2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Cyber-attack Detection Framework for Connected Vehicles in V2X Networks Based on An Iterative UFIR Filter

Kai Jiang, Zhiyang Ju, Lingying Huang and Rong Su

***Abstract*—Connected vehicles have great advantages in driving safety and energy efficiency under the support of vehicle-to-everything (V2X) networks, while they are also vulnerable to malicious cyber-attacks. To enhance the cyber security of connected vehicles, a cyber-attack detection framework is proposed based on multi-source information fusion specifically for the vehicle localization system. In this framework, an iterative unbiased finite impulse response (UFIR) filter is utilized to estimate the vehicle position with low computational load, based on the vehicle dynamics model and information from the inertial measurement system (IMU), GPS, and V2X networks. In addition, a discriminator module is developed to analyze the residuals between estimations and position information from different sources for cyber-attack detection. Finally, multiple simulation cases are implemented to validate the effectiveness of the proposed framework.**

***Index Terms*—Cyber-attack detection, Unbiased finite impulse response filter, V2X networks, Connected vehicles**

I. Introduction

Thanks to the advancement of communication technology, connected vehicles have greatly improved in terms of traffic efficiency, driving safety, and fuel economy. However, with the increasing connectivity of vehicles, they become more vulnerable to cyber-attacks that could compromise their safety, functionality, and even the privacy of their passengers [1]. In 2020, a research team demonstrated how they could use GPS spoofing to take control of a Tesla Model X's navigation system, causing the vehicle to deviate from its intended trajectory [2]. Besides, another example is the cyber-attack on GPS manufacturer Garmin, which resulted in a widespread outage of the company's services. The attack reportedly caused significant disruption to Garmin's localization systems. These incidents illustrate the growing threat of cyber-attacks on vehicles and transportation systems, highlighting the need for increased security measures and vigilance in protecting against such attacks.

To detect malicious cyber-attacks on localization systems and guarantee the driving security of connected vehicles, researchers have conducted a lot of relevant work. Information-oriented cyber-attack detection is a typical method of detecting cyber-attacks by leveraging communication security techniques [3], such as encryption, plausibility checking, and user authentication. Some popular works, such as signature-based attack detection methods for vehicular ad hoc networks (VANETs) [4], trust authentication approaches for mitigating malicious attack behaviors [5], probabilistic model checking methods for different deception attack detection [6], etc. had been developed for connected vehicles, respectively. Information-oriented cyber-attack detection method achieves good results in many scenarios, however, this approach focuses primarily on detecting attacks that exploit communication channels or involve the transmission of data. It cannot detect attacks that exploit other system vulnerabilities, such as hardware or software weaknesses.

Control-oriented cyber-attack detection is the other important method for cyber security in connected vehicles. One typical approach to control-oriented cyber-attack detection is to use data-driven methods, such as machine learning. Different classical supervisor machine learning methods were employed to detect and isolate the cyber-attacks in localization systems for autonomous robots [7]. The deep neural network was another topical approach for cyber-attack detection for localization systems in connected vehicles. In [8], convolutional neural network (CNN), general neural network (GNN), etc. were developed to extract the attack features and further used for attack detection. Besides, reinforcement learning (RL) was adopted for cyber-attack detection in connected vehicle navigation as well [9]. While data-driven approaches have effective performance in many applications, they are only effective against attacks related to the training data, making it difficult for them to detect new attacks. Additionally, the generation of training data for arbitrary cyber-attacks can be challenging, which further impacts the generalization performance of these approaches.

This research is supported by A*STAR under its RIE2020 Advanced Manufacturing and Engineering (AME) Industry Alignment Fund C Pre Positioning (IAF-PP) (Award A19D6a0053). *(Corresponding author: Rong Su.)*

Kai Jiang, Lingying Huang and Rong Su are with the School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, 639798, Singapore. Zhiyang Ju is with the School of Mechanical Engineering, Beijing Institute of Technology, Beijing 100081, China.

