Research Article

Proactive Flexible Interval Intermittent Jamming for WAVE-Based Vehicular Networks

Hao Li,1 Xiaoshuang Xing,2 Anqi Bi,2 and Jin Qian3

1School of Engineering and Applied Science, The George Washington University, Washington, DC 20052, USA
2Department of Computer Science and Engineering, Changshu Institute of Technology, Changshu, Jiangsu, China
3College of Computer Science and Technology, Taizhou University, Taizhou, Jiangsu, China

Correspondence should be addressed to Anqi Bi; anqi_b@cslg.edu.cn

Received 14 April 2021; Accepted 1 August 2021; Published 15 August 2021

Academic Editor: Yan Huang

Copyright © 2021 Hao Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we deal with the eavesdropping issue in Wireless Access in Vehicular Environments- (WAVE-) based vehicular networks. A proactive flexible interval intermittent jamming (FIJ) approach is proposed which predicts the time length $T$ of the physical layer packet to be transmitted by the legitimate user and designs flexible jamming interval (JI) and jamming-free interval (JF) based on the predicted $T$. Our design prevents eavesdroppers from overhearing the information with low energy cost since the jamming signal is transmitted only within JI. Numerical analysis and simulation study validate the performance of our proactive FIJ, in terms of jamming energy cost and overhearing defense, by comparing with the existing intermittent jamming (IJ) and FIJ.

1. Introduction

A WAVE- (Wireless Access in Vehicular Environments-) based vehicular network has been considered a promising way to improve safety and driving experience with vehicular level information exchange playing the most critical role. However, wireless communication is vulnerable to eavesdropping threats due to its broadcasting nature. The information exchanged among vehicles, including vehicle identities, locations, and speeds, is exposed to eavesdropping attackers. To protect this private information from leakage, reliable eavesdropping defense mechanisms must be designed.

Friendly jamming is an effective approach to defend against eavesdropping [1–5]. Continuous jamming (CJ), which requires the friendly jammer to keep sending jamming signals during the whole transmission of the legitimate transmitter, has been extensively studied in literature. Eavesdroppers are disabled via CJ in the cost of large energy consumption. In recent work [6], the authors argued that it is unnecessary to jam the whole transmission. Partially jamming the transmission of a data packet is capable of preventing eavesdroppers from getting sensitive information. Therefore, they proposed an intermittent jamming (IJ) scheme where the friendly jammer sends the jamming signal only in the jamming interval (JI) and keeps silent in the jamming-free interval (JF). This scheme can keep the information safe with low energy cost. However, the length of JI and JF was fixed in their design (as shown in Figure 1) without considering the length of the packet transmitted by the legitimate transmitter. This fixed design has drawbacks in the following aspects. When the length of the transmitted packet is short, unnecessary energy will be consumed during a long JI. On the other hand, a combination of JI and JF will occur repeatedly for a long packet. The jammer should switch between JI and JF frequently, and energy will be wasted due to the switching loss. Therefore, the length of the transmitted packet should be considered when designing the length of JI and JF to achieve better energy efficiency.
In this paper, we try to design a flexible interval JI (FIJ) scheme by setting the length of JI and JF according to the time length of the transmitted packet. For a specific physical packet with time length $T$, we will find the time duration within which the core information is transmitted and set this duration as JI. As for $T$, its actual value cannot be obtained before the physical packet is generated. However, if the jammer obtains the value of $T$ after the packet has been generated and decides the length of JI and JF accordingly, nonnegligible time delay will be introduced before starting the jamming process. This way, the jamming signal may not be able to be transmitted synchronously with the physical packet leading to degraded jamming performance. To deal with this problem, this paper will predict the value of $T$ and proactive FIJ will be enabled to achieve better jamming performance. As a summary, the contributions of this paper are as follows.

(i) The physical packet structure in WAVE-based vehicular networks is analyzed. For a specific physical packet with time length $T$, the time length of the “Application Data,” which is generated in the application layer and contains the core information to be transmitted, is obtained.

