JammingBird: Jamming-Resilient Communications for Vehicular Ad Hoc Networks

Hossein Pirayesh, Pedram Kheirkhah Sangdeh, Shichen Zhang, Qiben Yan, and Huacheng Zeng
Department of Computer Science and Engineering, Michigan State University
Email: {pirayesh,sangdeh,sczhang,qyan,hzeng}@msu.edu

***Abstract*—Current data-driven intelligent transportation systems are mainly reliant on IEEE 802.11p to collect and exchange information. Despite promising performance of IEEE 802.11p in providing low-latency communications, it is still vulnerable to jamming attacks due to the lack of a PHY-layer countermeasure technique in practice. In this paper, we propose JammingBird, a novel receiver design that tolerates strong constant jamming attacks. The enablers of JammingBird are two MIMO-based techniques: Jamming-resistant synchronizer and jamming suppressor. Collectively, these two new modules are able to detect, synchronize, and recover desired signals under jamming attacks, regardless of the PHY-layer technology employed by the jammers. We have implemented JammingBird on a vehicular testbed and conducted extensive experiments to evaluate its performance in three common vehicular scenarios: Parking lots (0∼15 mph), local traffic areas (25∼45 mph), and highways (60∼70 mph). In our experiments, while the jamming attacks degrade the throughput of conventional 802.11p-based receivers by 86.7%, JammingBird maintains 83.0% of the throughput on average. Experimental results also show that JammingBird tolerates the jamming signals with 25 dB stronger power than the desired signals.**

***Index Terms*—Jamming attacks, VANET, vehicular communications, experiment, jamming-resilient receiver**

I. Introduction

The efficiency of transportation systems is not merely about building better highways anymore; it is about intelligence. An intelligent transportation system (ITS) is a data-driven infrastructure that significantly contributes in improving public safety [1], economy [2], environmental ecosystems [3] of developed societies. To realize such a data-centric ITS, vehicular ad hoc networks (VANETs) are the primary mean of collecting data. VANETs offer efficient vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications for safety and non-safety data exchange [4]. IEEE 802.11p is the pervasive technology that provides low-latency wireless communications for VANETs. IEEE 802.11p amends IEEE 802.11 standard to meet the requirements of ITS applications in 5.9 GHz frequency band. Compared to legacy Wi-Fi, it uses 10 MHz bandwidth for better mobility management and enjoys higher maximum transmit power [5]. It can also establish communications with out-of-network users with wildcard BSSID for broadcasting time-intensive data, such as crashes and traffic congestion messages.

Despite all the amendments to meet the timing and throughput needs of ITS applications, IEEE 802.11p has remained almost defenseless for a decade when it confronts jamming attacks. In fact, even a simple constant jamming attack can be regarded as a big security threat for VANETs [6]. Causing denial of service at network users, such a jamming attack ages safety-related information and finally makes it outdated [7]. Thus, it is of great importance to reinforcing VANETs against jamming attacks [8]. In response to this urgent need, we have proposed JammingBird, as shown in Fig. 1. JammingBird rectifies the vulnerabilities of IEEE 802.11p at the PHY layer and effectively subverts strong constant jamming attacks. JammingBird can recover desired signals which are drowned into powerful jamming signals, a task that cannot be accomplished by conventional 802.11p-based receivers.

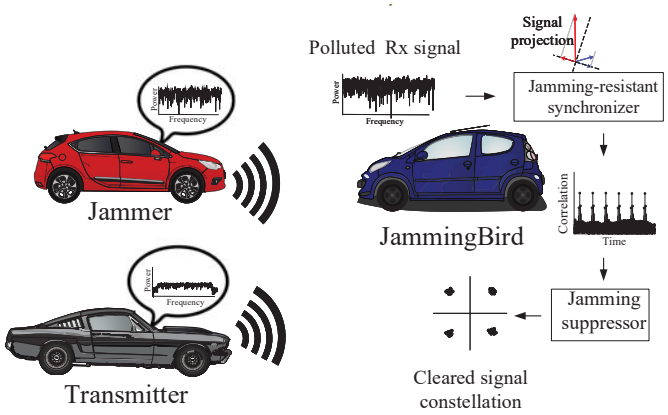
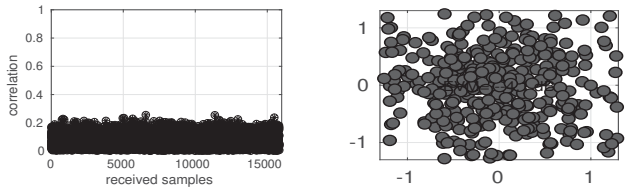


Fig. 1: JammingBird recovers packets buried in strong jamming signals with the aid of two modules. Jamming-resistant synchronizer identifies and synchronizes legitimate jammed packets. Jamming suppressor removes the jamming signal and recovers the desired packets.

A. Vulnerability of IEEE 802.11p to Jamming Attacks

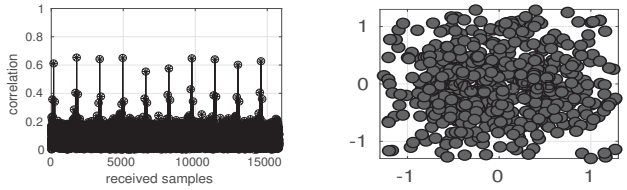
We have conducted a preliminary experiment on a conventional 802.11p-based receiver to show how vulnerable it is when facing jamming attacks. We have implemented the legitimate transmitter, conventional receiver, and jammer using USRP devices and laptops. First, we have considered a harsh test environment where all users moved on a highway in the same direction at 60∼70 mph. The legitimate users were 150 ft apart, and the jammer was located in between. The jammer was sending a noise-like signal to interrupt legitimate transmissions. In our experiments, an average of

978-1-6654-4108-7/21/$31.00



(a) Synchronization (b) Decoded signal

Fig. 2: Performance of conventional 802.11p-based receiver at a highway when JSR=20 dB.



(a) Synchronization (b) Decoded signal

Fig. 3: Performance of conventional 802.11p-based receiver at a parking lot when JSR=0 dB.

20 dB jamming to signal ratio (JSR) was observed at the receiver side. Fig. 2 shows the hardship of 802.11p-based receiver in decoding its desired signals. As shown in Fig. 2(a), it fails in coarse time synchronization. The receiver cannot notice the existence of desired packets. Even if the receiver is forced to proceed with the highest correlation peak (the most probable starting sample for a legitimate packet) over a long time window, the decoded signal will be erroneous as shown in Fig. 2(b). The signal is not recovered as it is highly polluted by the jamming signal.