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

The commonly used approach to control-oriented cyber-attack detection is the model-based method. The basic idea behind this approach is to create a model of the system, and then compare the predicted or estimated states to the expected behaviors based on the model. The authors in [10] utilized the Kalman filter and dynamics model to estimate the deception attacks in vehicle platoon position systems. Moreover, adaptive sliding mode method was used for cyber-attack detection in the connected vehicle as well [11]. These works greatly improved the detection accuracy and robustness by direct attack estimation, but they are only applicable to a certain kind of attack. In [12], the authors designed integrated frameworks to detect multiple cyber-attacks by sensor fusion and achieved satisfactory detection performance. However, the works were only developed for individual autonomous vehicles and failed to extend to connected vehicle platoons.

To further ensure the cyber security for connected vehicles or platoons, we propose a comprehensive cyber-attack detection framework capable of handling different types of attacks in this work. The framework mainly consists of three detectors, and each detector is developed through multi-source information fusion. In each detector, an iterative UFIR filter is employed to achieve the information fusion and get the position estimation, then a designed discriminator is used to evaluate the residuals between UFIR estimation and position measurements from different channels (GPS and V2X networks) and determine if there is a cyber-attack. Finally, the developed framework is validated on a vehicle simulation platform, and the simulation results demonstrate the framework is efficient to detect different cyber-attacks such as denial of service (DoS) attack, replay attack, etc.

The rest of this paper is organized as follows. Section II shows the detailed problem formulation. Section III presents the cyber-attack detection framework for connected vehicles. Section IV mainly depicts the simulation results and discussions. At last, the conclusion is shown in Section V.

II. Problem Formulation

In this section, the brief system composition and main research problem will be introduced.

A. Vehicle dynamics

To effectively make use of the onboard IMU information, a brief vehicle dynamics model is adopted in this work. The vehicle longitudinal, lateral, and yaw motions are considered in the dynamics model. The diagram and detailed equations of vehicle dynamics are shown as follows.

$$\begin{cases} m\dot{v}_y = -mv_x\gamma + 2[C_{cf}(\dfrac{v_y + l_f\gamma}{v_x} - \delta_f) + C_{cr}\dfrac{l_r\gamma - v_y}{v_x}], \\ m\dot{v}_x = mv_y\gamma + 2[C_{lf}s_f + C_{lr}s_r + C_{cf}(\delta_f - \dfrac{v_y + l_f\gamma}{v_x})\delta_f], \\ \Omega_z\dot{\gamma} = 2[C_{cf}l_f(\dfrac{v_y + l_f\gamma}{v_x} - \delta_f) - C_{cr}l_r\dfrac{l_r\gamma - v_y}{v_x}], \end{cases} \tag{1}$$

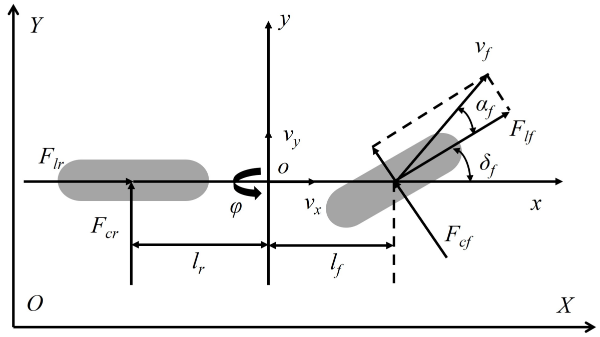


Fig. 1. Diagram of vehicle dynamics

.

where v_y and v_x are the vehicle longitudinal and lateral velocity, C_{lf} and C_{lr} are the longitudinal stiffness of the front and rear tire, C_{cf} and C_{cr} are the lateral stiffness of the front and rear tire, s_f and s_r refer to the tire slip rate of the front and rear wheel, l_f and l_r are the distances between the vehicle center of gravity and front wheel and real wheel, Ω denotes the vehicle yaw inertia, γ means the yaw rate, δ_f represents the steering angle, and m is the vehicle mass.