(ii) An FIJ scheme is proposed where the length of JI depends on the value of $T$ such that the friendly jammer disables the eavesdropper with less energy cost.

(iii) Support vector regression (SVR) is applied to learn the characteristics of the time length of $N$ historical physical packets and predict the time length of the future physical packet. Proactive FIJ is enabled by designing the length of JI according to the predicted time length of the next physical packet.

The paper is organized as follows. Section 2 discusses the related works. The considered system model is illustrated, and the problem is formulated in Section 3. The FIJ scheme is designed in Section 4, and the value of $T$ is predicted based on SVR in Section 5. Performance investigation is conducted in Section 6. Finally, the paper is concluded in Section 7.

2. Related Works

From the application layer to the link layer, the security threat has long been under concern [7–11]. The multimedia streaming scheme proposed in [12] deals with the security issues in the application layer. Authentication schemes are designed to ensure the confidentiality of communication in the transport layer [13–15]. The secured routing protocol proposed in [16, 17] provides a safe transmission in the network layer. [18] detects possible denial of service ahead of confirmation time in the link layer.

According to the IEEE 802.11p standard, driving-related information, including identity, location, speed, and direction, is transmitted through vehicle to vehicle (V2V) communication and vehicle to infrastructure (V2I) communication. This sensitive information is transmitted on the air and is exposed to eavesdropping attack in the physical layer due to the natural characteristics of wireless communication. By eavesdropping this information, a malicious user may track the driving information and analyze the driving route of legitimate users [19]. Therefore, it is necessary to tackle the eavesdropping attack in the physical layer for secure sensitive information transmission.

Friendly jamming has been widely applied to defend against eavesdropping attacks. It can help to improve the security of vehicle localization [20], location verification [21], and secure communication [22]. In most existing friendly jamming schemes, friendly jammers keep sending jamming signals. These schemes are known as CJ which consumes a large amount of energy. In order to reduce power consumption, [23] proposes temporary jamming to provide information security when encryption is limited. A later research [6] advances an IJ scheme where the friendly jammer sends the jamming signal only in the JI and keeps silent in the JF. The IJ scheme greatly decreases the power consumption while providing information security via achieving a high package error rate (PER) at the eavesdropper. However, this scheme fixes the length of JI and JF without considering the length of the packet transmitted by the legitimate transmitter. For a short physical packet, unnecessary energy will be consumed during a long JI. On the other hand, a combination of JI and JF will occur repeatedly for a long packet. Energy will be wasted during the frequent change between JI and JF. In order to further reduce the energy cost of the IJ scheme, this paper will design flexible JI and JF depending on the length $T$ of the transmitted packet.

In order to predict the time length $T$ of the physical packet to be transmitted in the next time, machine learning will be applied. Typical machine learning algorithms include linear regression, logistic regression, ridge regression, and...
support vector regression [24–29]. Linear regression [24] uses least square methods as cost function and optimizes the target model by Newton iteration. However, linear regression may obtain local optimum solution for some applications. Logistic regression [25] is based on the probabilistic mechanism, which determines parameters by maximum likelihood estimation. However, logistic regression is a linear model in essence and may not be suitable for the vibrating samples. By adding an additional degree of deviation to the regression estimate, ridge regression can effectively reduce the variance [27]. Nevertheless, this model requires samples involved to be multidimensional. In our work, the time length of the historically transmitted physical packets will be taken as the samples. They are one-dimensional vibrating samples. Therefore, neither logistic regression nor ridge regression fits our application. On the other hand, support vector regression (SVR) [28] maps samples into the high-dimensional feature space by nonlinear change. Thus, the performance of SVR is independent of the physical packet to be transmitted.

N

Therefore, we will utilize the SVR model to learn the characteristics of the time length of N historical physical packets and predict the time length of the physical packet to be transmitted.