We have repeated our experiments in a benign test environment, where all the nodes were static in an open parking lot. Jammer and the legitimate transmitter were located 100 ft away from the receiver. The observed JSR was about 0 dB. Fig. 3 show the performance of 802.11p-based receiver. Despite a marginal improvement in synchronization, the receiver was still unable to decode the desired signal. Clearly, the constant jamming attack completely brought down the 802.11p-based communication. One may think this issue can be easily treated by adjusting transmit power on the legitimate transmitter. However, high transmit power levels unnecessarily densify the networks, exacerbate undesirable events like broadcast storms, and beget large backoff windows across the legitimate users.

B. Proposed Receiver Design: JammingBird

We propose JammingBird, a new wireless receiver design to recover desired data packets in the presence of constant jamming attacks. As shown in Fig. 1, JammingBird takes advantage of recent advances in MIMO technology to mitigate unknown jamming signals and decodes the data packets. It addresses the underlying challenges of 802.11p-based receivers in encountering jamming attacks: packet detection, synchronization, and data recovery. Specifically, JammingBird reinforces 802.11p receivers with two novel modules.

JammingBird approaches the packet detection and synchronization problems with *jamming-resistant synchronizer*. This module comprises spatial projection filters to alleviate jamming signals by destructively combining those signals over different antennas. The spatial projection averts the jamming effect, making JammingBird able to notice the existence of a legitimate packet and find its starting sample. The legitimate, yet polluted, packets will be passed to *jamming suppressor* module. This module leverages the IEEE 802.11p frame structure and offers a blind jamming mitigation technique. It does not need the channel state information (CSI) between the jammer and receiver. Instead, it uses the short training field (STF) in the legitimate frames to calculate the jamming CSI ratio and recovers the desired packets. Collectively, these two modules lay the foundation of JammingBird.

We have implemented JammingBird on a proof-of-the-concept vehicular wireless testbed and evaluated its performance on three common scenarios in VANETs: parking lots ($0\sim15$ mph), local traffic areas ($25\sim45$ mph), and highways ($60\sim70$ mph). For these cases, JammingBird respectively reaches 26.2 Mbps, 22.2 Mbps, and 19.5 Mbps. In our experiments overall cases, while the jammer degrades the throughput of regular 802.11p-based receivers by 86.7%, JammingBird maintains 83.0% of throughput when facing jamming signals. The experimental result proves the efficacy of JammingBird in mitigating unknown and strong constant jamming attacks.

II. System Model

We suit JammingBird for a V2X communication link between a single-antenna transmitter and a two-antenna receiver, as shown in Fig. 1. The transmitter and receiver can be either an onboard unit on a vehicle or a roadside unit connected to the backbone infrastructure. Although it is a miniature networking scenario, it is the most common V2X case, given the simplicity of both onboard and roadside units in typical VANETs. The V2X communications are established using OFDM modulation specified in IEEE 802.11p PHY. Let us assume that $\mathrm{X}[l,k] \in \mathcal{CN}(0,1)$ is the legitimate message transmitted over the lth OFDM symbol and the kth subcarrier. A single-antenna jammer disrupts the V2X communications by constantly sending powerful arbitrary signals. Let us consider that the legitimate message $\mathrm{X}[l,k]$ is obscured with $\mathrm{X}_j[l,k] \in \mathbb{C}$ from the jammer. Please note that it does not mean the jammer uses OFDM modulation. Instead, $\mathrm{X}_j[l,k]$ translates the effect of jamming signal in frequency domain.

We assume block fading channel within a packet. This is a mild assumption in VANETs, given the very short length of packets. We denote the channel gain between the ith antenna of receiver and the legitimate transmitter by $\mathrm{H}_i[k] \in \mathbb{C}$ over kth subcarrier. We also denote channel gain between ith antenna of receiver and the jammer by $\mathrm{H}_{j,i}[k] \in \mathbb{C}$ over kth subcarrier. Therefore, on the lth OFDM symbol and the kth subcarrier, the received signal by legitimate receiver can be expressed as:

$$\mathbf{Y}[l,k] = \mathbf{H}[k]\mathrm{X}[l,k] + \mathbf{H}_j[k]\mathrm{X}_j[l,k] + \mathbf{Z}[l,k], \qquad (1)$$

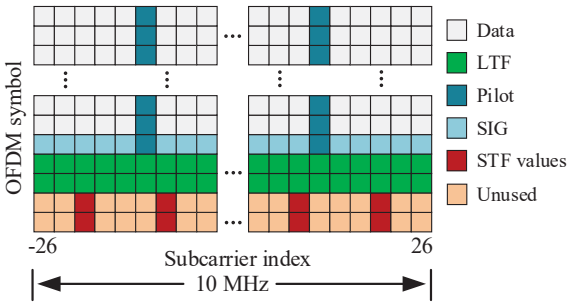


Fig. 4: IEEE 802.11p frame format for V2X communications.

where $\mathbf{Y}[l,k] = [\mathrm{Y}_1[l,k], \mathrm{Y}_2[l,k]]^{\mathrm{T}} \in \mathbb{C}^{2\times 1}$ denotes the received signal on both antennas. $\mathbf{H}[k] \triangleq [\mathrm{H}_1[k],\ \mathrm{H}_2[k]]^{\mathrm{T}} \in \mathbb{C}^{2\times 1}$ is the compound channel between the receiver and legitimate transmitter, and $\mathbf{H}_j[k] \triangleq [\mathrm{H}_{j,1}[k],\ \mathrm{H}_{j,2}[k]]^{\mathrm{T}} \in \mathbb{C}^{2\times 1}$ is the compound channel between receiver and the jammer. $\mathbf{Z}[l,k]$ stands for AWGN noise.

The jammer can arbitrarily choose its signal type. For instance, jammer can leverage noise-like, LTE-like, or CDMA-like signals to interfere the legitimate transmissions over the entire bandwidth of interest. V2X communications, on the other hand, leverage IEEE 802.11p frame format. Fig. 4 depicts the frame format used by V2X communications over 10 MHz at 5.9 GHz band. The frame comprises 64 subcarriers, including 12 null subcarriers and 52 valid subcarriers to carry data and pilot signal samples. The frame consists of a preamble field, signal field (SIG), and data field. While preamble and signal fields are of fixed length, the length of data field depends on the payload size. The preamble field is mainly used for packet detection, time and frequency synchronizations, and channel estimation. It consists of two identical short training field (STF) OFDM symbols and two identical long training field (LTF) OFDM symbols. In the frequency domain, each STF symbol only uses 12 subcarriers, as shown in Fig. 4. LTF symbols use a sequence of $+1$ and -1 values and populate all 52 valid subcarriers. The SIG field carries the modulation and coding scheme index and also determines the length of the frame. The data is mapped into 48 subcarriers, and the remaining four subcarriers are assigned to pre-known pilot signals for phase offset correction at the receiver.