Additionally, to predict the location of connected vehicles, the brief vehicle motion dynamics geodetic coordinate system is also considered. The motion dynamics are shown below:

$$\begin{cases} \dot{Y} = v_x sin\varphi + v_y cos\varphi, \\ \dot{X} = v_x cos\varphi - v_y sin\varphi, \\ \dot{\varphi} = \gamma, \end{cases} \tag{2}$$

where X and Y are the coordinates of vehicle, and φ means the yaw angle.

Then combining the vehicle dynamics and motion dynamics together, we could obtain the final vehicle model. Moreover, as the vehicle measurements are not continual signals, the system model and output model are formulated in discrete form:

$$\begin{cases} x_{k+1} = f(x_k, u_k) + \omega_k, \\ y_k = g(x_k) + v_k, \end{cases} \tag{3}$$

where $x = [v_y, v_x, \gamma, Y, X, \varphi]^{\mathrm{T}}$ denotes the system state, y expresses the system output which may change with different sensing devices, ω and v are system and measurement noises which are assumed to be independent Gaussian white noise with zero mean, f and g are system equation and measurement equation, and $u = \delta_f$ refers to the input.

B. Problem statement

In connected and automated vehicles, location information is very important for further decision-making and underlying control. Generally, the location information of connected vehicles can be achieved from GPS and V2X networks easily. Moreover, the onboard IMU can also measure the vehicle acceleration and indirectly provide the location information.

The brief system description is shown in Fig. 2. These pieces of information from different channels together build the efficient navigation system of the connected vehicles, while they are also vulnerable to external cyber-attacks because of vehicle connectivity. Malicious cyber-attacks could disrupt the normal operation of the system and further result in serious traffic accidents. Therefore, to enhance the cyber security and driving safety of connected vehicles, a cyber-attack detection framework is proposed in this work.

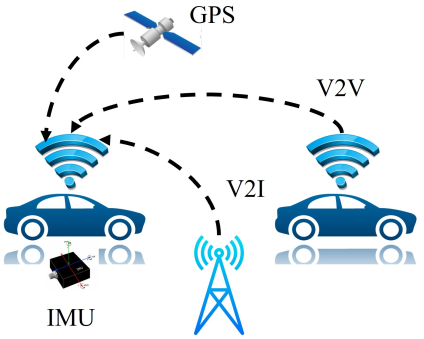


Fig. 2. System description of connected vehicles

.

The proposed framework consists of three detectors, which are used to estimate the vehicle pose states. The first detector is developed based on the GPS and IMU information fusion. The information fusion is realized through an iterative UFIR filter, where the IMU measurements are used in the prediction process and GPS measurements are used in the update process. Finally, by evaluating the estimation residuals, cyber-attacks against GPS can be detected effectively. Similarly, the second detector is built based on the information from V2X networks and IMU, and utilized for cyber-attack detection in V2X networks. Nevertheless, the third detector is designed to provide short-term location estimation according to the system model and IMU measurements, when the GPS and V2X networks are all under cyber-attacks. The flowchart of the detection framework is presented in Fig. 3.

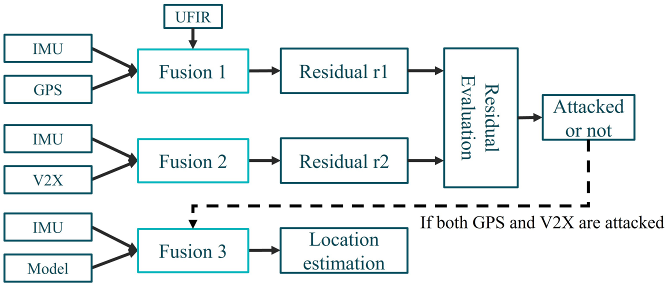


Fig. 3. Cyber-attack detection framework for connected vehicles

.

Remark: In this work, as the IMU device is installed inside the connected vehicles and it doesn't have any information exchange with the external environment, it is difficult to be attacked by the potential hacker. Therefore, we assume the IMU measurements are reliable and used as the baseline in the three detectors.

III. Methodology of the Cyber-Attack Detection Framework

In this section, the UFIR estimation algorithm and detailed cyber-attack detection method will be introduced.

