Physical Layer Authentication Based on Nonlinear Kalman Filter for V2X Communication

JIAN WANG1,2, YAMENG SHAO1,2, YANCONG WANG1,2, Yuming Ge3, and Rundong Yu3

1College of Computer Science and Technology, Jilin University, Changchun 130012, China
2Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun 130012, China
3Technology and Standards Research Institute, China Academy of Information and Communications Technology, Beijing 100191, China

Corresponding author: Yancong Wang (yancong18@mails.jlu.edu.cn)

This work was supported in part by the National Nature Science Foundation under Grant 61572229 and Grant 6171101066, in part by the Jilin Provincial Science and Technology Development Foundation under Grant 20170204074GX and Grant 20180201068GX, in part by the Jilin Provincial International Cooperation Foundation under Grant 20180414015GH, and in part by the CERNET Innovation Project under Grant NGH20170413.

ABSTRACT Authentication is an important guarantee for vehicle to everything (V2X) commercial deployment. Currently, V2X security often use identity authentication schemes based on public key infrastructure (PKI). These schemes need to transmit certificates and signatures when sending safety-related information such as basic safety messages (BSMs), which need to occupy extra bandwidth and reduce the available channel capacity. So, V2X communication efficiency will be seriously affected in traffic congestion. In this paper, we propose a V2X authentication model based on physical layer characteristics. Then we use the Kalman filter to refine the iterative model and threshold model. The iterative model mainly realizes the priori and posteriori estimation of the current time based on the physical layer characteristics of the previous time, which provides the basis for the entire authentication process. The threshold model analyzes the mathematical characteristics of the priori estimation, and gives the calculation method of the authentication threshold. Since the conventional Kalman filter can only be used for linear discrete system, we use extended Kalman filter and unscented Kalman filter to extend the characteristics used for authentication to non-linearity. At the same time, iterative model and threshold model are improved according to these two algorithms. In terms of security and performance, we compare the proposed schemes with the conventional V2X authentication scheme and physical layer authentication scheme, and the effects of these schemes are analyzed by experiment. We select three characteristics for simulation: received signal strength indication (RSSI), the distance between the two vehicles, and the relative speed between the two vehicles. Then we analyze the process and effect of these two filters, and the factors that affect the threshold. Through experiments, the proposed authentication schemes can effectively take the responsibility of identity authentication in the V2X environment, and have high security level and low overhead, which can reduce the consumption of communication resources by security.

INDEX TERMS Physical-layer authentication, V2X security, extended Kalman filter, unscented Kalman filter.

I. INTRODUCTION The vehicle to everything uses the latest generation of information and communication technology to realize omnidirectional vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P), and vehicle to network/cloud (V2N/V2C) network connections. Identity security and authentication are an important guarantee for V2X commercial deployment. V2X communication process between users, vehicles, infrastructures and clouds requires identity legitimacy authentication for participants such as on-board unit (OBU) and roadside unit (RSU). It can prevent vehicles from making wrong judgments once hackers break through and attack one or all of OBUs and RSUs, which will lead to accidents such as vehicle collisions that endanger people and public safety. Therefore, in the V2X environment, security
incidents are more harmful than the traditional Internet, which highlights the importance of V2X security.

V2X is facing a variety of security threats, including forgery of communication content, deletion of communication content, replay of communication content, malicious requests for communication resources, fake communication identities, and user privacy [1]–[3]. The use of authentication can effectively solve these security threats, improving the safety of driving. On the basis of ensuring the effectiveness and efficiency of V2X, it can also improve traffic efficiency and driving experience. Currently, countries such as Europe and the United States have researched and deployed V2X communication security schemes and certification management platforms based on PKI. The PKI-based security schemes mainly use certificates and signatures technologies to realize the authentication of the vehicles [4], [5].

As the vehicle moves at high speed, V2X direct communication has extremely high requirements on the communication delay and the real-time of messages [6]. Direct communication refers to communication between vehicles or communication between vehicle and roadside facility. It has the characteristics of short connection time and short timeliness of information [7], [8]. Therefore, traditional wireless communication technologies such as WiFi and 4G cannot meet the requirements of direct communication. The current V2X communication technology includes Dedicated Short-Range Communications (DSRC) technology based on WiFi and cellular-V2X (C-V2X) technology based on cellular networks. For V2X security, the use of certificates and signatures can effectively reduce the risks. However, certificates and signatures require additional communication resources. When sending a BSM, additional certificates and signatures will be appended to the back of the message, which reduces the available channel capacity and the maximum number of vehicles in this channel. In the special cases such as traffic congestion and bad communication environment, the maximum number of the channel may be lower than the total number of surrounding vehicles. At this time, V2X loses its effect and may cause traffic accidents.

Therefore, reducing the overhead of certificates and signatures can increase the available channel capacity. One solution is to reduce the size of certificates and signatures, but it will reduce the security of the communication. The physical layer authentication can effectively solve this problem. Physical layer authentication uses characteristics such as inherent attributes of communication devices or channel characteristics to identify different vehicles. These characteristics are difficult to be imitated by malicious attackers, effectively guaranteeing the security of V2X communication. At the same time, the use of physical layer authentication does not require additional security information, thus increasing the available capacity of the channel.

This paper focuses on V2X security. And we design a V2X physical layer authentication scheme for the problem of signatures occupying extra resources. Our main contributions are summarized as:

1) An authentication model based on physical layer characteristics is proposed. The physical layer characteristics that can be used for authentication include not only the unique characteristics of the communication devices, such as frequency offset and clock offset, but also the unique channel characteristics due to the high-speed movement of the vehicle. In addition, we also adopt the moving state of the vehicles. The moving state is continuous, and the BSM contains information such as position, speed, acceleration which can be confirmed by the sensors such as radar or camera. So moving state information can also assist in authentication.

2) Based on the Kalman filter, we have refined the iterative model and threshold model in the authentication model. The iterative model mainly realizes the priori and posteriori estimation of the current time based on the physical layer characteristics of the previous time, which provides the basis for the entire authentication process. The threshold model analyzes the mathematical characteristics of the priori estimation, and summarizes the calculation method of the authentication threshold.

3) Since the conventional Kalman filter can only be used for linear discrete system, we introduced extended Kalman filter and unscented Kalman filter to extend the physical characteristics to non-linearity. At the same time, iterative model and threshold model are improved according to the core ideas of these two algorithms.

4) In terms of security and performance, we compare the proposed schemes with the conventional V2X authentication scheme and physical layer authentication scheme. Then we use experiments to analyze the effect of the authentication scheme based on physical layer characteristics. In the experiments, we select three characteristics: RSSI, the distance between the two vehicles, and the relative speed between the two vehicles. We analyze the processes and effects of extended Kalman filter and unscented Kalman filter, the authentication process and its effects, and the factors that affect the threshold. It can be seen from the experiments that our proposed authentication scheme can effectively take the responsibility of identity authentication in the V2X environment, and have high security level and low overhead, which can reduce the consumption of communication resources by security.