III. Problem Description

In order to study the vulnerability of the 802.11p-based receiver, we briefly describe the main steps followed by the conventional receiver for recovering its desired signals in a non-hostile environment. As shown in Fig. 5, 802.11p-based receiver resembles the legacy Wi-Fi's receiver.

When a signal is received and sampled at the receiver, it first determines the existence of legitimate packets within the stored signal. Upon confirmation, it leverages correlation-based synchronization modules for correcting time and frequency offsets. The valid and corrected portion of the received signal is then converted into the frequency domain by the OFDM demodulation. The receiver employs LTF symbols in the preamble to estimate the channel at each subcarrier. The channel estimation takes place once for the entire frame. Then, the channel equalization subverts the effect of the estimated channel and recovers modulated symbols. Lastly, the phase offset is corrected using the pilot samples embedded into the frame as phase references. Now, the critical question is how a simple jamming attack can bring down the entire signal reception and recovery mechanisms.

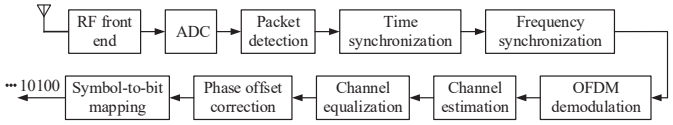


Fig. 5: Conventional 802.11p-based receiver for V2X communications.

A. Achilles heels of 802.11p-based receiver

Despite its subtle design, the 802.11p-based receiver experiences a hard time when it encounters jammers. In fact, the jammers impact multiple Achilles heels of the 802.11p-based receiver.

Physical Carrier Sensing: At both transmitter and receiver sides, the medium access of IEEE 802.11p is based on physical carrier sensing in part. At a time instance, the channel status is detected as occupied if a considerable energy level is detected over the spectrum. Under such a circumstance, the receiver actively looks for legitimate packets, and a potential transmitter postpones its transmission. As such, a jamming attack not only ages the information at the transmitters, it keeps the receivers unnecessarily active and inflicts a computational burden to them.

Packet Detection: The receiver uses auto-correlation of the received time-domain STF signal to detect the presence of a legitimate packet. Given the limited length of STF signal and possible dominance of jamming signals, auto-correlation result could be too ambiguous and full of spurious spikes. Consequently, the false alarm rate in packet detection tends to be drastically high.

Synchronization: Let us assume the receiver detects the presence of a legitimate packet by any means, such as a visible and sudden change in energy of received signal. Finding the start of the frame, which is buried in jamming signal, is a tedious task. Furthermore, the frequency synchronization is prone to large errors, and itself may cause additional frequency offset.

Channel Equalization: To avert the distortions from wireless medium, the channel gains should be estimated first. This is a challenging task under jamming attacks, as the packets' preambles are highly polluted by jamming signals. Also, the channel of jamming signal cannot be estimated in general, as the jammer can use any signals for jamming purposes.

These weak spots make the conventional 802.11p-based receiver vulnerable to jamming attacks. As shown by our preliminary experiments, the receiver may fail to decode signals when exposed to hostile environments.

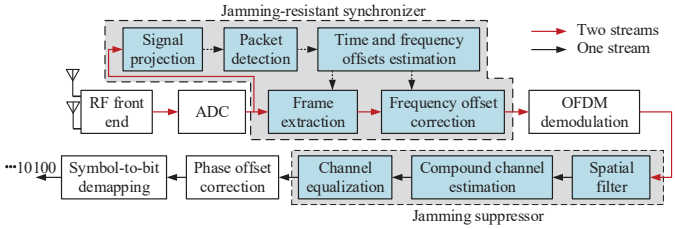


Fig. 6: The structure of JammingBird with its new modules.

B. Design Objectives and Challenges

JammingBird is designed as a treatment to Achilles heels of 802.11p-based receiver. JammingBird needs to address the shortcomings of the 802.11p-based receiver in packet detection, synchronization, and channel equalization.

First, JammingBird should be able to detect the presence of legitimate packets which are likely drowned into strong and unknown jamming signals. Second, if the existence of legitimate signals is confirmed, it must detect start of packets at sample level and correct frequency offset. These tasks are cumbersome due to the dominance of jamming signal, finite length of preamble, and offset injection from the jammer. The limited length of the preamble prevents correlation-based synchronization to bare clear correlation spikes as expected in asymptomatic cases (even under strong jamming attacks). Also, it is quite possible that frequency offset traces from jammer mislead the synchronization module in compensating the frequency offset between legitimate transmitter and the receiver.

When legitimate portion of the signal is detected, and offsets are compensated, JammingBird should suppress the jamming signal, equalize the channels, and recover the desired packets. This is another challenging task. It is not possible to acquire the channel gains between the jammer and receiver as the jammer is not bounded to any specific communication technology. Hence, its power level, frame format, and waveform are arbitrary. Also, due to the strong and uncontrolled power emitted by the jammer, the estimation of channels between legitimate users is very challenging, if not impossible.

IV. JammingBird: A Jamming-Resilient Receiver

JammingBird bears high-power and unknown constant jamming attacks. It is blessed with two new modules as shown in Fig. 6, namely *jamming-resistant synchronizer* and *jamming suppressor*. Jamming-resistant synchronizer enables the receiver to detect the packets and successfully perform time and frequency synchronizations in the presence of a jamming attack. Once the start of a legitimate packet is identified, and the offsets are compensated, the polluted signal will be translated into the frequency domain and passed to the jamming suppressor. The jamming suppressor first removes the effect of jamming signals from the received signal with the aid of a spatial filter. The cleared signal is then used for channel estimation and equalization. These two brand new modules effectively subvert the jamming signals, enabling JammingBird to survive under strong jamming attacks. In the following, each new module is presented in detail.

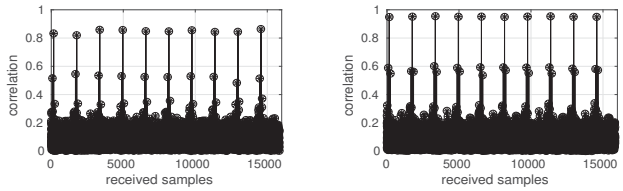
A. Jamming-Resistant Synchronizer

The jamming-resistant synchronizer identifies and extracts the portion of received time-domain signals containing legitimate IEEE 802.11p packets. Thereafter, the frequency offset between the legitimate transmitter-receiver pair is compensated. The synchronizer module leverages a spatial filter to determine the existence and beginning of packets in the presence of jamming attacks. The design of this filter is not contingent on channel knowledge and can be accomplished blindly. The filter alleviates the impact of jamming signals, allowing us to apply conventional correlation-based packet detection and synchronization techniques.