The UFIR filter is a kind of novel estimation method that utilizes previous measurement batches to estimate current system states. Unlike the Kalman filter, UFIR filter only relies on the number of historical measurements, thus, it is more robust to inaccurate initial values, biased noise statistics, and model mismatch. These features of the UFIR filter make it more suitable for practical estimation scenarios.

As is shown in Eq. (3), the vehicle system is formulated as a nonlinear model. To better implement the estimation, model linearization is necessary. Then the Eq. (3) can be described as below:

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + \omega_k, \\ y_k = Hx_k + \upsilon_k, \end{cases} \tag{4}$$

where A, B, and H are the model paraments.

The method to derive the UFIR filter is to extend Eq. (4) from the time instant $m = k - N + 1$ to K, and apply the discrete convolution. The extended equations are presented as follows:

$$X_{k,m} = A_N x_m + B_N U_{k,m} + E_N W_{k,m}, \tag{5}$$

$$Y_{k,m} = H_N x_m + \bar{B}_N U_{k,m} + \bar{E}_N W_{k,m} + V_{k,m}, \tag{6}$$

where the initial value x_m can be read from the measurements, and the extended states are defined as:

$$\begin{aligned} &X_{k,m} = [x_k, x_{k-1} \cdots x_m]^{\mathrm{T}}, Y_{k,m} = [y_k, y_{k-1} \cdots y_m]^{\mathrm{T}}, \\ &U_{k,m} = [u_k, u_{k-1} \cdots u_m]^{\mathrm{T}}, W_{k,m} = [w_k, w_{k-1} \cdots w_m]^{\mathrm{T}}, \\ &V_{k,m} = [v_k, v_{k-1} \cdots v_m]^{\mathrm{T}}. \end{aligned} \tag{7}$$

The extended parameter matrixs are denoted as below:

$$\begin{aligned} A_N &= [A^N, A^{N-1} \cdots A]^{\mathrm{T}}, \\ B_N &= \begin{bmatrix} B & AB & \cdots & A^{N-2}B & A^{N-1}B \\ 0 & B & \cdots & A^{N-3}B & A^{N-2}B \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & B & AB \\ 0 & 0 & \cdots & 0 & B \end{bmatrix}, \\ E_N &= \begin{bmatrix} I & A & \cdots & A^{N-2} & A^{N-1} \\ 0 & I & \cdots & A^{N-3} & A^{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & I & A \\ 0 & 0 & \cdots & 0 & I \end{bmatrix}, \\ H_N &= \bar{H}_N A_N, \\ \bar{H}_N &= diag(H \cdots H)_N, \\ \bar{B}_N &= \bar{H}_N B_N, \\ \bar{E}_N &= \bar{H}_N B_N. \end{aligned} \tag{8}$$

According to Eq. (6) and ordinary least square, the estimation $\hat{x}_k$ can be calculated as:

$$\hat{x}_k = \Phi_{k,m} Y_{k,m} + \bar{\Phi}_{k,m} U_{k,m}, \tag{9}$$

where $\Phi_{k,m}$ and $\bar{\Phi}_{k,m}$ are the UFIR filter gains to be determined by the recent measurements and objective function. Meanwhile, the real value of x_k can be achieved based on the system model Eq. (5).

$$x_k = A^N x_m + \acute{B}_N U_{k,m} + \acute{E}_N W_{k,m}, \tag{10}$$

where $\acute{B}_N$ and $\acute{E}_N$ denote the first row vectors of B_N and E_N respectively.

Finally, by fulfilling the unbiasedness condition $E[x_k] = E[\hat{x}_k]$ of UFIR filter theory, the UFIR filter gains and estimation at k step are achieved [13]. The detailed derivation process is shown as below:

$$\Phi_{k,m} = A^N (H_N^{\mathrm{T}} H_N)^{-1} H_N^{\mathrm{T}}, \tag{11}$$

$$\bar{\Phi}_{k,m} = \acute{B}_N - \Phi_{k,m} \bar{B}_N. \tag{12}$$

$$\begin{aligned} \hat{x}_k =& A^N (H_N^{\mathrm{T}} H_N)^{-1} H_N^{\mathrm{T}} Y_{k,m} \\ &+ (\acute{B}_N - A^N (H_N^{\mathrm{T}} H_N)^{-1} H_N^{\mathrm{T}} \bar{B}_N) U_{k,m}, \end{aligned} \tag{13}$$

Remark: The measurement interval N is a parameter that can be adjusted in this algorithm, and it has a significant impact on the estimation errors and computational complexity. In this paper, we adopt a simple method of trial and error to obtain the sub-optimal measurement interval N_{op}. The analytical method to calculate N_{op} based on mean square error minimization can be found in [14].