The rest of this paper is organized as follows: Section II outlines the physical layer authentication scheme and the study of nonlinear Kalman filter. Section III introduces the model and process of V2X physical layer authentication. Section IV introduces the authentication schemes based on extended Kalman filter and unscented Kalman filter. Section V analyzes the effect of the authentication schemes based on physical layer characteristics and
the factors that affect the threshold through experiments. Section VI summarizes the paper and gives conclusions.

II. RELATED WORK
At present, the mainstream solution schemes of V2X security are based on PKI, which use certificates and signatures to provide security protection for BSMs. Vijayakumar et al. [9] use a computationally efficient two-way anonymous authentication scheme based on the anonymous certificates and signatures for vehicular ad-hoc networks (VANETs) to verify the message source and integrity. Balaji et al. [10] proposed an enhanced dual authentication and key management scheme for VANETs using the elliptic curve cryptography (ECC) and the Diffie-Hellman key exchange protocol. Physical-layer authentication identifies a device by its physical characteristics or the characteristics of the communication channel. The physical layer characteristics that can be used include carrier frequency offset, phase offset, clock offset and other radio “fingerprints” [11]–[14]. Hou uses CFO to implement the physical layer authentication under time-varying conditions [15], [16]. The channel characteristics depend on the state of the device and the surrounding environment, so the channel characteristics can also be used for authentication [17]. Xiao designed an authentication scheme using channel state information [18]. Choi [19] proposed a challenge-response physical-layer authentication scheme, which combined the key and channel state information for the authentication of legitimate users in orthogonal frequency division multiplexing (OFDM) systems. Wang et al. [20] used deep neural networks to authenticate CSI-based users. This authentication algorithm does not require deep analysis of channel changes. Threshold-based physical layer authentication usually adopts methods such as minimum likelihood [21], [22]. Its advantage is lower computational complexity and lower additional overhead. The physical layer authentication schemes based on machine learning has also been proposed to implement adaptive authentication [23], [24]. The vector machines algorithm [25], K-nearest neighbors [26], neural network [27], [28], etc. have been used for physical layer authentication. In addition, the physical layer watermark uses the information embedded in the original data signal to complete the authentication without additional information transmission [29]. The randomness of the channel can generate the key required for authentication [30], [31]. Due to the high-speed mobility of the vehicle, the channel changes quickly, so the authentication scheme based on channel characteristics is very suitable for V2X. The continuity of the vehicle’s moving states can also assist in authentication. Abdelaziz et al. [32] use the angle information of the vehicle and the GPS position information to authenticate the vehicle. Lim and Tuladhar [33] use radar information for authentication.

The Kalman filter is commonly used for data processing. It uses the characteristics of the linear system to recur the state equations to calculate the optimal solution under the minimum mean square error, thereby reducing the effect of noise in the system [34], [35]. Kalman filter is aiming at the linear system, so it needs to be improved when it encounters a nonlinear system. Generally, an approximate method is used to obtain the suboptimal solution [36]. The extended Kalman filter uses Taylor series expansion to convert nonlinear state equations and observation equations into linear equations. Generally, only first-order expansion is performed to reduce the computational complexity [37], [38]. Unscented Kalman filter uses a sampling method to approximate the probability density distribution of nonlinear equations [39], [40], and uses an unscented transformation method to reduce the number of sampling points [41]. With the development of information technology, Kalman filter can be used not only for signal processing, but also for vehicle state estimation [42], [43]. Therefore, we can use the characteristics of Kalman filter in the V2X environment to solve the problems of physical layer authentication.

III. MODELS
A. AUTHENTICATION MODEL
In security-related research, Alice, Bob, and Eve are commonly used to represent three different types of entities. Alice represents a legitimate sender, and Bob represents a legitimate receiver. In a V2X environment, they can be OBUs or RSUs. Alice periodically broadcasts BSMs or other safety-related information, which needs security-related processing to ensure the reliability and legitimacy. Eve represents a malicious attacker. It can be an illegal OBU, an illegal mobile device that supports V2X direct communication, or a pseudo base station. In the V2X environment, vehicles move at high speed, so the communication time between OBUs and RSUs is short, and the timeliness of messages is high. Traditional two-way authentication and encryption methods will seriously affect the efficiency of communication. Therefore, V2X direct communication uses broadcast to send BSMs, and does not use two-way authentication. The security-related information needs to be included in the BSMs. After receiving a BSM, receiver can directly authenticate the identity of the sender and judge the authenticity of the message. So there is no need to encrypt the BSMs. Eve can easily monitor the BSMs of the surrounding vehicles, so the BSMs need to be anonymized. Anonymous methods are beyond the scope of this paper. The security problems caused by Eve mainly include message forgery, message tampering, message replay, and imitation of legal identity. Because of the time stamp included in the BSM, the problem of message replay can be solved well. Other security issues can be summarized into two categories in the Alice-Bob-Eve model, shown in Figure 1.

One is that Eve uses a false identity to send a false BSM to Bob (that is Figure 1(a)), and the other is that Eve imitates

---

*Figure 1. Eve’s strategies for sending a false BSM.*
Alice to send BSMs (that is Figure 1(b)). Authenticating the identity of the sender is an effective way to solve these problems. When Eve uses a false identity, Bob can use identity authentication to filter out all the BSMs sent by Eve and keep only the BSMs sent by Alice, which effectively guarantees the safety of the vehicle. When Eve imitates Alice to send a forged or tampered BSM, Bob will check whether the BSM matches the corresponding hash value to determine whether the BSM is fake. In the V2X security system based on PKI, certificates and signatures are generally used for identity authentication during direct communication. The certificate ensures the legality of Alice’s identity, and the signature provides security protection for the BSMs sent by Alice. However, certificates and signatures consume additional bandwidth, thus reducing the available channel capacity.