To compute the filter, we perform an eigenvalue decomposition (EVD) on the received signals from both antennas. Let us denote $\mathbf{y} \in \mathbb{C}^{2\times N_s}$ as the received time-domain signals on both receiving antennas and denote N_s as the number of collected samples on each antenna. Auto-correlation of the received samples is $\mathbf{R}_{\text{yy}} = \mathbb{E}\{\mathbf{y}\mathbf{y}^{\text{H}}\}$, where the symbols $[\cdot]^{\text{H}}$ and $\mathbb{E}\{\cdot\}$ represent the conjugate transpose and expectation operators, respectively. EVD of the $\mathbf{R}_{\text{yy}}$ can be expressed as $[\mathbf{Q}, \Lambda, \mathbf{Q}^{-1}] = \text{EVD}(\mathbf{R}_{\text{yy}})$, where Λ is the diagonal matrix comprising the eigenvalues of $\mathbf{R}_{\text{yy}}$ on its diameter. The columns of $\mathbf{Q} \in \mathbb{C}^{2\times 2}$ are the eigenvectors of $\mathbf{R}_{\text{yy}}$.

The signaling space can be completely spanned by columns of $\mathbf{Q}$ as its two bases. We decompose the signaling space into two complementary subspaces, each spanned by a column vector in $\mathbf{Q}$. Assume that the desired signal subspace is spanned by $\mathbf{Q}_s \in \mathbb{C}^{2\times 1}$, and the jamming subspace is spanned by $\mathbf{Q}_j \in \mathbb{C}^{2\times 1}$, and $\mathbf{Q} = [\mathbf{Q}_s, \mathbf{Q}_j]$. Then, we apply the signal subspace basis as the projection filter over the received signal by letting $\mathbf{y}_p = \mathbf{Q}_s^{\text{H}}\mathbf{y}$. To find the basis of desired signal subspace, we examine both available bases and look up the cross-correlation results in synchronization. If visible spikes are witnessed, the vector that achieves a higher correlation peak will be selected as the spatial projection filter. At the same time, the emergence of correlation spikes reveals the existence of legitimate packets. Once a legitimate packet is detected, the projected signal onto desired signal subspace will be subjected to conventional time synchronization. The extracted signal is used for computing the carrier frequency offset as $\theta = 1/64 \cdot \angle(\sum_{n=M}^{n=M+64} y_p[n] y_p[n+64]^{\text{H}})$, where $\angle(\cdot)$ is the angle of a complex number, and M is the position of the first LTF sample, and $\mathbf{y}_p[n]$ is the nth column of $\mathbf{y}_p$. The frequency offset is then compensated by multiplying $e^{-j\theta n}$ to synchronized signal.

To illustrate the effectiveness of jamming-resistance synchronizer, we have repeated the experiment conducted in Section I-A under the same networking scenario and communication environment. This time, we have leveraged a jamming-resistant synchronizer. Fig. 7 shows the performance of our proposed synchronizer. Comparing Fig. 7(a) with Fig. 2(a), it is evident that the jamming-resistant synchronizer is able to successfully detect and synchronize legitimate packets in



(a) Synchronization result (b) Synchronization result

Fig. 7: Jamming-resistant synchronizer at: (a) highway with JSR=20 dB and (b) parking lot with JSR=0 dB.

a very hostile environment, where the transmissions undergo strong jamming attacks on a highway. The conventional receiver, however, fails to do so. Comparing Fig. 7(b) with Fig. 3(a), it can bee seen that our proposed synchronizer outperforms conventional 802.11p-based receiver in finding and synchronizing packet at a parking lot where JSR equals to 0 dB.

Albeit successful in synchronization and packet detection, the proposed spatial filter is not capable of suppressing the jamming signal and clearing it for final signal recovery. As such, we use another module to mitigate the jamming signals.

B. Jamming Suppressor

We describe two main steps that jamming suppressor takes toward recovering the desired signals in the following.

*1) **Jamming Signals Filtering**:* We design a spatial filter and apply it to the received signal in (1). The filter is able to remove the effect of jamming signal effectively. Let us denote the jamming suppressor filter as $\mathbf{U}[k] = [\mathrm{U}_1[k], \mathrm{U}_2[k]]^{\mathrm{T}} \in \mathbb{C}^{2\times 1}$. For such a filter, we have the following proposition.

Proposition 1: The jamming suppressor filter $\mathbf{U}[k] = [1, -\mathrm{H}_{j,1}[k]/\mathrm{H}_{j,2}[k]]^{\mathsf{H}}$ *completely removes the jamming signal* $\mathrm{X}_j[l,k]$ *from the received signal if noise is negligible.*

Proof: Upon applying the jamming suppressor filter on the received signal as $\mathrm{Y}_c[l,k] = \mathbf{U}^{\mathsf{H}}[k]\mathbf{Y}[l,k]$, the filtered signal on subcarrier k and OFDM symbol l can be expressed as:

$$\begin{aligned}\mathrm{Y}_c[l,k] =& \mathbf{U}^{\mathsf{H}}[k]\mathbf{H}[k]\mathrm{X}[l,k] + \mathbf{U}^{\mathsf{H}}[k]\mathbf{H}_j[k]\mathrm{X}_j[l,k] \\ &+ \mathbf{U}^{\mathsf{H}}[k]\mathbf{Z}[l,k].\end{aligned} \tag{2}$$

To clear the effect of jamming signal in (2), the term $\mathbf{U}^{\mathsf{H}}[k]\mathbf{H}_j[k]\mathrm{X}_j[l,k]$ needs to be nullified. It is equivalent to letting $\mathrm{U}_1^{\mathsf{H}}[k]\mathrm{H}_{j,1}[k] + \mathrm{U}_2^{\mathsf{H}}[k]\mathrm{H}_{j,2}[k] = 0$. Such a condition will be easily met if $\mathrm{U}_1^{\mathsf{H}}[k] = 1$, and $\mathrm{U}_2^{\mathsf{H}}[k] = -\mathrm{H}_{j,1}[k]/\mathrm{H}_{j,2}[k]$. This completes the proof and confirm the efficacy of the design presented in Proposition 1.