The batch UFIR algorithm consists of some high-dimension matrix operations which are related to the number of recent measurements N. Therefore, it is necessary to integrate an iterative algorithm in the batch UFIR to reduce the computational load. It is assumed that the x_k is calculated based on the equations above and historical measurements, the iterative procedure can be denoted as follows:

$$\hat{x}_{k+1} = A\hat{x}_k + BU_{k+1} + K_{k+1}[z_{k+1} - H(A\hat{x}_k + BU_{k+1})], \tag{14}$$

where

$$K_{k+1} = \Psi_{k+1} H^{\mathrm{T}}, \tag{15}$$

$$\Psi_{k+1} = [H^{\mathrm{T}} H + (A \Psi_k A^{\mathrm{T}})^{-1}]^{-1}. \tag{16}$$

Here, Ψ is defined as the generalized noise power gain (GNPG) that is calculated through the recent measurements as well [15]. The initial expression is presented as below:

$$\Psi_k = A^M (H_M^{\mathrm{T}} H_M)(A^M)^{\mathrm{T}}. \tag{17}$$

In order to estimate the location information in our application, the IMU measurements are used in the prediction process, and the information from GPS and V2X networks are used in the update process. Then, by combining the introduced UFIR filter and system model, the fused location information can be achieved.

Remark: The UFIR filter has shown superior performance compared to the Kalman filter when handling situations where there is unknown knowledge of disturbances and noises. As a result of this advantage, the UFIR estimator is employed for cyber-attack detection, particularly in cases where it is difficult to determine the distribution of disturbances or model uncertainty in real-world connected vehicles.

To enhance the resilience of the localization system against cyber-attacks and avoid the potential loss of state information in connected vehicles, we establish a distributed state observer based on multi-source information fusion.

In this work, we assume that GPS can provide the longitudinal X_{GPS} and lateral displacement Y_{GPS} of a vehicle. The V2X networks can offer location information X_{V2X} and Y_{V2X}. IMU can provide the longitudinal acceleration $a_{x,IMU}$, lateral acceleration $a_{y,IMU}$ and yaw rate γ_{IMU}.

1) Information Fusion of the GPS and IMU

Based on Eq. (13), the initial estimation $\hat{x}_k$ is achieved through batch UFIR filter. Then to accelerate the estimation, the iterative algorithm is adopted in the update process. In the update process, the IMU measurement will be used to update the acceleration a_y and a_x, and vehicle yaw rate γ. The detailed formula derivation is shown below.

$$\hat{x}_{1,k+1|k} = \begin{bmatrix} \hat{v}_{y,k+1|k} \\ \hat{v}_{x,k+1|k} \\ \hat{\gamma}_{k+1|k} \\ \hat{Y}_{k+1|k} \\ \hat{X}_{k+1|k} \\ \hat{\varphi}_{k+1|k} \end{bmatrix} = \begin{bmatrix} \hat{v}_{y,k} + T \cdot a_{y,IMU} \\ \hat{v}_{x,k} + T \cdot a_{x,IMU} \\ A_3 \hat{x}_k + B_3 u_k \\ A_4 \hat{x}_k + B_4 u_k \\ A_5 \hat{x}_k + B_5 u_k \\ \hat{\varphi}_k + T \cdot \gamma_{IMU} \end{bmatrix}, \tag{18}$$

where T is the sample time, A_i and B_i is the ith row of the parameter matrix A and B in Eq. (4).