Communication device has some unique characteristics, such as frequency offset, clock offset, etc. As the vehicle moves at high speed, the communication channel between Alice and Bob changes rapidly, and its characteristics are also unique. These characteristics are difficult to imitate by Eve, so they can be used for identity authentication. In addition, Alice’s moving state is continuous, and BSM contains information on the moving state such as position, speed, acceleration, etc. Bob’s radar, camera and other sensors can confirm Alice’s moving state. So, the moving state also can assist in identity authentication. We use $U_t$ to represent the set of $n$ physical layer characteristics at time $t$:

$$U_t = (u_t(1), u_t(2), u_t(3), \ldots, u_t(n))^T$$  \hspace{1cm} (1)

where $u_t^i$ represents the $i$-th characteristic, which can be physical layers characteristic such as carrier frequency offset (CFO), RSSI, channel state information (CSI), or moving-state information such as vehicle speed, direction angle, GPS and so on. Suppose that only one BSM is sent at each time, and Alice and Bob have completed authentication at time $t - 1$, so Bob can calculate the physical layer characteristic $U_t^P$ at time $t$ based on the information at the previous $t - 1$ times, and Bob can measure the physical layer characteristic $Z_t$ at time $t$. At time $t$, there are two cases. One is that the sender is Alice, that is, $H_0$ in (2). At this time, the absolute value of the difference between $U_t^P$ and $Z_t$ will be less than the threshold $T_t$. The other case is that the sender is Eve, that is, $H_1$ in (2), where the absolute value of the difference between $U_t^P$ and $Z_t$ will be greater than the threshold $T_t$. We can find that this authentication process is iterative. For the initial time $t_0$, Alice and Bob need to complete identity authentication by other means. Common method is using certificates and signatures. The threshold $T_t$ is related to the selected physical layer characteristics. As the characteristics change, the threshold $T_t$ also needs to be iterated and updated.

$$\begin{cases} H_0 : |Z_t - U_t^P| < T_t \\ H_1 : |Z_t - U_t^P| \geq T_t \end{cases}$$  \hspace{1cm} (2)

The proposed V2X physical layer authentication scheme is divided into three phases, and its flow chart is shown in Figure 2.

---

**B. ITERATIVE MODEL**

The iterative model is the important part of the authentication scheme. In this model, the physical layer characteristic $U_t^P$ at the current time needs to be calculated according to $U_{t-1}^P$.
at the previous time. And the model collects information preparing for updating the threshold $T_i$. The state transition of the physical layer characteristics at time $t$ can be expressed as (3)

$$U_t = f(U_{t-1}) + W_t$$  \hspace{1cm} (3)

where $W_t$ is process noise. Bob obtains the physical layer characteristics at time $t$ through his sensors and corresponding measurement methods, and the observation process is expressed as (4)

$$Z_t = h(U_t) + V_t$$  \hspace{1cm} (4)

where $V_t$ is the observation noise. For Bob, noise will seriously affect its observation result $Z_t$, so taking $Z_t$ as the optimal solution to participate in the next state transition will have a greater impact and lead to the failure of the entire authentication scheme.

The conventional Kalman filter is oriented to a linear discrete system, that is, we need to select linear physical layer characteristics, so the state equation and observation equation can be expressed as (5) and (6)

$$U_t = AU_{t-1} + W_t$$  \hspace{1cm} (5)

$$Z_t = HU_t + V_t$$  \hspace{1cm} (6)

where $A$ is the state transition matrix, $H$ represents the transition matrix from the current state to the observation, $W_t$ and $V_t$ represent the process noise and observation noise respectively, and $W_t \sim N(0, Q), V_t \sim N(0, R)$. The Kalman filter uses feedback to estimate the process state, which can be divided into two stages:

1) Time propagation: estimate the current state vector and error covariance according to the information at the previous time, and constitute a priori estimate, that is (7) and (8)

$$\tilde{U}_t = A\tilde{U}_{t-1}$$  \hspace{1cm} (7)

$$\tilde{P}_t = AP_{t-1}A^T + Q$$  \hspace{1cm} (8)

where $\tilde{U}_t$ represents the prior estimate of the physical layer characteristics at time $t$, and $\tilde{P}_t$ represents the covariance matrix of the priori estimate.

2) Observation update: combine the prior estimate and observation values to form the posterior estimates, that is (9) to (11)

$$\hat{U}_t = \tilde{U}_t + K_t(Z_t - H\tilde{U}_t)$$  \hspace{1cm} (9)

$$\hat{P}_t = (I - K_tH)\tilde{P}_t$$  \hspace{1cm} (10)

$$K_t = \tilde{P}_tH^T(H\tilde{P}_tH^T + R)^{-1}$$  \hspace{1cm} (11)

where $K_t$ is the Kalman gain, $\hat{U}_t$ is the posterior estimate of the physical layer characteristics, and $\hat{P}_t$ is the covariance matrix of the posterior estimate.

According to the process of Kalman filter, we choose $H\hat{U}_t$ as the prediction value for the physical layer characteristics at the current time, that is (12)

$$U_t^P = H\hat{U}_t$$  \hspace{1cm} (12)

### C. Threshold Model

The threshold model is the most important part of the judgment phase. In each iteration, the threshold needs to be updated based on the observation and the information in the previous iteration. This can effectively reduce the impact of noise on the threshold, thereby reducing the false alarm rate.

To calculate the threshold $T_i$, we first need to analyze the features of $Z_t - H\hat{U}_t^-$. According to (7), $\hat{U}_t^-$ represents the estimated physical layer characteristics at time $t$ based on the optimal result $\hat{U}_{t-1}$ at time $t - 1$ without process noise. Because observation value $Z_t$ is not considered, $\hat{U}_t^-$ is the priori estimate of the physical layer characteristics. Then we estimate the observation value $Z_t$ without observation noise, that is, $\hat{U}_t^-$ is brought into the (6), and the prior estimate of $Z_t$ is $H\hat{U}_t^-$. This complies with the description of the authentication process in Subsection III-A. We set the error of the prior estimate to $\epsilon_i$, that is (13)

$$e_i = U_t - \hat{U}_t^-$$  \hspace{1cm} (13)

and $E(e_i) = 0, E(e_i^T e_i^T) = \tilde{P}_t^-$. According to (6) and (13), we can get

$$e_i = Z_t - H\hat{U}_t^- = H\epsilon_i + V_t$$  \hspace{1cm} (14)

and $E(e_i) = 0, E(e_i^T e_i^T) = H\tilde{P}_t^-H^T + R$. So (2) can be rewritten as (15)

$$\begin{array}{l}
H_0 : |\epsilon_i| < T_i \\
H_1 : |\epsilon_i| \geq T_i
\end{array}$$  \hspace{1cm} (15)

We can see that $\epsilon_i$ is the superposition of two Gaussian distributions. Therefore, for the $i$-th element $\epsilon_i(i)$ in $\epsilon_i$, there is $\epsilon_i(i) \sim (0, D_t(i, i))$. $D_t(i, i)$ represents the value of the $i$-th row and $i$-th column of $D_t$, that is, the variance of $\epsilon_i(i)$. According to the features of the Gaussian distribution, the probability of successful authentication of the $i$-th element is (16)

$$P_A(i) = P[|\epsilon_i(i)| < T_t(i)]$$

where $P_A$ represents the set of all probabilities that the $i$-th element authenticates successfully. In order to facilitate the calculation of $T_t(i)$, the $Q$ function is used, that is (17)

$$T_t(i) = \sqrt{D_t(i, i)}Q^{-1}\left(1 - \frac{P_A(i)}{2}\right)$$  \hspace{1cm} (17)