When the jamming suppressor filter is designed, it nullifies $\mathbf{U}^{\mathsf{H}}[k]\mathbf{H}_j[k]\mathrm{X}_j[l,k]$ on subcarrier k. Therefore, (2) can be represented as:

$$\mathrm{Y}_c[l,k] = \mathrm{H}_c[k]\mathrm{X}[l,k] + \mathrm{Z}_c[l,k], \tag{3}$$

where $\mathrm{H}_c[k] \triangleq \mathrm{H}_1[k] - \mathrm{H}_2[k].\mathrm{H}_{j,1}[k]/\mathrm{H}_{j,2}[k]$ and $\mathrm{Z}_c[l,k] \triangleq \mathrm{Z}_1[l,k] - \mathrm{Z}_2[l,k].\mathrm{H}_{j,1}[k]/\mathrm{H}_{j,2}[k]$. The desired signal in (3) can be recovered with equalizing $\mathrm{H}_c[k]$ over subcarrier k. It is evident that neither jamming suppression step nor signal recovery step is reliant on the exact values of $\mathrm{H}_{j,1}[k]$ and $\mathrm{H}_{j,2}[k]$. Jamming suppressor, instead, uses the CSI ratio of $\mathrm{H}_{j,1}[k]/\mathrm{H}_{j,2}[k]$ for both eliminating the jamming signal and recovering the desired one. Due to the unknown PHY technology used by the jammer, it is not possible to compute the CSI ratio by dividing the individual CSI values at two antennas of the receiver. However, it is possible to directly calculate the CSI ratio using IEEE 802.11p frame format.

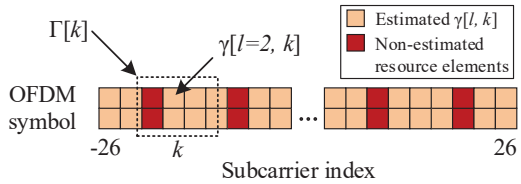


Fig. 8: An illustration of the averaging filter applied for estimating $\tilde{\gamma}[k]$ on subcarrier k.

We take advantage of the unused time-frequency resources within the 802.11p frames to estimate the required jammer CSI ratio over each subcarrier. Denote $\gamma[l,k]$ as the jammer CSI ratio for the signal sample received on OFDM symbol l and subcarrier k. Then, we estimate $\gamma[l,k]$ as:

$$\gamma[l,k] = \frac{\mathrm{Y}_1[l,k]}{\mathrm{Y}_2[l,k]}, \quad \text{for } k \in \mathcal{K} \text{ and } l \in \mathcal{L}, \tag{4}$$

where $\mathcal{K}$ is the set of 40 valid subcarriers in IEEE 802.11p frames that are not assigned to the STF sequence. $\mathcal{L} = \{1, 2\}$ refers to the first two OFDM symbols shown in Fig. 4.

We face the following two challenges regarding the estimation of $\gamma[l,k]$ in (4).

Challenge 1: $\gamma[l,k]$ cannot be estimated over all the subcarriers using the received IEEE 802.11p frames. One may argue that $\gamma[l,k]$ can be calculated when there is no IEEE 802.11p frame inside the received signal. This is not possible in practice as the receiver would not carry out the necessary signal processing steps unless it detects the presence of a legitimate IEEE 802.11p frame.

Challenge 2: From (4), it is evident that $\gamma[l,k]$ is equal to $\mathrm{H}_{j,1}[k]/\mathrm{H}_{j,2}[k]$ only when $\mathrm{Z}_1[k,l]$ and $\mathrm{Z}_2[k,l]$ are zero. As this is not the case in real wireless environments, $\gamma[l,k]$ includes the effect of noise as the estimation error.

To overcome these challenges, we use an averaging filter to interpolate the values of $\gamma[l,k]$ for the missing subcarriers and reduce the impact of noise. Fig. 8 shows an instance of the averaging filter on subcarrier k. The averaging process on subcarrier k can be expressed as:

$$\tilde{\gamma}[k] = \frac{1}{|\Gamma[k]|} \sum_{k \in \Gamma[k]} \gamma[k,l], \tag{5}$$

where $\Gamma[k] = \{k - k_l \leq k \leq k + k_u \text{ and } l = 1, 2\}$, in which k_l and k_u define the lower and upper bounds of the averaging window, respectively.

We resort to simulation in order to evaluate the performance

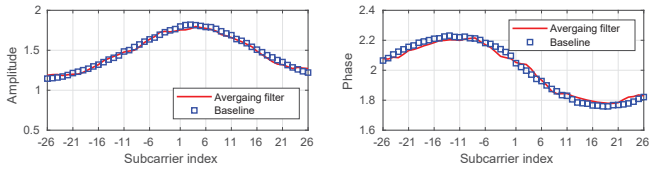


Fig. 9: Amplitude and phase of interpolated $\tilde{\gamma}[k]$ v.s. ideal estimation of $\gamma[k]$ for all subcarriers.

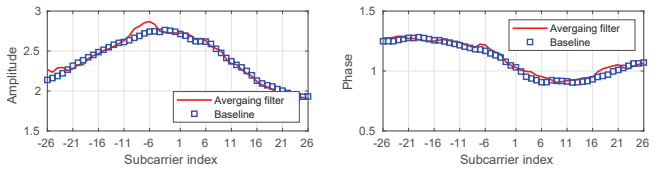


Fig. 10: Amplitude and phase of interpolated $\tilde{\gamma}[k]$ when JNR is 20 dB v.s. ideal estimation of $\gamma[k]$ in noise-free scenario.

of averaging filter in interpolating the missing subcarriers and canceling noise. Fig. 9 shows the amplitude and phase of the interpolated $\tilde{\gamma}[k]$ for all the subcarriers when the averaging filter in (5) is applied and noise is negligible. As the baseline, we use actual $\gamma[k]$ under the same channel realization. Fig. 10 shows the amplitude and phase of the estimated $\tilde{\gamma}[k]$ when the averaging filter is applied, and the jamming signal power to noise power ratio (JNR) is 20 dB. The baseline shows the results for the same setting in the noise-free scenario. The simulation results in Fig. 9 and Fig. 10 show that we can successfully interpolate the $\tilde{\gamma}[k]$ values for missing subcarriers and reduce the impact of the noise by using the filter presented in (5).

*2) **Desired signal recovery**:* Once the filter is applied to the received signal, the jamming suppressor follows its second task. Estimating the compound channel $\mathrm{H}_c[k]$, it recovers the desired signal $\mathrm{X}[l,k]$ over OFDM symbol l and subcarrier k. To do so, it leverages LTF symbols embedded into the preamble of IEEE 802.11p frames and uses the linear least-square method to estimate the compound channel. The estimated channel on subcarrier k can be expressed as $\hat{\mathrm{H}}_c[k] = (\mathrm{Y}_c[3,k] + \mathrm{Y}_c[4,k]) \,/\, (2.\mathrm{X}[3,k])$ for all k. Please note that the LTF OFDM symbols are identical. As such, $\mathrm{X}[3,k] = \mathrm{X}[4,k]$.