In this part, the system outputs are the GPS measurements, so the measurement equation is:

$$y_{1,k+1} = H_1 \hat{x}_{1,k+1|k} = \begin{bmatrix} \hat{Y} \\ \hat{X} \end{bmatrix}, \tag{19}$$

where $H_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$.

Following the Eq.(15) and Eq.(16), the noise power gain Ψ and bias correction gain K can be calculated. Then the GPS measurements are presented as:

$$z_{1,k+1} = \begin{bmatrix} Y_{GPS} \\ X_{GPS} \end{bmatrix}. \tag{20}$$

The final estimation can be obtained through:

$$\hat{x}_{1,k+1} = \hat{x}_{1,k+1|k} + K_{k+1}(y_{1,k+1} - z_{1,k+1}), \tag{21}$$

besides, the estimate residual r is defined as:

$$r_{1,k+1} = y_{1,k+1} - z_{1,k+1}. \tag{22}$$

At last, by repeating the estimation cycle, we can implement the information fusion of GPS and IMU efficiently.

2) Information Fusion of the V2X networks and IMU

The information provided by V2X networks is the vehicle position (X_{V2X} and Y_{V2X}) as well, so the fusion of V2X networks and IMU is quite similar to the GPS and IMU fusion. The only difference between the first fusion and this section is the output measurements. Therefore, the prediction process would not be introduced in this section.

The measurements of V2X networks are depicted as:

$$z_{2,k+1} = \begin{bmatrix} Y_{V2X} \\ X_{V2X} \end{bmatrix}. \tag{23}$$

Then the final estimation and residual are shown as:

$$\hat{x}_{2,k+1} = \hat{x}_{2,k+1|k} + K_{k+1}(y_{2,k+1} - z_{2,k+1}), \tag{24}$$

$$r_{2,k+1} = y_{2,k+1} - z_{2,k+1}. \tag{25}$$

3) Information Fusion of the IMU and vehicle states

In the extreme operation situation, we assume both GPS and V2X networks may be attacked simultaneously, therefore, we have to utilize the IMU measurement and vehicle model to provide short-term location estimation. The detailed estimation equations are shown as follows:

$$\hat{x}_{3,k+1|k} = A\hat{x}_k + Bu_k \tag{26}$$

$$y_{3,k+1} = H_3\hat{x}_{3,k+1|k} = \begin{bmatrix} \hat{a}_y \\ \hat{a}_x \\ \hat{\gamma} \end{bmatrix}, \tag{27}$$

where $H_3 = \begin{bmatrix} (A_1 - P)/T & 0 & 0 & 0 & 0 & 0 \\ 0 & (A_2 - Q)/T & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$, $P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$, $Q = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$.

$$z_{3,k+1} = \begin{bmatrix} \hat{a}_{y,IMU} \\ \hat{a}_{x,IMU} \\ \hat{\gamma}_{IMU} \end{bmatrix}. \tag{28}$$

$$\hat{x}_{3,k+1} = \hat{x}_{3,k+1|k} + K_{k+1}(y_{3,k+1} - z_{3,k+1}), \tag{29}$$

In this section, the IMU measurement is used in the update process but not the prediction process. Since the IMU measured vehicle acceleration is not the system state, we have to use the system states to represent the vehicle acceleration and thereby derive the output matrix H_3.

4) Cyber-attack detection method

During each estimation step, we can get the residuals between UFIR estimations and measurements and use them to detect cyber-attacks. To improve the detection accuracy and robustness, an evaluation function is proposed here:

$$R_t = \sqrt{\frac{1}{\Delta T}\int_t^{t-\Delta T} (r_t^{\mathrm{T}} r_t)\, d\tau}, \tag{30}$$

where R denotes the evaluation function, and ΔT refers to the evaluation interval which set as 1s in this work.

At each time instant, the evaluation function represents the acceleration of the residuals in the last ΔT interval. The acceleration could deal with random outliers in the residuals efficiently and further reduce the misdetection. At last, by comparing the evaluated residuals of $fusion1$ and $fusion2$ with the preset threshold in each estimation loop, the cyber-attack and corresponding attacked channel can be identified.