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}} dt$ is the right-tail function of Gaussian distribution, $Q^{-1}(x)$ is the inverse function of $Q(x)$. It can be seen that $P_A(i)$ represents the probability of $|\epsilon_i(i)| < T_t(i)$, and we can set $P_A(i)$ in the initialization phase. It can be seen from (17) that $T_t(i)$ is related to the probability $P_A(i)$ and the variance $D_t(i, i)$. $P_A(i)$ is a preset value, which cannot affect the update of $T_t(i)$. $D_t(i, i)$ is related to Kalman filter and changes with the iterative process, so it can affect the update of $T_t(i)$.
IV. AUTHENTICATION SCHEMES BASED ON NONLINEAR KALMAN FILTER

In Section III we describe the authentication scheme and related models, and the most important iterative model is based on Kalman filter algorithm. However, the Kalman filter needs to select linear physical layer characteristics. Therefore, in practice, many nonlinear characteristics cannot be used for authentication. In this section, two kinds of nonlinear Kalman filter are used to extend the authentication scheme described in Section III, which are extended Kalman filter and unscented Kalman filter, respectively.

A. AUTHENTICATION SCHEMES BASED ON EXTENDED KALMAN FILTER

Extended Kalman filtering uses Taylor series expansion to approximate nonlinear state and observation equations into linear equations, which is a sub-optimal scheme. Since the solution of the second derivative is complicated, the extended Kalman filter generally expands the first-order Taylor series. Therefore, at the posterior estimate \( \hat{U}_{t-1} \), (3) can be expanded to (18)

\[
U_t = f(\hat{U}_{t-1}) + A_{t-1}(U_{t-1} - \hat{U}_{t-1}) + W_t
\]

where \( A_{t-1} \) represents the Jacobian matrix of \( f(U_{t-1}) \) at \( \hat{U}_{t-1} \), that is, \( A_{t-1} = \frac{af}{\partial U} |_{\hat{U}_{t-1}} \). Similarly, at the prior estimate \( \hat{U}_t^- \), (4) expands to (19)

\[
Z_t = h(\hat{U}_t^-) + H_t(U_t - \hat{U}_t^-) + V_t
\]

where \( H_t \) represents the Jacobian matrix of \( h(U_t) \) at \( \hat{U}_t^- \), that is, \( H_t = \frac{ah}{\partial U} |_{\hat{U}_t^-} \). The nonlinear state equations and observation equations are transformed into linear ones, and the subsequent prediction and update stages are the same as the conventional Kalman filter algorithm.

1) Time propagation: estimate the current state vector and error covariance according to the information at the previous time, and constitute a priori estimate, that is (20) and (21)

\[
\hat{U}_t^- = f(\hat{U}_{t-1})
\]

\[
\hat{P}_t^- = A_{t-1}\hat{P}_{t-1}A_{t-1}^T + Q
\]

where \( \hat{U}_t^- \) represents the priori estimate of the physical layer characteristics at time \( t \), and \( \hat{P}_t^- \) represents the covariance matrix of the priori estimate.

2) Observation update: combine the priori estimate and observation values to form the posterior estimates, that is (22) to (24)

\[
K_t = \hat{P}_t^-H_t^T(H_t\hat{P}_t^-H_t^T + R)^{-1}
\]

\[
\hat{U}_t = \hat{U}_t^- + K_t(Z_t - h(\hat{U}_t^-))
\]

\[
\hat{P}_t = (I - K_tH_t)\hat{P}_t^-
\]

Referring to the analysis in Subsection III-C, we choose \( h(\hat{U}_t^-) \) as the predicted value of the physical layer characteristics at the current time. Take (13) into (18), we can get

\[
\varepsilon_t = Z_t - h(\hat{U}_t^-) = H_t\varepsilon_t + V_t
\]

and \( E(\varepsilon_t) = 0, D_t = E(\varepsilon_t\varepsilon_t^T) = H_t\hat{P}_t^-H_t^T + R \). The calculation method of the threshold \( T_t \) and judgment conditions remain unchanged.

We summarize the process of V2X physical layer authentication scheme based on extended Kalman filter as follows:

1) In the initialization phase, the authentication is completed using certificates and signatures. The probability of successful authentication \( P_A \) is set, and the corresponding physical layer characteristic \( U_0 \) is recorded.

2) At time \( t \), \( A_t \) and \( H_t \) are calculated to form the state equation and the observation equation.

3) At time \( t \), the iterative process is completed according to (20)-(24).

4) At time \( t \), the threshold \( T_t \) is calculated according to (17) and (25).

5) At time \( t \), identity authentication is performed according to (15). The case is indicated that the authentication is successful, and continue to step 2 for the next iteration. The case is indicated that the authentication has failed, and return to step 1 to restart the entire authentication process.

B. AUTHENTICATION SCHEMES BASED ON UNSCENTED KALMAN FILTER

Extended Kalman filter approximates nonlinear equations to linear equations, but the corresponding Jacobian matrices need to be calculated in each iteration. For complex systems, the amount of calculation is high and the accuracy is low, resulting in a reduction in the filtering effect and incorrect authentication result. Unscented Kalman filter uses sampling to approximate the probability density distribution of nonlinear equations, so its accuracy is high.

First, in the initialization phase, we need to calculate the mean \( \hat{U}_0 \) and covariance \( \hat{P}_0 \) of the physical layer characteristics, that is (26) and (27)

\[
\hat{U}_0 = E[U_0]
\]

\[
\hat{P}_0 = E[(U_0 - \hat{U}_0)(U_0 - \hat{U}_0)^T]
\]

Based on the conventional Kalman filter, the unscented Kalman filter adds the stage of calculating Sigma points and weights. The iterative process is as follows:

1) Calculate Sigma points and weights: \( 2n + 1 \) Sigma sampling points are needed, that is (28) to (30)

\[
\chi_{t-1}^0 = \hat{U}_{t-1}
\]

\[
\chi_{t-1}^j = \hat{U}_{t-1} + \left(\sqrt{(n+\kappa)\hat{P}_{t-1}}\right)_j
\]

\[
\chi_{t-1}^n = \hat{U}_{t-1} - \left(\sqrt{(n+\kappa)\hat{P}_{t-1}}\right)_{j-n}
\]

where \( (\cdot)_j \) refers to the \( j \)-th column of the matrix, \( \kappa = \alpha^2(n+\lambda) - n \), and \( \alpha \) and \( \lambda \) are the scale parameters.
that determine how far the Sigma points distribution is within the range of the mean. The weight calculation method is (31) to (33)

\[ w_0^{(m)} = \frac{\kappa}{n + \kappa} \]
\[ w_0^{(c)} = \frac{\kappa}{n + \kappa} + (1 - \alpha^2 + \beta) \]
\[ w_j^{(m)} = w_j^{(c)} = \frac{1}{2(n + \kappa)} \quad j = 1, 2, \ldots, 2n \]  

And \( w_j^{(m)} \) is used to calculate the mean, and \( w_j^{(c)} \) is used to calculate the covariance. \( \beta \) is used to adjust the precision of the covariance. For Gaussian distribution \( \beta = 2 \) is optimal.