3. Problem Formulation

We are under a general vehicle communication scenario in a vehicular network under the WAVE protocol. As shown in Figure 2, the legitimate user U_A is sending its driving information to U_B. Meanwhile, there is an eavesdropper U_T trying to overhear the packets being sent. A cooperative jammer U_J located near U_A is sending jamming signals with power P_J to degrade the packets received by eavesdropper U_T.

For a physical packet with time length T, U_J sends jamming signals in the JI with length T_J and keeps silence in the JF with length T_F. Here, T_J ≤ T, T_F ≤ T, and T_J + T_F = T. Let W_J indicate the energy cost of the cooperative jammer, B_J indicate the bit error rate (BER) of U_E during JI, B_E indicate the BER of U_E during JF, and B_E indicate U_E’s average BER within T. It can be derived that

\[ W_J = T_J \cdot P_J, \]

\[ B_E = \frac{T_J}{T} \cdot B_J + \frac{T_F}{T} \cdot B_E. \]

The closed-form expressions of the BERs for different modulation schemes have been given in [30]. It can be found that BER is always a decreasing function of the signal to noise plus interference ratio (SNIR), denoted by γ. During JF, no jamming signal is transmitted by the jammer. Therefore, \( γ^J_B = \frac{E_b}{N_0} \) when calculating B_E. Here, E_b is the received signal energy per bit and N_0 is the power spectral density of the noise. On the other hand, the receiving performance of U_E is degraded by the jammer during JI. Therefore, \( γ^I_B = \frac{E_b}{(N_0 + \phi_J)} \) when calculating B_J. Here, \( \phi_J = P_J/|h_{JE}|^2 \) is the received jamming signal power spectral density with |h_{JE}|^2 indicating the channel gain from U_J to U_E and B being the channel bandwidth. Obviously, \( γ^I_B \leq γ^J_B \) and \( B_J \geq B_E \). Therefore, B_E is an increasing function of T_J. According to (1), it can be found that W_J is also an increasing function of T_J. Recall that we want to disable the eavesdropping of U_E with low energy cost; we need to decide a proper T_J that can ensure a high enough BER at U_E while achieving a W_J as low as possible.

4. Design of Flexible Interval IJ Scheme

In order to obtain a high enough B_E while maintaining a low W_J, the jammer should transmit jamming signals only during the transmission time of the most significant part of the physical packet. Figure 3 shows the component of a physical packet. Intuitively, the “Application Data,” which is generated in the application layer, contains the core information to be transmitted by U_A to U_E. Therefore, “Application Data” is the most significant part of the physical packet. If the jammer can identify the time duration within which the “Application Data” is transmitted and sends jamming signals only during this time, U_E’s eavesdropping will be disabled and U_E’s energy cost will be reduced. Therefore, the main challenge to be solved in our design is to identify the time duration within which the “Application Data” is transmitted.

According to [31], a physical packet is consisting of a 16 µs PLCP preamble, a 4 µs Signal Field, and a variable-length Data Field. The Data Field is constructed by 16 bits of the PLCP Header, the WSPM-T-Header, the WSPM-N-Header, the LLC Header, the MAC Header, 32-bit FCS, 6-bit tail, and variable-length Application Data. Moreover, n bits pad bits are also added in the Data Field to make the length of the Data Field divisible by N_{DBPS}. Therefore, n takes a value between 0 and N_{DBPS} – 1. The value of N_{DBPS} depends on the modulation schemes and the coding rates. Typical values of N_{DBPS} in WAVE-based vehicular networks are listed in Table 1.