IV. Simulation results

In this section, multiple simulation tests are carried out on the MATLAB/Simulink platform to validate the effectiveness of our proposed cyber-attack detection framework. The detailed vehicle parameters are shown in the following table.

TABLE I
Vehicle parameters used in the simulation platform.

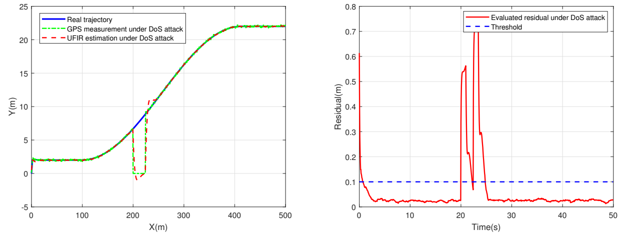
Parameters	Values and Units
Vehicle mass	1500 kg
Distance of front wheel axle from CG	1.3 m
Distance of rear wheel axle from CG	1.4 m
Vehicle moment of inertial on yaw axis	2000 $kg \cdot m^2$
Concerning stiffness	40000 N/rad
Longitudinal velocity of vehicle	10 m/s

In order to demonstrate the capability of detecting different cyber-attacks, three simulation cases are implemented. In the first case, the DoS attack is injected into the GPS system. Secondly, the replay attack is added to the V2V network. At last, the framework performance is validated when the GPS and V2X networks are all under cyber-attacks.

A. DoS cyber-attack against GPS

In this case, the DoS cyber-attack is injected into the GPS to test the performance of the proposed detection framework. The vehicle position estimation based on UFIR filter is shown in Fig. 4a. As is seen in this figure, the estimation could track the real trajectory well and has small differences with GPS measurement when there are no cyber-attack. Once the DoS cyber-attack is injected, the residuals between UFIR estimation and GPS measurement become larger which could help with the cyber-attack detection.

Fig. 4b describes the processed residuals in the whole test cycle. In this figure, we can find that the processed residual is extremely over the pre-set threshold when the cyber-attack is injected, which means our proposed framework can detect the GPS DoS cyber-attack effectively.

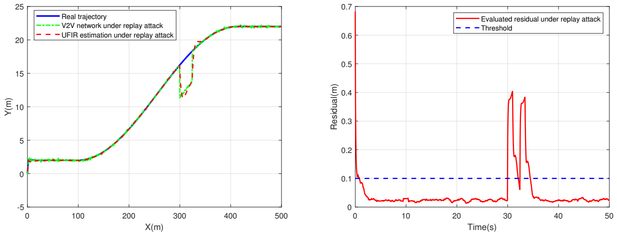


(a) UFIR estimation (b) Evaluated residual

Fig. 4. Cyber-attack detection under GPS DoS cyber-attack.

B. Replay cyber-attack against V2V network

The detection performance of the proposed framework with regard to replay cyber-attack is investigated in this case. The replay cyber-attack is injected into the V2V network and the detection results are presented in Fig. 5. The preset threshold is the same as the first case, and it is smaller than the processed residual obviously when the replay attack occurs. Finally, based on the residual evaluation, we could detect the cyber-attack in the V2V network and send an alert to the main controller.



(a) UFIR estimation (b) Evaluated residual

Fig. 5. Cyber-attack detection under V2V replay cyber-attack.

C. DoS cyber-attack against GPS and replay cyber-attack against V2V network simultaneously

In this case, the replay cyber-attack and DoS cyber-attack are injected into the GPS and V2V network at the same time. As mentioned in Section II, if both the GPS and V2X networks are attacked, the framework may provide short-term location estimation based on the vehicle dynamics and IMU measurement. Fig. 6 describes the estimation performance in the whole test cycle. Specifically, as is seen in the zoom-in part, our proposed UFIR filter can still follow the real trajectory even when the GPS and V2V network are under different attacks. The simulation results illustrate the effectiveness of our framework in extreme working conditions.