2) Time propagation: estimate the current state vector and error covariance according to the information at the previous time, and constitute a priori estimate, that is (34) to (40)

\[ x'_{t|t-1} = f(x'_{t-1|t-1}) \]  
\[ \hat{U}_t^- = \sum_{j=0}^{2n} w_j^{(m)} x'_{t|t-1} \]  
\[ \hat{P}_t^- = \sum_{j=0}^{2n} w_j^{(m)} [x'_{t|t-1} - \hat{U}_t^-] [x'_{t|t-1} - \hat{U}_t^-]^T + Q \]  
\[ y'_{t|t-1} = h(x'_{t|t-1}) \]  
\[ \tilde{Z}_t^- = \sum_{j=0}^{2n} w_j^{(m)} y'_{t|t-1} \]  
\[ M_t = \sum_{j=0}^{2n} w_j^{(c)} [x'_{t|t-1} - \hat{U}_t^-] [y'_{t|t-1} - \tilde{Z}_t^-]^T + R \]  
\[ N_t = \sum_{j=0}^{2n} w_j^{(c)} [x'_{t|t-1} - \hat{U}_t^-] [x'_{t|t-1} - \hat{U}_t^-]^T \]  

where \( x'_{t|t-1} \) represents the priori estimate of the Sigma points. \( \hat{U}_t^- \) is the mean value of the Sigma points and corresponds to the priori estimate of the physical layer characteristics at time \( t \), and \( \hat{P}_t^- \) represents the covariance matrix of the priori estimate. \( y'_{t|t-1} \) represents the observation estimate corresponding to the Sigma points, \( \tilde{Z}_t^- \) represents the priori estimate of the observation, and its covariance matrix is \( M_t \). \( N_t \) represents the covariance between the priori estimate and the observation value to calculate the Kalman gain.

3) Observation update: combine the priori estimate and observation values to form the posterior estimates, that is (41) to (43)

\[ K_t = N_t M_t^{-1} \]  
\[ \hat{U}_t = \hat{U}_t^- + K_t(Z_t - \tilde{Z}_t^-) \]  
\[ \hat{P}_t = \hat{P}_t^- - K_t M_t K_t^T \]

where \( K_t \) is the Kalman gain, \( \hat{U}_t \) is the posterior estimate of the physical layer characteristics, and \( \hat{P}_t \) is the covariance matrix of the posterior estimate.

According to the analysis of Subsection III-C, we choose \( \tilde{Z}_t^- \) as the predicted value of the physical layer characteristics at the current time, so \( \varepsilon_t \) is expressed as (44)

\[ \varepsilon_t = Z_t - \tilde{Z}_t^- \]

and \( E(\varepsilon_t) = 0, D_t = E(\varepsilon_t \varepsilon_t^T) = M_t \). The calculation method of the threshold \( T_t \) and judgment conditions remain unchanged.

We summarize the process of V2X physical layer authentication scheme based on extended Kalman filter as follows:

1) In the initialization phase, the authentication is completed using certificates and signatures. The probability of successful authentication \( P_A \) is set. The corresponding physical layer characteristic \( U_0 \) is recorded. And the initial mean \( \hat{U}_0 \) and covariance \( \hat{P}_0 \) are calculated.

2) At time \( t \), Sigma points and weights are calculated.

3) At time \( t \), the Sigma points are used to complete the iterative process of unscented Kalman filter, that is, (34)-(43).

4) At time \( t \), the threshold \( T_t \) is calculated according to (17) and (44).

5) At time \( t \), identity authentication is performed according to (15). The case \( H_0 \) indicates that the authentication is successful, and continue to step 2 for the next iteration. The case \( H_1 \) indicates that the authentication has failed, and return to step 1 to restart the entire authentication process.

C. COMPARISON AND ANALYSIS

At present, the mainstream schemes of V2X security are using certificates and signatures. Usually BSMs are sent every 100ms. To reduce the extra bandwidth overhead of certificates, SAE J2945/1 [44] stipulates that the BSMs with a certificate and a signature are transmitted approximately every 500 ms, and other BSMs are transmitted with a certificate digest (8 bytes) and a signature to reduce the overall message length. Physical layer authentication can replace signatures. So the above process will become that BSMs with a certificate and a signature are transmitted every 500 ms and BSMs with a digest are transmitted every 100 ms. The size of a BSM is small (that is 50-150 bytes) and its transmission frequency is high [45]. The size of a signature is 64 bytes, so it takes a lot of overhead. The physical layer authentication does not need to transmit any bytes, so it can reduce the overhead of security.

The conventional physical layer authentication scheme is based on the mean [20], which is given by (45)

\[ L_t \triangleq \|Z_t - \tilde{Z}_t\| \geq T_M \]  

where \( \|x\| \) is the Frobenius norm of the matrix \( x \) and \( \tilde{Z}_t \) is the mean of historical \( Z_t \). \( T_M \) is the threshold,
which is given by (46)

\[ T_M = Q^{-1}(P_f/2) \|V_t\| \]  

(46)

The mean-based scheme is mainly for static situation. It has poor performance for authentication when the vehicle is moving. For nonlinear characteristics, the mean value cannot be used to predict the characteristics of the next time. The proposed schemes based on nonlinear Kalman filter can adapt to time-varying physical layer characteristics. And it can also solve the problem that conventional Kalman filter can only be used in linear systems. We analyze the security and performance of these schemes through experiments in Section V.