When the Data Field is constructed, it will be divided into symbols. Each symbol consists of N_{DBPS} bits and is 4 µs long in time. According to [6], the minimum length of the WSPM-T-Header, the WSPM-N-Header, the LLC Header, and the MAC Header is 2 bytes, 2 bytes, 2 bytes, and 24 bytes, respectively. There are a total of 30 bytes, which are 240 bits, in the physical packet before the Application Data in the Data Field. In the time domain, the time length of these 240 bits will be T_s = 240/N_{DBPS} × 4 µs. As mentioned before, there are 6-bit tail, 32-bit FCS, and 0 to N_{DBPS} – 1 bits pad bits after the Application Data. These are totally 38 to 37 + N_{DBPS} bits,
Then, we have packet is BPSK modulated with the coding rate being $1/2$. According to the value of $T$, the value of $NDBPS$ can be saved when in the aforementioned example, while most energy can been generated. To solve this problem, we learn the characteristics of the time length of $T$ after the physical packet has been transmitted with the FCS modulated (that is, the FCS, the tail bits, and the pad bits are transmitted after the Application Data). Therefore, the time length after transmitting the Application Data, and the pad bits are transmitted after the Application Data. Then, for a physical packet of length $T$, the flexible interval $IJ$ scheme will be designed as shown in Figure 4. According to the value of $NDBPS$ given in Table 1, the value of $T_2$ can be easily obtained. For example, $T_2 = 60 \mu s$ and $6.3 \mu s \leq T_2 \leq 10.17 \mu s$ when the physical packet is BPSK modulated with the coding rate being $1/2$.

The PLCP preamble, the Signal Field, and the headers are transmitted before the Application Data. The time length before transmitting the Application Data in the physical packet, which is denoted by $T_1$, can be calculated as $T_1 = 16 \mu s + 4 \mu s + t_i$. On the other hand, the FCS, the tail bits, and the pad bits are transmitted after the Application Data. Therefore, the time length after transmitting the Application Data in the physical packet, which is denoted by $T_2$, can be calculated as $T_2 = t_2$. Then, for a physical packet of length $T$, the flexible interval $IJ$ scheme will be designed as shown in Figure 4. According to the value of $NDBPS$ given in Table 1, the value of $T_1$, $T_2$ can be easily obtained. For example, $T_1 = 60 \mu s$ and $6.3 \mu s \leq T_1 \leq 10.17 \mu s$ when the physical packet is BPSK modulated with the coding rate being $1/2$.

Theoretical, the best anti-raisdropping performance can be achieved when $T_2$ takes the lower bound value, which is $T_2 = 6.3 \mu s$ in the aforementioned example, while most energy can be saved when $T_2$ takes the upper bound value, that is, $T_2 = 10.17 \mu s$ in the example.

### 5. Predicting the Time Length of the Physical Packet Based on SVR

This section is aimed at obtaining the time length $T$ of the physical packet to be transmitted. As discussed in Section 1, the jamming performance will be degraded if the jammer tries to obtain the value of $T$ after the physical packet has been generated. To solve this problem, we learn the characteristics of the time length of $N$ historical physical packets and predict the time length of the physical packet to be transmitted (that is, the $(N+1)$-th physical packet) via machine learning. Then, proactive FJ will be enabled by designing the length of $IJ$ and $JF$ according to the predicted result, and the jamming signal will be able to be transmitted synchronously with the physical packet to ensure the jamming performance.

Let $\{(x_1, t_1), (x_2, t_2), \ldots, (x_N, t_N)\}$ denote $N$ historical records, called as samples, regarding the time length of the physical packets. Here, $x_i = i, 1 \leq i \leq N$, is the index of the physical packet that has been transmitted with the $x_N$-th physical packet being the most recently transmitted one. $t_i$ is the time length in $\mu s$ of the $x_i$-th physical packet. Then, we utilize the SVR model [28] to learn the characteristics of the time length of $N$ historical physical packets by finding the hyperplane that fits the $N$ samples. To simplify the calculation, we first scale the time length values of the samples. Let $y_i$ denote the scaled value of $t_i$, then

$$y_i = 10 \times \frac{t_i}{t_{\text{max}}},$$

with $t_{\text{max}} = \max\{t_1, t_2, \ldots, t_N\}$. The scaled value $y_i$ will be distributed within $[0, 10]$. SVR define the function of the fitting hyperplane as

