC algorithm. The implementation uses Python v3.12.0. Parameter values are listed in Table I.

B. Results

We discuss first a specific run (i.e, one trajectory of the 10 experimental runs). In Fig. 4 we observe that, for both types of FDI, the **KF-Reported** (blue dashed line) tends to follow the reported positions (in brown). The AoA-based cooperative positioning (yellow color) provides a good estimates during



(a) Impulse FDI attack

(b) Pulse FDI attack

Fig. 4: Position estimates in the presence of FDI attacks (example scenario).

an FDI attack, but with some errors (modelling propagation phenomena). Hacked positions are disregarded when AoA measurements are used for **KF-Cooperative** (green), improving AoA-based positioning in 68.0% of Impulse FDI cases and in 67.78% of Pulse FDI cases.

To evaluate how much the impact of FDI can be mitigated, we analyzed the errors observed in the hacked positions, the estimated location when applying **KF-Reported**, the positions obtained by the cooperative method, and the location obtained from **KF-Cooperative**. All errors were calculated as the Euclidean distance between estimate and true position, i.e. $|z - \tilde{z}|$. The statistical analysis of the errors in the position estimates for both Impulse and Pulse FDI is summarized in Table II and Table III. The analysis was only performed at the moments when a hack was injected.

TABLE II: Accuracy of Position Estimation Errors against Impulse FDI Attacks

Error Type	*Impulse FDI Pos.*	*KF-Reported*	*Coop. Pos.*	*KF-Cooperative*
Average (m)	22.73	17.40	10.12	8.60
Std. Dev. (m)	8.46	6.74	5.92	4.21
%<10m	8.0	14.0	50.0	60.0

TABLE III: Accuracy of Position Estimation Errors against Pulse FDI Attacks

Error Type	*Pulse FDI Pos.*	*KF-Reported*	*Coop. Pos.*	*KF-Cooperative*
Average (m)	23.58	16.28	10.47	9.01
Std. Dev. (m)	8.10	7.00	8.80	6.75
%<10m	7.5	19.72	50.83	66.39

C. Discussion

The error analysis shows that **KF-Reported** improves the reported positions, but is not sufficient to significantly reduce the localization error. Alternatively, **KF-Cooperative** has better performance. When the cooperative position estimate is available , the estimate from the reported position is mitigated. This shows that obtaining additional information is crucial for the usefulness of KF in this type of scenario.

IV. Conclusions and Future Work

We introduce a mitigation scheme for FDI in a vehicular scenario. Our proposed approach integrates a KF assisted by cooperative Wireless Positioning using AoA to mitigate localization errors caused by FDI. Specifically, our method reduced Impulse FDI-induced localization errors to less than $10m$ in 60.0% of cases, and Pulse FDI-induced errors similarly to less than $10m$ in 66.39% of cases.

Future work will include the simulation of shadowing effects due to urban obstacles (e.g. buildings) and the modeling of multipath reception over multiple antennas. We will use advanced kinematic models to account for rapid maneuver changes due to interactions with other road users, including lane changes. In addition, other KF architectures, such as the Extended Kalman Filter (EKF) and the Unscented Kalman Filter (UKF), will also be explored.

References

[1] M. Ahmed and A. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," Complex Adaptive Systems Modeling, vol. 8, no. 4, 2020.

[2] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False Data Injection Attacks against State Estimation in Wireless Sensor Networks," in 49th IEEE CDC. IEEE, 2010, pp. 5967–5972.

[3] J. D. Cabelin, P. V. Alpano, and J. R. Pedrasa, "SVM-based Detection of False Data Injection in Intelligent Transportation System," in ICOIN, 2021, pp. 279–284.

[4] S. A. Almalki and F. T. Sheldon, "Deep learning to improve false data injection attack detection in cooperative intelligent transportation systems," in IEEE 12th IEMCON, 2021, pp. 1016–1021.

[5] H. Ji, L. Wang, H. Qin et al., "In-vehicle network injection attacks detection based on feature selection and classification," Automotive Innovation, vol. 7, pp. 138–149, 2024.

[6] J. Li and Y. Zhang, "Detection of False Data Injection attack in CPS by Adaptive Unscented Kalman Filter," in 49th IEEE IECON, 2023, pp. 1–6.

[7] M. Elsisi, M. Altius, S.-F. Su, and C.-L. Su, "Robust kalman filter for position estimation of automated guided vehicles under cyberattacks," IEEE Trans. on Instr. and Meas., vol. 72, pp. 1–12, 2023.

[8] A. S. Tummala and R. K. Inapakurthi, "A Two-Stage Kalman Filter for Cyber-attack Detection in Automatic Generation Control System," Journal of Modern Power Syst. and Clean Energy, vol. 10, no. 1, pp. 50–59, 2021.

[9] A. Pages-Zamora, J. Vidal, and D. H. Brooks, "Closed-Form Solution for Positioning based on Angle of Arrival Measurements," in The 13th IEEE PIMRC, vol. 4. IEEE, 2002, pp. 1522–1526.