V. EXPERIMENTAL RESULTS

In this section, we first compare our nonlinear-Kalman-filter-based physical layer authentication (NKF-based PLA) with the conventional certificate-and-signature-based authentication (CS-based authentication) and mean-based physical layer authentication (Mean-based PLA), in term of security and performance. Then we analyze two authentication schemes based on nonlinear Kalman filter through simulation. First, we select RSSI as the first physical layer characteristic, here using a lognormal distribution model [46], that is (47)

\[ P(d) = P(d_r) + 10y \log\left(\frac{d}{d_r}\right) + \sigma_{t}^{(\text{RSSI})} \]  

(47)

where \( P(d) \) refers to the RSSI at the distance \( d \) between the sender and receiver. \( d_r \) is the reference distance, \( \sigma_{t}^{(\text{RSSI})} \) conforms to zero-mean Gaussian distribution, and its variance is \( \sigma_{t}^{(\text{RSSI})^2} \). Therefore, the RSSI at time \( t \) is related to the distance between the two vehicles, that is (48)

\[ P_t^{(\text{RSSI})} = P(d_r) + 10y \log\left(\frac{d_t}{d_r}\right) + \sigma_{t}^{(\text{RSSI})} \]  

(48)

The vehicles moving scenario for simulation is shown in Figure 3. The moving states between Alice and Bob are that they are away from each other with a constant acceleration, the initial relative distance is 10 meters, the initial relative speed of them is 0, and the relative acceleration is 2m/s². Eve is in front of Alice to send false BSMs, 30 meters away from Bob, and relative acceleration is also 2m/s². The BSM transmission rate is 10Hz, that is, one BSM is broadcast every 100ms. Therefore, the moving states are expressed as (49) and (50)

\[ d_t = d_{t-1} + v_{t-1} \Delta t + a \Delta t^2 + \sigma_{t}^{(d)} \]  

(49)

\[ v_t = v_{t-1} + a \Delta t + \sigma_{t}^{(v)} \]  

(50)

where \( d_t \) represents the distance between at time \( t \), \( v_t \) represents the relative speed at time \( t \), and \( a \) represents the relative acceleration. \( \Delta t \) represents the interval between two BSMs, that is, 100ms. \( \sigma_{t}^{(d)} \) and \( \sigma_{t}^{(v)} \) represent the noise of state transition, both of which conform to zero-mean Gaussian distribution, and the variances are \( \sigma_{d_t}^2 \) and \( \sigma_{v_t}^2 \), respectively, because the acceleration has a small amplitude fluctuation. The state equation and observation equation can be expressed as (51) and (52)

\[
U_t = \begin{bmatrix}
P_t^{(\text{RSSI})} \\
v_t \\
\end{bmatrix} = \begin{bmatrix}
P(d_r) + 10y \log\left(\frac{d_{t-1} + v_{t-1} \Delta t + a \Delta t^2}{d_r}\right) \\
v_{t-1} + a \Delta t \\
\end{bmatrix} \\
+ \begin{bmatrix}
\sigma_{t}^{(\text{RSSI})} \\
\sigma_{t}^{(d)} \\
\sigma_{t}^{(v)} \\
\end{bmatrix}
\]  

(51)

\[
Z_t = U_t + V_t
\]  

(52)

where \( V_t \) represents observation noise and is in accordance with Gaussian distribution. According to (51) and (52), we simulate the moving states to generate RSSI, distance and speed data. Then we implement the NKF-based PLA and Mean-based PLA, and use this data to simulate the authentication process. These simulations are achieved through MATLAB. We set the simulation time to 30 seconds, which means 300 BSMs have been sent.

Figure 4 shows the overhead of certificates and signatures for CS-based authentication and physical layer authentication. According to IEEE 1609.2 [5], assuming that the ID of certificate is the maximum to support as many vehicles as possible, and other items are as small as possible. So the size of an explicit certificate is 239 bytes and the size of a signature is 64 bytes. We use the procedure described in IV-C to send BSMs periodically, and calculate the percentage of certificates and signatures. Figure 4(a) shows the percentage of certificates and signatures in a conventional V2X security scheme. We can see that due to the small size of the BSM, certificates and signatures occupy a lot of communication resources during the transmission of the BSM. So the security overhead of V2X is too large. Figure 4(b) shows the security overhead of the physical layer authentication. We can see that physical layer authentication can effectively reduce the overhead of signatures, thus improving the efficiency of communication.

Table 1 shows the comparison of four certification schemes: CS-based authentication, Mean-based physical layer authentication, extended-Kalman-filter-based physical layer authentication (EKF-based PLA) and unscented-Kalman-filter-based physical layer authentication (UUKF-based PLA). The accuracy in the table indicates the probability that the authentication scheme correctly identifies the sender. Overhead represents the additional cost of certificates.
and signatures. Security represents the security level of these schemes. Certificates and signatures can solve security problems, such as the forgery of communication content, deletion of communication content, malicious requests for communication resources and fake communication identities. And user privacy can be solved by anonymous certificates.

TABLE 1. Performance and Security for different authentication schemes.

| Scheme           | Accuracy | Overhead | Security |
|------------------|----------|----------|----------|
| CS-based PLA     | 100%     | High     | High     |
| Mean-based PLA   | 42.47%   | Low      | Low      |
| EKF-based PLA    | 83.87%   | Low      | High     |
| UKF-based PLA    | 83.40%   | Low      | High     |

FIGURE 4. The overhead of certificates and signatures for different authentication schemes.

FIGURE 5 shows the process of extended Kalman filter and unscented Kalman filter. The true values in the figure represent the results after extended Kalman filter and unscented Kalman filter. We can conclude that the two types of nonlinear Kalman filter can effectively reduce the impact of observation noise and guarantee the increasing or decreasing characteristics of the selected physical layer. Good filtering results ensure the stability of the authentication process and reduce the probability of errors.

Figure 6 shows the authentication process based on extended Kalman filter and unscented Kalman filter, that is, the changing process of $e_t$ and $T_t$ in (15). In the experiment, we set $V_t = [0.6, 1.0, 0.5]^T$ and $P_A = [0.95, 0.95, 0.95]^T$. The judgment condition for successful authentication is $|e_t(i)| < T_t(i)$, that is $-T_t(i) < e_t(i) < T_t(i)$. Therefore, we set the upper bound and the lower bound to be $T_t$ and $-T_t$, respectively. $e_t$ falling between the upper and lower bounds indicates successful authentication, and falling outside indicates failed authentication. It can be seen from the figure that in most cases, the authentication is successful, because the authentication success probability is set to 95%, that is, the probability is 95% that $e_t$ falls between $-T_t$ and $T_t$. $Q^{-1}(\frac{1-P_A(0)}{2})$ is an important factor that affects the threshold $T_t(i)$. This value is a constant, and the greater the value of $P_A(i)$, the greater this value, so the larger $T_t(i)$ is. When $P_A(i)$ is 95%, $Q^{-1}(\frac{1-P_A(0)}{2})$ is 1.96. According to (17), it can be seen from the figure that the value of $D_t(i, i)$ is close to the observation noise $V_t(i)$. This indicates that the observation noise has a greater influence on the threshold $T_t(i).$ Only when the authentication processes of $P_{\alpha}^{RSSI}$, $d_t$ and $v_t$ are all successful, can we think that the entire authentication process is successful, so it can effectively reduce the probability of errors. In addition, in actual use of the authentication scheme, the probability $P_A(i)$ can be set according to the selected physical layer characteristics to adjust the error rate of authentication. In short, the authentication scheme based on extended Kalman filter and unscented Kalman filter can effectively take the responsibility of identity authentication in the V2X environment.
VI. CONCLUSION
V2X security is an important guarantee for Internet of Vehicles. V2X faces a variety of security threats, and the use of authentication can effectively solve these security threats and improve the safety of vehicle driving. Many countries in the world have already carried out V2X security research and test verification based on PKI. For V2X security, the use of certificates and signatures can effectively reduce the risks faced by V2X communications. However, certificates and signatures require additional communication resources. In special cases such as traffic congestion and poor communication environment, the maximum number of vehicles in...
the channel may be lower than the number of surrounding vehicles, which may cause traffic accidents. Physical layer authentication uses physical characteristics such as inherent physical characteristics of devices or channel characteristics to identify different devices. These characteristics are difficult to be imitated by malicious attackers, effectively guaranteeing the security of V2X. At the same time, the physical layer authentication does not need to transmit additional security information, thus increasing the available channel capacity.