$$f(x) = w^T x + b. \quad (4)$$

Here, $x = (x_1, x_2, \ldots, x_N)^T$, $w = (w_1, w_2, \ldots, w_N)^T$, and $b = (b_1, b_2, \ldots, b_N)^T$. The SVR model is aimed at minimizing the maximum margin between $y = (y_1, y_2, \ldots, y_N)^T$ and $f(x)$. According to [32], the target function of the SVR model can be defined as

$$\min \frac{1}{2} \|w\|^2 + C \sum_{i=1}^{N} (\xi_i + \xi_i^*) \quad (5)$$

subject to

$$y_i - (w^T x_i + b) \leq \epsilon + \xi_i, \quad i = 1, 2, \ldots, N$$

$$y_i \leq \epsilon + \xi_i^*, \quad i = 1, 2, \ldots, N$$

$$\xi_i \geq 0, \xi_i^* \geq 0, \quad i = 1, 2, \ldots, N.$$

![Figure 3: Physical packet structure.](image-url)
Here, \( C > 0 \) is the constant regularization parameter and \( \xi \) and \( \xi^* \) are slack variables whose values are close to 0. Slack variables are introduced according to soft margin loss theory to cope with infeasible constraints of the optimization problem. The Lagrangian function of (5) is given in

\[
L(w, b, \alpha, \eta) = \frac{1}{2} \|w\|^2 + C \sum_{i=1}^{N} (\xi_i + \xi_i^*) \\
+ \sum_{i=1}^{N} \alpha_i (w^T x_i + b - y_i - \varepsilon_i - \xi_i) \\
- \sum_{i=1}^{N} \alpha_i^* (w^T x_i + b - y_i - \varepsilon_i - \xi_i^*) \\
- \sum_{i=1}^{N} (\eta_i \xi_i + \eta_i^* \xi_i^*).
\]

Here, \( L \) is the Lagrangian and \( \eta, \eta^*, \alpha, \alpha^* \) are Lagrange multipliers (also referred to as dual variables) that should satisfy positivity constraints, i.e., \( \alpha_i \geq 0, \alpha_i^* \geq 0, \eta_i \geq 0, \) and \( \eta_i^* \geq 0 \).

In this condition, the target function of the SVR model can be transferred to its dual problem. By optimizing the dual variables in Lagrangian function, the original target function (5) would be solved as well. Specifically, according to the SVR framework and Karush-Kuhn-Tucker (KKT) conditions, we optimize the minimum of the partial derivatives of \( L \) with respect to the variables \( (w, b, \xi, \xi^*) \), namely,

\[
\frac{\partial L}{\partial w} = 0 \rightarrow w = \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) x_i, \tag{8}
\]

\[
\frac{\partial L}{\partial b} = 0 \rightarrow \sum_{i=1}^{N} (\alpha_i - \alpha_i^*) = 0, \tag{9}
\]

\[
\frac{\partial L}{\partial \xi_i} = 0 \rightarrow C - \alpha_i - \eta_i = 0, \tag{10}
\]

\[
\frac{\partial L}{\partial \xi_i^*} = 0 \rightarrow C - \alpha_i^* - \eta_i^* = 0. \tag{11}
\]

Substituting (8), (9), (10), and (11) into (7), the dual optimization problem can be yielded, and the problem converts to minimizing the objective function as follows:

\[
\min_{\alpha, \alpha^*, \eta, \eta^*} \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} (\alpha_i - \alpha_i^*)(\alpha_j - \alpha_j^*)(x_i^T x_j) \\
+ \sum_{i=1}^{N} y_i(\alpha_i - \alpha_i^*) + \varepsilon(\alpha_i + \alpha_i^*). \tag{12}
\]