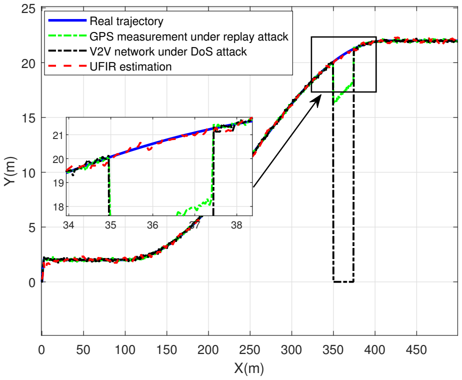


Fig. 6. Cyber-attack detection framework for connected vehicles

.

V. Conclusion

This study investigates the issue of cyber-attack detection in connected and automated vehicles. We propose a comprehensive attack detection framework based on multi-source information fusion to detect different malicious cyber-attacks against connected vehicles. In this framework, we employ the UFIR filter to improve detection accuracy and robustness during the information fusion process. Finally, we implement three simulation cases to validate the attack detection framework, and the simulation results demonstrate the excellent performance of our proposed approach. In the future, we plan to study efficient resilient control strategies based on this detection framework to ensure the driving security of connected vehicles.

References

[1] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective," *IEEE Transactions on Intelligent Vehicles*, 2022.

[2] K. Ghorbani, N. Orouji, and M. R. Mosavi, "Navigation message authentication based on one-way hash chain to mitigate spoofing attacks for gps l1," *Wireless Personal Communications*, vol. 113, pp. 1743–1754, 2020.

[3] Y. Sun, S. Abeywickrama, L. Jayasinghe, C. Yuen, J. Chen, and M. Zhang, "Micro-doppler signature-based detection, classification, and localization of small UAV with long short-term memory neural network," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 8, pp. 6285–6300, 2020.

[4] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616–632, 2021.

[5] D. Suo and S. E. Sarma, "Real-time trust-building schemes for mitigating malicious behaviors in connected and automated vehicles," in *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, pp. 1142–1149. IEEE, 2019.

[6] E. Shaikh, N. Mohammad, and S. Muhammad, "Model checking based unmanned aerial vehicle (uav) security analysis," in *2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, pp. 1–6. IEEE, 2021.

[7] Á. M. Guerrero-Higueras, N. DeCastro-Garcia, and V. Matellan, "Detection of cyber-attacks to indoor real time localization systems for autonomous robots," *Robotics and Autonomous Systems*, vol. 99, pp. 75–83, 2018.

[8] E. M. Khanapuri, R. Sharma, and K. Brink, "Learning-based detection of stealthy false data injection attack applied to cooperative localization problem," in *AIAA SCITECH 2022 Forum*, p. 2543, 2022.

[9] S. Dasgupta, T. Ghosh, and M. Rahman, "A reinforcement learning approach for global navigation satellite system spoofing attack detection in autonomous vehicles," *Transportation research record*, vol. 2676, no. 12, pp. 318–330, 2022.

[10] Z. Ju, H. Zhang, and Y. Tan, "Distributed deception attack detection in platoon-based connected vehicle systems," *IEEE transactions on vehicular technology*, vol. 69, no. 5, pp. 4609–4620, 2020.

[11] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3893–3902, 2018.

[12] D. Zhang, C. Lv, T. Yang, and P. Hang, "Cyber-attack detection for autonomous driving using vehicle dynamic state estimation," *Automotive Innovation*, vol. 4, pp. 262–273, 2021.

[13] D. Simon and Y. S. Shmaliy, "Unified forms for kalman and finite impulse response filtering and smoothing," *Automatica*, vol. 49, no. 6, pp. 1892–1899, 2013.

[14] Y. S. Shmaliy, S. Zhao, and C. K. Ahn, "Unbiased finite impluse response filtering: An iterative alternative to kalman filtering ignoring noise and initial conditions," *IEEE Control Systems Magazine*, vol. 37, no. 5, pp. 70–89, 2017.

[15] S. Zhao, Y. S. Shmaliy, and F. Liu, "Fast kalman-like optimal unbiased fir filtering with applications," *IEEE Transactions on Signal Processing*, vol. 64, no. 9, pp. 2284–2297, 2016.