In this paper we propose an authentication model based on the physical layer characteristics. The model uses the characteristics of devices and the channel characteristics. In addition, we introduce the moving states of the vehicles into this model. Based on the Kalman filter, we refine the iterative model and threshold model in the authentication model. The iterative model mainly realizes the priori and posteriori estimation of the current time based on the physical layer characteristics of the previous time, which provides the basis for the entire authentication process. The threshold model analyzes the mathematical characteristics of the priori estimation, and gives the calculation method of the authentication threshold. In order to utilize the non-linear physical layer characteristics, we improve the iterative model and threshold model based on extended Kalman filter and unscanted Kalman filter. Finally, we compare our schemes with conventional schemes and use experiments to analyze the effects of authentication schemes which select three characteristics: RSSI, the distance between the two vehicles, and the relative speed between the two vehicles. The proved filters can ensure the stability of the authentication process and reduce the probability of errors. In addition, the authentication scheme based on extended Kalman filter and unscanted Kalman filter can effectively take the responsibility of identity authentication in the V2X environment, and have high security level and low overhead, which can reduce the consumption of communication resources by security.

REFERENCES

[1] A. Alnasser, H. Sun, and J. Jiang, “Cyber security challenges and solutions for V2X communications: A survey,” Comput. Netw., vol. 151, pp. 52–67, Mar. 2019.

[2] J. Wang, Y. Shao, Y. Ge, and R. Yu, “A survey of vehicle to everything (V2X) testing,” Sensors, vol. 19, no. 2, p. 334, Jan. 2019.

[3] A. Ghosal and M. Conti, “Security issues and challenges in V2X: A survey,” Comput. Netw., vol. 169, Mar. 2020, Art. no. 107093.

[4] C. Adams and S. Lloyd, Understanding PKI: Concepts, Standards, and Deployment Considerations. Reading, MA, USA: Addison-Wesley, 2003.

[5] IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, IEEE Standard 1609.2-2016, 2016.

[6] S. Li, Y. Liu, J. Wang, and Z. Sun, “SCMAC: A slotted-contention-based media access control protocol for cooperative safety in VANETs,” IEEE Internet Things J., vol. 7, no. 5, pp. 3812–3821, May 2020.

[7] S. Chen, J. Hu, Y. Shi, and L. Zhao, “LTE-V: A TD-LTE-based V2X solution for future vehicular network,” IEEE Internet Things J., vol. 3, no. 6, pp. 997–1005, Dec. 2016.

[8] R. Weber, J. Misener, and V. Park, “C-V2X-A communication technology for cooperative, connected and automated mobility,” in Proc. Mobile Commun.-Technol. Appl. 24. ITG-Symp., 2019, pp. 1–6.

[9] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balasamy, and P. G. Shynu, “Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks,” Future Gener. Comput. Syst., vol. 78, pp. 943–955, Jan. 2018.

[10] N. Alangudi Balaji, R. Sukumar, and M. Parvathy, “Enhanced dual authentication and key management scheme for data authentication in vehicular ad hoc network,” Comput. Electr. Eng., vol. 76, pp. 94–110, Jun. 2019.

[11] K. Zeng, K. Govindan, and P. Mohapatra, “Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks],” IEEE Wireless Commun., vol. 17, no. 5, pp. 56–62, Oct. 2010.

[12] B. Danee, H. Lueckeen, S. Capkun, and K. El Defrawy, “Attacks on physical-layer identification,” in Proc. 3rd ICM Conf. Wireless Netw., 2010, pp. 89–98.

[13] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in Proc. 14th ACM Int. Conf. Mobile Comput. Netw., 2008, pp. 116–127.

[14] O. Ureten and N. Serinken, “Wireless security through RF fingerprinting,” Can. J. Electr. Comput. Eng., vol. 32, no. 1, pp. 27–33, 2007.

[15] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, “Physical layer authentication for mobile systems with time-varying carrier frequency offsets,” IEEE Trans. Commun., vol. 62, no. 5, pp. 1658–1667, May 2014.

[16] W. Hou, X. Wang, and J.-Y. Chouinard, “Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates,” in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2012, pp. 3559–3563.

[17] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, “Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks],” IEEE Wireless Commun., vol. 17, no. 5, pp. 63–70, Oct. 2010.

[18] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication in time-variant channels,” IEEE Trans. Wireless Commun., vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[19] J. Choi, “A coding approach with key-channel randomization for physical-layer authentication,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 1, pp. 175–185, Jan. 2019.

[20] Q. Wang, H. Li, D. Zhao, Z. Chen, S. Ye, and J. Cai, “Deep neural networks for CSI-based authentication,” IEEE Access, vol. 7, pp. 123026–123034, 2019.

[21] Z. Gu, H. Chen, P. Xu, Y. Li, and B. Vucetic, “Physical layer authentication for non-coherent massive SIMO-enabled industrial IoT communications,” 2020, arXiv:2005.12688 [Online]. Available: http://arxiv.org/abs/2005.12688.

[22] H. Frossell, R. Thobaben, H. Al-Zubaidy, and J. Gross, “Physical layer authentication in mission-critical MTC networks: A security and delay performance analysis,” IEEE J. Sel. Areas Commun., vol. 37, no. 4, pp. 795–808, Apr. 2019.

[23] H. Fang, X. Wang, and L. Hanzo, “Learning-aided physical layer authentication as an intelligent process,” IEEE Trans. Commun., vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[24] X. Qiu, T. Jiang, S. Wu, and M. Hayes, “Physical layer authentication enhancement using a Gaussian mixture model,” IEEE Access, vol. 6, pp. 53583–53592, 2018.