Obviously, (12) is the dual form of the target function and a typical quadratic programming problem. The problem could be easily solved by several mathematical frameworks, such as SMO, and obtained the corresponding \( \alpha, \alpha^* \). In the involved experiments, we directly apply the toolkit in MATLAB. Then, the hyperplane function (4) becomes

\[
f(x) = w^T x + b = \sum_{i=1}^{N} \alpha_i y_i x_i^T x + b. \tag{13}
\]

The SVR model usually takes linear function, polynomial function, Radial Basis Function (RBF), or sigmoid function as kernel function. In our work, considering that \( t_i \) is one-dimensional and vibrates greatly, smooth kernel function is applicable. Besides, [33] has proved that RBF with proper \( \delta \) could smoothly fit any curve compared with other kinds of kernel functions. Accordingly, we choose RBF given in (14) as kernel function when training the SVR model [33]:

\[
K(x_i, x) = \exp \left(-\frac{\|x_i - x\|^2}{2\delta^2}\right). \tag{14}
\]

That is, \( x_i^T x \) in (13) should be replaced by \( K(x_i, x) \) as shown in (14).

After getting the hyperplane function given in (13), we can predict the time length \( T \) of the \( x_{t+1} \)th physical packet by substituting \( x = N + 1 \) into (13) and conducting the reverse conversion of (3). That is, \( T = f(N + 1) * t_{max}/10. \)

6. Numerical Analysis and Simulation Study

In this section, we first investigate the performance of FIJ for securing the transmission of physical packets with a known time length. Then, SVR is applied to find the hyperplane that fits the samples of 500 historically transmitted physical packets and predict the time length of the physical packet to be transmitted. Proactive FIJ is conducted based on the prediction result, and the performance is studied.

6.1. Performance Investigation of FIJ for Securing the Transmission of Physical Packets with Known \( T \) 

This subsection compares the performance of the FIJ scheme with the IJ scheme proposed in [6]. Besides, the performance of our design when \( T_P^2 \) takes the lower bound value (referred to as FIJ-shortest TF in the following) and the upper bound value (referred to as FIJ-longest TF in the following) is also investigated. The simulation is performed in MATLAB 2018b using the WLAN toolbox. We use function “wlanNonHTConfig” to generate non-HT packets transmitted in the WAVE-based vehicular network. The channel bandwidth is set to be 10 MHz, and we are using the default sampling rate for
10 MHz. We set the delay profile as “Urban NLOS” because most of the V2V communication happens in an urban area and does not have a line of sight. BPSK modulation is used, and the coding rate $r$ is set to be 1/2 and 3/4.

The performance comparison is conducted from two aspects. To validate the antieavesdropping performance of our design, the packet error rate (PER) of $U_{E}$, which is the ratio of the number of physical packets not successfully decoded by $U_{E}$ to the number of the physical packets sent by the transmitter $U_{A}$, is adopted. The function “V2VPERSimulator” from MATLAB is utilized to simulate the PER. The energy cost for sending jamming signals referred to as the jamming energy cost in the following is used to investigate the energy efficiency of our design.

According to [6], the optimal transmission power of $U_{J}$ is set to be $P_{J} = 760$ mW for BPSK modulation with coding rate $r$ being 1/2. The corresponding $T_{J}$ and $T_{F}$ are 47.12 $\mu$s and 28.88 $\mu$s, respectively, in the IJ scheme. While for BPSK modulation with $r = 3/4$, the IJ scheme is set as $P_{J} = 760$ mW, $T_{J} = 37.2$ $\mu$s, and $T_{F} = 22.8$ $\mu$s. The setting of the IJ scheme is fixed regardless of the length of the transmitted physical packet. On the other hand, the length of $T_{J}$ and $T_{F} = T_{F}^{1} + T_{F}^{2}$ in our design is flexible which can be calculated as given

\[
\begin{align*}
T_{J} &= 12 + 12 + 9 \mu s \\
T_{F} &= 12 + 12 + 9 + 9 \mu s
\end{align*}
\]
in Section 4. $U_f$’s transmission power in our flexible interval IJ scheme is set to be the same as that in the IJ scheme, which is $P_f = 760$ mW.