We have assumed perfect estimation of $\gamma[k] = \mathrm{H}_{j,1}[k]/\mathrm{H}_{j,2}[k]$ so far. However, this is not a pragmatic assumption. To point out this issue, we replace the $\gamma[k]$ by $\gamma[k]+\varepsilon$, where ε denotes the estimation error. Then, the filtered signal in (3) can be rewritten as:

$$\mathrm{Y}_c[l,k] = \mathrm{H}_c^{'}[k]\mathrm{X}[l,k] + \varepsilon \mathrm{H}_{j,2}[k]\mathrm{X}_j[l,k] + \mathrm{Z}_c^{'}[l,k], \quad (6)$$

where $\mathrm{H}_c^{'}[k] \triangleq \mathrm{H}_1[k] - (\gamma[k]+\varepsilon)\mathrm{H}_2[k]$ and $\mathrm{Z}_c^{'}[l,k] \triangleq \mathrm{Z}_1[l,k] - (\gamma[k]+\varepsilon)\mathrm{Z}_2[l,k]$. The second term in (6) shows the jamming signal scales with ε and introduces an additional error in compound channel estimation. To reduce the impact of this undesired jamming signal as well as the additive noise in channel estimation process, we use channel smoothing technique. We bound $2 \sim 4$ subcarriers together and estimate the compound channel. Once the compound channel is estimated for all subcarriers, its effect is equalized and the signal is recovered as $\hat{X}[l,k] = \mathrm{Y}_c[l,k]/\mathrm{H}_c[k]$ for all k.

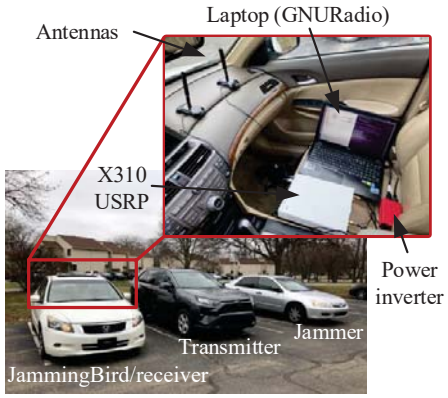


Fig. 11: Our vehicular testbed for evaluating JammingBird.

V. Experimental Evaluation

We have built JammingBird on a proof-of-the-concept vehicular testbed and evaluated its performance on real-world scenarios. We first describe the testbed and test scenarios in detail. Then, we present the performance metrics and experimental results.

A. Experimental Setting

Prototype of JammingBird, Legitimate Transmitter, and Jammer: We have implemented JammingBird using a laptop and an X310 USRP device equipped with two antennas. For the legitimate transmitter, we use an N210 USRP device and a laptop. We use GNURadio protocol stack to drive the USRP devices and carry out the signal processing. The carrier frequency is set to 5.810 GHz, and the sampling rate is set to 10 MSps. The transmit power is also set to 13 dBm. Additionally, we have prototyped a jammer using an N210 USRP device connected to a laptop. The jammer constantly sends noise-like signals with a power of 20 dBm. Each of the legitimate users and the jammer has individually been mounted on a vehicle, as shown in Fig. 11.

Test Scenarios: Fig. 12 shows satellite pictures of our experimental environments: (i) parking lot scenario (Fig. 12(a)) where all three vehicles are mobile at speed of 0∼15 mph; (ii) local street scenario (Fig. 12(b)) where all vehicle move at speed of 25∼45 mph; and (iii) highway scenario (Fig. 12(c)) where the vehicles drive at relatively high speed of 60∼70 mph.

B. Performance Metrics and Baseline

We use error vector magnitude (EVM) and throughput as the metrics for evaluating the performance of JammingBird and conventional 802.11p-based receivers.

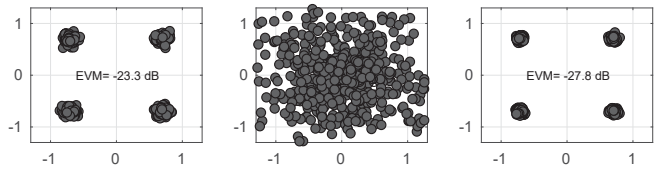
EVM: EVM measures the quality of the recovered symbols. Let us denote $\mathrm{X}[k,l]$ as the symbol transmitted on

(a) Parking lot scenario. (b) Local street scenario. (c) Highway scenario.

Fig. 12: Three outdoor scenarios for evaluating the performance of JammingBird and conventional 802.11p-based receiver.

TABLE I: EVM specification in IEEE standards [9].

EVM (dB)	(inf -5)	[-5 -10)	[-10 -13)	[-13 -16)	[-16 -19)	[-19 -22)	[-22 -25)	[-25 -27)	[-27 -30)	[-30 -32)	[-32 -inf)
Modulation	N/A	BPSK	QPSK	QPSK	16QAM	16QAM	64QAM	64QAM	64QAM	256QAM	256QAM
Coding rate	N/A	1/2	1/2	3/4	1/2	3/4	2/3	3/4	5/6	3/4	5/6
η(EVM)	0	0.5	1	1.5	2	3	4	4.5	5	6	20/3



(a) (b) (c)

Fig. 13: The constellation of the decoded signal by: (a) JammingBird under attack; (b) conventional received under attack; and (c) conventional receiver in jamming-free environment.

subcarrier k and OFDM symbol l, and denote $\hat{\mathrm{X}}[k,l]$ as the corresponding received symbol. The EVM is expressed as $\mathrm{EVM} = 10\log_{10}(\mathbf{E}_{k,l}\{|\mathrm{X}[k,l] - \hat{\mathrm{X}}[k,l]|^2\}/\mathbf{E}_{k,l}\{|\mathrm{X}[k,l]|^2\})$.

Throughput: The achievable throughput can be calculated as $r = \frac{48}{80} \times 10 \times \eta(\mathrm{EVM})$ Mbps, where 48 is the number of data subcarriers, 80 is the length of an OFDM symbol, 10 MHz is the bandwidth, and η is the average number of transmitted data bits per subcarrier. Table I specifies the value of $\eta(\mathrm{EVM})$ for different ranges of EVM [9].

Performance Baseline: As the baseline, we use the performance of a conventional 802.11p-based receiver in the jamming-free scenario, where the jammer is turned off.