[25] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang, and Y. Lu, “Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks,” IEEE Trans. Ind. Inform., early access, Jan. 15, 2020, doi: 10.1109/TII.2020.2963962.

[26] F. Pan, Z. Pang, H. Wen, M. Lavisott, M. Xiao, R.-F. Liao, and J. Chen, “Threshold-free physical layer authentication based on machine learning for industrial wireless CPS,” IEEE Trans. Ind. Inform., vol. 15, no. 12, pp. 6481–6491, Dec. 2019.

[27] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, and M. Cao, “Deep-Learning-Based physical layer authentication for industrial wireless sensor networks,” Sensors, vol. 19, no. 11, p. 2440, May 2019.

[28] X. Qiu, J. Dai, and M. Hayes, “A learning approach for physical layer authentication using a adaptive neural network,” IEEE Access, vol. 8, pp. 26139–26149, 2020.

[29] N. Goergen, W. S. Lin, K. J. R. Liu, and T. C. Clancy, “Extrinsic channel-performance analysis,” in Proc. 14th ACM Int. Conf. Mobile Comput. Netw., 2008, pp. 116–127.

[30] http://arxiv.org/abs/2005.12686

[31] J. Choi, “Physical layer authentication for non-coherent massive SIMO-enabled industrial IoT communications,” 2020, arXiv:2005.12688 [Online]. Available: http://arxiv.org/abs/2005.12688.

[32] H. Frossell, R. Thobaben, H. Al-Zubaidy, and J. Gross, “Physical layer authentication in mission-critical MTC networks: A security and delay performance analysis,” IEEE J. Sel. Areas Commun., vol. 37, no. 4, pp. 795–808, Apr. 2019.

[33] H. Fang, X. Wang, and L. Hanzo, “Learning-aided physical layer authentication as an intelligent process,” IEEE Trans. Commun., vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

[34] X. Qiu, T. Jiang, S. Wu, and M. Hayes, “Physical layer authentication enhancement using a Gaussian mixture model,” IEEE Access, vol. 6, pp. 53583–53592, 2018.
[31] X. Du, D. Shan, K. Zeng, and L. Huie, “Physical layer challenge-response authentication in wireless networks with relay,” in Proc. INFOCOM IEEE Conf. Comput. Commun., Apr. 2014, pp. 1276–1284.

[32] A. Abdelaziz, C. E. Koksal, R. Burton, F. Barickman, J. Martin, J. Weston, and K. Woodruff, “Beyond PKI: Enhanced authentication in vehicular networks via MIMO,” in Proc. IEEE 19th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC), Jun. 2018, pp. 1–5.

[33] K. Lim and K. M. Talukdar, “LIDAR: Lidar information based dynamic V2V authentication for roadside infrastructure-less vehicular networks,” in Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2019, pp. 1–6.

[34] Y. Zhaosheng and Z. Zhong, “A real-time traffic vol. prediction, model based on the Kalman filtering theory,” China J. Highway Transp., vol. 12, no. 3, pp. 63–67, 1999.

[35] S. Thrun, W. Burgard, and D. Fox, Probabilistic Robotics, vol. 1. Cambridge, MA, USA: MIT Press 2000.

[36] K. Ito and K. Xiong, “Gaussian filters for nonlinear filtering problems,” IEEE Trans. Autom. Control, vol. 45, no. 5, pp. 910–927, May 2000.

[37] S. J. Julier and J. K. Uhlmann, “New extension of the Kalman filter to nonlinear systems,” Proc. SPIE, vol. 3068, pp. 182–193, Jul. 1997.

[38] S. S. Kia, J. Hechtbauer, D. Gogokhiya, and S. Martinez, “Server-assisted distributed cooperative localization over unreliable communication links,” IEEE Trans. Robot., vol. 34, no. 5, pp. 1392–1399, Oct. 2018.

[39] Z. Gao, Y. Liu, C. Yang, and X. Chen, “Unscented Kalman filter for continuous-time nonlinear fractional-order systems with process and measurement noises,” Asian J. Control, pp. 1–12, 2019. [Online]. Available: https://doi.org/10.1002/asjc.2077

[40] T. Knudsen and J. Leth, “A new continuous discrete unscented Kalman filter,” IEEE Trans. Autom. Control, vol. 64, no. 5, pp. 2198–2205, May 2019.

[41] H. Zhou, Z. Liu, and X. Yang, “Motor torque fault diagnosis for four wheel independent motor-drive vehicle based on unscented Kalman filter,” IEEE Trans. Veh. Technol., vol. 67, no. 3, pp. 1969–1976, Mar. 2018.

[42] R. K. Jaiswal and C. D. Jaidhar, “Location prediction algorithm for a nonlinear vehicular movement in VANET using extended Kalman filter,” Wireless Netw., vol. 23, no. 7, pp. 2021–2036, Oct. 2017.

[43] S. Antonov, A. Fehn, and A. Kugi, “Unscented Kalman filter for vehicle state estimation,” Vehicle Syst. Dyn., vol. 49, no. 9, pp. 1497–1520, Sep. 2011.

[44] On-Board System Requirements for V2V Safety Communications, SAE Standard J2945/1, 2016.

[45] J. B. Kenney, “Dedicated short-range communications (DSRC) standards in the united states,” Proc. IEEE, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[46] L. Cheng, B. Henty, D. Stancil, F. Bai, and P. Mudalige, “Mobile Vehicle-to-Vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band,” IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1501–1516, Oct. 2007.

JIAN WANG received the B.Sc., M.Sc., and Ph.D. degrees in computer science from Jilin University, China, in 2004, 2007, and 2011, respectively. He is currently a Professor with Jilin University. He has published over 40 articles on international journals. His research interests include wireless communication and vehicular networks, especially for network security and privacy protection.

YAMENG SHAO received the M.E. degree from the College of Software Engineering, Jilin University, in 2016, and the M.S. degree (Hons.) in electronics from the Queen’s University of Belfast, U.K., in 2018. She is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Jilin University. Her main research interest includes MEC supports for vehicular networks.

YANCONG WANG received the B.E. degree in the Internet of Things from Jilin University, China, in 2016, and the M.S. degree (Hons.) in electronic from the College of Computer Science and Technology, Jilin University. Her main research interest includes vehicular networks.

YUMING GE received the Ph.D. degree from the Institute of Computing Technology, Chinese Academy, in 2014. He is currently a Senior Engineer with the China Academy of Information and Communications Technology. His research interest includes vehicular networks.

RUNDONG YU received the M.S. degree in electrical and computer engineering from the Worcester Polytechnic Institute, in 2015. He is currently an Engineer with the China Academy of Information and Communications Technology. His research interest includes vehicular networks.