We change the length of the PSDU from 38 octets to 438 octets resulting in the time length of the physical packets changing from $76 \mu s$ to $608 \mu s$ for BPSK modulation with $r = 1/2$ and from $60 \mu s$ to $412 \mu s$ for BPSK modulation with $r = 3/4$. The PER of $U_f$ is shown in Figure 5. It can be found that $U_f$’s PER increases with the increasing of the PSDU length for schemes other than FIJ-shortest TF. With the increase of the PSDU length, more information bits are enclosed in a physical packet. The probability of information bits within a physical packet being incorrectly decoded will increase resulting in an increased PER. For the FIJ-shortest TF scheme, $U_f$’s SNR keeps low since $U_f$ sends jamming signals during the whole transmission time of the “Application Data.” Therefore, $U_f$’s PER is always close to 100% regardless of the PSDU length. Small performance fluctuations occur for the FIJ-longest TF scheme. In the FIJ-longest TF scheme, the length of $T_f$ is fixed to be $(37 + ND_{DBPS})/ND_{DBPS} \times 4 \mu s$ by assuming that there are always $ND_{DBPS} - 1$ pad bits in the physical packet. However, the length of the pad bits varies with the PSDU length leading to insufficient jamming of the “Application Data” for some PSDU length and thus performance fluctuations on $U_f$’s PER. Moreover, one can see that a higher coding rate $r$ causes a higher PER. A higher $r$ implies more information bits, and less redundant bits are enclosed in a physical packet, which means that more information is transmitted in a physical packet and the transmission efficiency is improved. However, the redundant bits play an important role in error correction, and less redundant bits can decrease $U_f$’s error correction capability and lead to a higher PER.

The results regarding the jamming energy cost are given in Figure 6. We found that our FIJ scheme consumes less energy when the physical packet is short (for example, when the PSDU is 100 bytes long). While for long physical packets, the IJ scheme performs better in terms of energy cost. This is because the length of $T_f$ and $T_i$ are fixed in IJ. In other words, $T_f / T_i$ is fixed for any PSDU length (i.e., any physical packet length). In the flexible interval IJ scheme, the length of $T_f = T_i^1 + T_i^2$ is fixed, while the length of $T_f = T - T_i$ increases with the length of the physical packet. Therefore, $T_f / T$ increases with the increasing of the PSDU length leading to more jamming energy cost compared with the IJ scheme proposed in [6].

In order to further improve the jamming energy cost of the flexible interval IJ scheme, we conduct enhanced-FIJ in our simulation study. The enhanced-FIJ is designed by taking the same $T_i^1$ and $T_i^2$ as that of the FIJ scheme. While for the “Application Data” transmitted within $T_p$, the IJ scheme proposed in [6] is applied. That is, $T_i$ is further divided into sub-jamming intervals and subjamming-free intervals according to the IJ scheme proposed in [6]. The performance of enhanced FIJ-shortest TF and enhanced FIJ-longest TF is shown by green dashed lines and black solid lines in Figures 5 and 6. We found that enhanced FIJ-shortest TF can achieve PER performance almost the same as the IJ scheme while saving 10% energy.

6.2. Performance Investigation of Proactive FIJ. In this subsection, we first generate 600 samples $(x_i, t_i)$ with $x_i = i$, $1 \leq i \leq 600$. $68 \mu s \leq t_i \leq 3140 \mu s$ is generated as follows. (1) Generate a random number following a lognormal distribution with the mean $\mu$ being 2 and the standard deviation $\sigma$ being 0.5. (2) The generated random number first times 785 then is rounded down to a multiple of 4 to match the pattern of the time length of physical packets. (3) If the result is not within the section of proper time length (68 $\mu s$-3140 $\mu s$), repeat the process until the result falls into the section. (4) Repeat the process until the value of $t_1, t_2, \ldots, t_{600}$ is generated. Then, we train the SVR model with the scaled first 500 samples, that is, $(1, y_1), (2, y_2), \ldots, (500, y_{500})$, to find the hyperplane that fits these 500 samples.