C. A Case Study

We conducted a case study to delineate the evaluation process of JammingBird in detail. We consider a local street scenario as shown in Fig. 12(b). JammingBird effectively recovers the desired signal as shown in Fig. 13(a), where the measured EVM and throughput are -23.3 dB and 24 Mbps, respectively. Fig. 13(b) shows that the conventional receiver fails to decode the desired signal under the same jamming attack. As the baseline, Fig. 13(c) shows the constellation of decoded signal by a conventional receiver in a jamming-free environment. The EVM and corresponding throughput of the baseline are -27.8 dB and 30 Mbps, respectively. We can see that JammingBird is capable of mitigating the jamming signal and achieve 80.0% of the jamming-free throughput.

D. Experimental Results

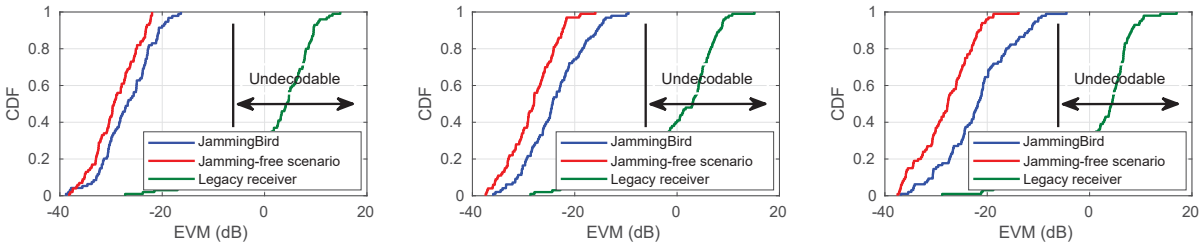
We have performed the previous test for all the test scenarios and recorded the following experimental results.

EVM: Fig. 14 shows the cumulative distribution function (CDF) of the measured EVMs for 100 random realizations in each of the three test scenarios.

As illustrated in Fig. 14, JammingBird successfully suppresses the jamming signals and follows the baseline with a slight degradation in all test scenarios. In particular, the gap between the performance of JammingBird and the baseline is respectively 3.5 dB, 3.8 dB, and 6.3 dB, in parking lot, local street, and highway scenarios. The average measured EVM for the conventional 802.11p-based receiver is 4.5 dB in the parking lot scenario, 3.0 dB in the local street scenario, and 4.2 dB in highway scenario, respectively. The results indicate complete failure of conventional 802.11p-based receiver since data can be recovered if achieved EVM is less than -8.0 dB.

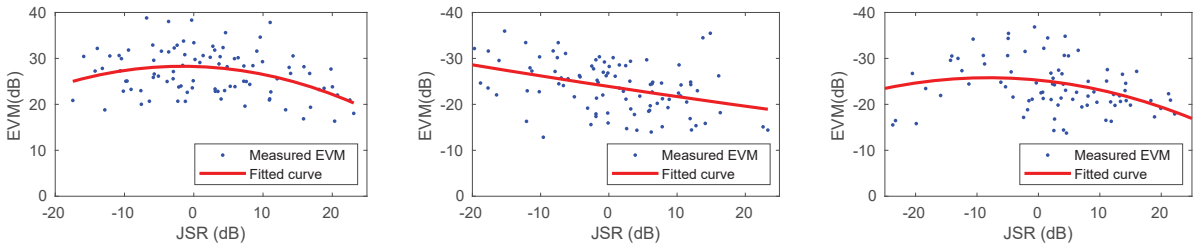
We sorted the measured EVMs of the decoded packets for different JSR values, as shown in Fig. 15. The fitted curves reflect the overall behavior of the measured EVMs. We can see that as the JSR values increase, the fitted curves of the measured EVMs gradually increase. This is mainly due to the error caused by the non-ideal jamming suppressor filter design and the interpolation error in practice, which are magnified as the power of jamming signal increases. Also, as shown in Fig. 15, JammingBird can recover the desired data in the face of jamming signals with 25 dB stronger power than the desired ones.

Throughput: Fig. 16 shows the achieved throughput by JammingBird and conventional receiver in different test scenarios. The average achievable throughput of JammingBird is 26.2 Mbps in the parking lot, 22.2 Mbps in the local street, and 19.5 Mbps in the highway. Under the same test settings, the throughput of the conventional receiver is 6.4 Mbps in the parking lot, 3.1 Mbps in the local street, and 1.8 Mbps in the highway. On average, JammingBird achieves 18.9 Mbps higher throughput than the conventional receiver under constant jamming attacks. The average achievable throughput in the jamming-free scenario is 28.4 Mbps in the parking lot, 27.4 Mbps in the local street, and 26.0 Mbps in the highway. As such, while attacked by strong jamming signals, JammingBird can reach about 83.0% of the throughput of the



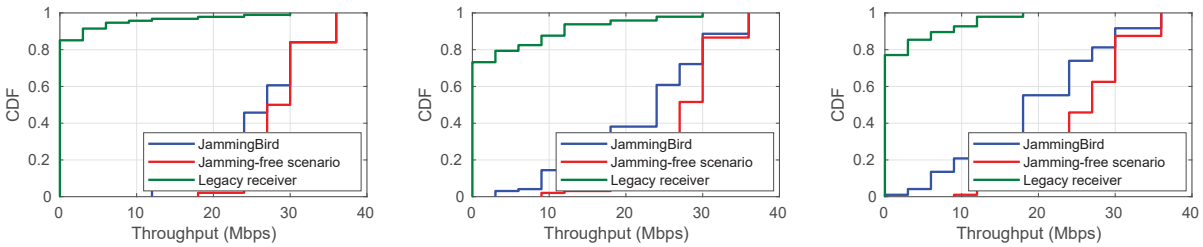
(a) Parking lot scenario. (b) Local street scenario. (c) Highway scenario.

Fig. 14: The distribution of the measured EVMs in different scenarios.



(a) Parking lot scenario. (b) Local street scenario. (c) Highway scenario.

Fig. 15: The measured EVMs versus JSR values.



(a) Parking lot scenario. (b) Local street scenario. (c) Highway scenario.

Fig. 16: The achieved throughput at different test scenarios.

conventional receiver in a jamming-free scenario.

VI. Related Work

In our literature review, we focus on two trajectories. We first review jamming attacks and their countermeasures designed for VANETs. Then, we review MIMO-based anti-jamming techniques.

Jamming Attacks and Anti-Jamming Strategies in VANETs: The security threats in VANETs can be divided into three types of attacks: (i) attacks on vehicular systems, (ii) attacks on information, and (iii) attacks on infrastructure [10]. In the first type of attack, the attacker may target interrupting the social engineering, malware integration, sensor impersonation, and bogus information. The second type attempts to attack the information circulating through the VANETs using jamming attacks, spoofing attacks, fake information, and false position attack. The third type considers attacking the back-end and the network, such as the bogus information between the roadside units and central entities. In [7], [11], Punal *et al.* evaluated the vulnerability of the V2V communications in the face of different class of jamming attacks, including reactive jamming attacks and periodic jamming attacks.

Very limited work has been done so far to countermeasure jamming attacks in VANETs. There are two basic approaches in the literature to do so. As the first approach, the users in a jammed area can use an alternative infrastructure (e.g., cellular networks) for their communications. The authors in [12], [13] proposed to use unmanned aerial vehicles (UAVs) as relays to reroute the users' data traffic to alternative roadside infrastructure when the serving one is out of service due to jamming attacks. As the second approach, detection mechanisms might be used to detect and/or localize the jammer within the network [14]. In [15]–[17], a series of different techniques were proposed for jamming detection in VANETs. In [18], [19], learning-based approaches were proposed to detect and localize the jamming attacks in VANETs.

MIMO-based Anti-jamming Techniques: In [20], [21], Yan *et al.* proposed a jamming cancellation technique for 802.11-based communications against reactive jamming attacks using a MIMO receiver design. The proposed scheme requires the legitimate transmitter's channel knowledge and frame structure

modification to insert user-defined pilot signals for jamming mitigation purposes. In [22], Zeng *et al.* proposed a MMSE-based jamming mitigation solution for 802.11-based communications against constant jamming attacks. In [23], Pirayesh *et al.* proposed a MIMO-based jamming-resilient receiver to secure ZigBee communications against constant jamming attacks. The authors used an online learning approach to decode the ZigBee packets in the face of the jamming signal. In particular, they designed a light-weight neural network and used the received ZigBee preamble signal within the packet for training the network. In [24], [25], jamming-resistant schemes were devised to secure massive MIMO uplink communications against constant jamming attacks. The schemes leverage the jamming CSI to design a jamming cancellation receiver in the spatial domain. However, a prior knowledge of the received jamming signal power on all antennas was required to estimate the jammer CSI.

JammingBird differs from the aforementioned MIMO-based and VANET-oriented countermeasures in the following aspects: First, JammingBird does not require any prior knowledge about the jammer, including its waveform, maximum transmit power, and signaling technology. Second, JammingBird does not require any modification in the standard framework of 802.11p-based transceivers in terms of extra signaling overhead for jamming mitigation purposes. Instead, it uses the 802.11p PHY-layer protocol and leverage MIMO technology to suppress the jamming signal and recover data.

VII. Conclusion

In this paper, we have designed JammingBird, a jamming-resilient receiver to secure vehicular communications against high-power constant jamming attacks. The enablers of JammingBird are two MIMO-based techniques: Jamming-resistant synchronizer and jamming suppressor. These two modules enable JammingBird to detect, synchronize, and recover desired signals under strong constant jamming attacks. We have implemented JammingBird on a proof-of-the-concept vehicular testbed and conducted extensive experiments to evaluate its performance under common vehicular test scenarios. Experimental results show that JammingBird is able to maintain 83.0% of throughput when legitimate communications undergo strong constant jamming attacks.

Acknowledgement

This work was supported in part by the NSF grants CNS-2100112, CNS-2113618, CNS-1950171, and CNS-1949753.

References

[1] W. H. Organization *et al.*, "Association for safe international road travel," *Global Status Report on Road Safety*, 2018.

[2] U. Farooq, J. L. Hardy, L. Gao, and M. A. Siddiqui, "Economic impact/forecast model of intelligent transportation systems in Michigan: An input output analysis," *Journal of Intelligent Transportation Systems*, vol. 12, no. 2, pp. 86–95, 2008.

[3] M. Barth and K. Boriboonsomsin, "Environmentally beneficial intelligent transportation systems," *IFAC Proceedings Volumes*, vol. 42, no. 15, pp. 342–345, 2009.

[4] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, 2018.

[5] U. FCC, "In the matter of use of the 5.850-5.925 GHz band," *Notice of Proposed Rulemaking, ET Docket*, no. 19-138, pp. 19–129.

[6] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *arXiv preprint arXiv:2101.00292*, 2021.

[7] O. Punal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE transactions on vehicular technology*, vol. 64, no. 2, pp. 524–540, 2014.

[8] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[9] IEEE Standards Association, "IEEE 802.11p: IEEE standard for information technology–local and metropolitan area networks–specific requirements–part 11: Wireless LAN medium access control (MAC) and physical layer (PHY)," 2014.

[10] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Vehicular Communications*, vol. 19, p. 100179, 2019.

[11] O. Puñal, A. Aguiar, and J. Gross, "In VANETs we trust? characterizing RF jamming in vehicular networks," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*, pp. 83–92, 2012.

[12] X. Lu, D. Xu, L. Xiao, L. Wang, and W. Zhuang, "Anti-jamming communication game for UAV-aided VANETs," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2017.

[13] L. Xiao, X. Lu, D. Xu, Y. Tang, L. Wang, and W. Zhuang, "UAV relay in VANETs against smart jamming with reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4087–4097, 2018.

[14] A. T. Nguyen, L. Mokdad, and J. Ben Othman, "Solution of detecting jamming attacks in vehicle ad hoc networks," in *Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems*, pp. 405–410, 2013.

[15] L. Mokdad, J. Ben-Othman, and A. T. Nguyen, "DJAVAN: Detecting jamming attacks in vehicle ad hoc networks," *Performance Evaluation*, vol. 87, pp. 47–59, 2015.

[16] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6475–6488, 2016.

[17] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining," *IEEE Communications Letters*, vol. 23, no. 3, pp. 442–445, 2019.

[18] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Vehicular Communications*, vol. 13, pp. 56–63, 2018.

[19] S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao, and H. Zhou, "Delimitated anti jammer scheme for Internet of vehicle: Machine learning based security approach," *IEEE Access*, vol. 7, pp. 113311–113323, 2019.

[20] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "MIMO-based jamming resilient communication in wireless networks," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, pp. 2697–2706, 2014.

[21] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming resilient communication using MIMO interference cancellation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1486–1499, 2016.

[22] H. Zeng, C. Cao, H. Li, and Q. Yan, "Enabling jamming-resistant communications in wireless MIMO networks," in *Proceedings of IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, 2017.

[23] H. Pirayesh, P. Kheirkhah Sangdeh, and H. Zeng, "Securing ZigBee communications against constant jamming attack using neural network," *IEEE Internet of Things Journal*, 2020.

[24] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 210–223, 2018.

[25] H. Akhlaghpasand, E. Björnson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 182–186, 2019.