Taking the RBF kernel function into consideration, two parameters need to be set in the SVR model, namely, regularization parameter $C$ and Gaussian kernel parameter $\delta$. We use the grid search technique to find the optimal values. Specifically, the optimal range of regularization parameter $C$ is $\{10^{-3}, 10^{-2}, 10^{-1}, 1, 5, 10, 10^2, 10^3\}$, and the range of

![Figure 7](image_url)
δ is \{10^{-3}, 10^{-2}, 10^{-1}, 1,10,10^2, 10^3\}. In our training experiment, we set the constant regularization parameter \(C = 5\), the slack variables \(\xi, \xi^*\) close to 0, and \(\delta\) in the Gaussian kernel equal to 100. The training result is shown in Figure 7. Based on the trained SVR model, we predict the value of \(f(501)\) then design the length of JI, denoted by \(T^501\), according to Section 4 with \(T = T^501 = \max\{f(501) \ast t_m/10\} \ast T\). Sequentially, we train the SVR model with samples \((2, y_2), (3, y_3), \cdots, (501, y_{501})\) and predict the value of \(f(502)\); train the SVR model with samples \((3, y_3), (4, y_4), \cdots, (502, y_{502})\) and predict the value of \(f(503)\); \cdots; and train the SVR model with samples \((60, y_{60}), (61, y_{61}), \cdots, (559, y_{559})\) and predict the value of \(f(560)\). Then, we will get \(T^502, T^503, \cdots, T^560\). After that, we transmit 500 packets for each time length \(t_k, 501 \leqslant k \leqslant 560\), and jam their transmission according to the obtained \(T^k_j\) to observe the PER. The results are given in Figure 8. It can be found that proactive FIJ based on SVR can lead to similar PER compared with the FIJ scheme derived from known time length. Taking an average of the results for \(T = t_{501}\) to \(T = t_{560}\), the average PER by using proactive FIJ is 96.59%. It is 0.77% less than the average PER achieved by using FIJ with known time length. Proactive FIJ based on SVR can effectively secure the transmission of the physical packets in WAVE-based vehicular networks.

7. Conclusion
In conclusion, FIJ provides a way to save more energy than existing JJ when dealing with eavesdropping attacks in WAVE-based vehicular networks. Proactive FIJ leads to no processing delay for deciding the length of JJ and JF thanks to its capability of predicting T. Simulation results confirm that our design is capable of defending eavesdropping attacks while enhancing the performance in energy saving.

Data Availability
No publicly archived dataset has been applied.

Disclosure
Part of the content is included in a conference paper entitled “Flexible Interval Intermittent Jamming against Eavesdropping in WAVE Based Vehicular Networks,” which has been accepted by the 9th International Conference on Computational Data and Social Networks (CSoNet 2020). Compared with the conference version, this manuscript enables proactive FIJ by predicting the time length of physical packets based on SVR. Organization and presentation have been improved, and evaluation has been conducted to validate the performance of proactive FIJ. This work is part of the first author Hao Li’s Ph.D. dissertation entitled “Enhancing Physical Layer Security in Wireless Communications Using Secrecy Extraction and Friendly Jamming.”

Conflicts of Interest
The authors declare that they have no conflicts of interest.

Authors’ Contributions
Hao Li and Xiaoshuang Xing contributed equally to this study and share first authorship.

Acknowledgments
This work was supported by the Youth Program of National Natural Science Foundation of China (grant numbers 61802274 and 61602062) and Natural science fund for colleges and universities in Jiangsu Province (grant number 18KJB510044).

References