Hindawi
Security and Communication Networks
Volume 2019, Article ID 2064348, 18 pages
https://doi.org/10.1155/2019/2064348

Research Article

Estimating the Relative Speed of RF Jammers in VANETs

Dimitrios Kosmanos,[1] **Antonios Argyriou**,[1] **and Leandros Maglaras**[2]

[1]*Department of Electrical & Computer Engineering, University of Thessaly, Volos, Greece*
[2]*Department of Computing Technology, De Montfort University, Leicester, UK*

Correspondence should be addressed to Leandros Maglaras; leandrosmag@gmail.com

Received 20 May 2019; Revised 24 October 2019; Accepted 5 November 2019; Published 23 November 2019

Academic Editor: Emanuele Maiorana

Vehicular Ad Hoc Networks (VANETs) aim at enhancing road safety and providing a comfortable driving environment by delivering early warning and infotainment messages to the drivers. Jamming attacks, however, pose a significant threat to their performance. In this paper, we propose a novel Relative Speed Estimation Algorithm (RSEA) of a moving vehicle that approaches a transmitter (Tx)-receiver (Rx) pair that interferes with their radio frequency (RF) communication by conducting a denial of service (DoS) attack. Our scheme is completely passive and uses a pilot-based received signal without hardware or computational cost to, firstly, estimate the combined channel between the transmitter-receiver and jammer-receiver and, secondly, to estimate the jamming signal and the relative speed between the jammer-receiver using the RF Doppler shift. Moreover, the relative speed metric exploits the angle of projection (AOP) of the speed vector of the jammer in the axis of its motion in order to form a two-dimensional representation of the geographical area. Our approach can effectively be applied for any form of the jamming signal and is proven to have quite accurate performance, with a mean absolute error (MAE) value of approximately 10% compared to the optimal zero MAE value under different jamming attack scenarios.

1. Introduction

Autonomous vehicles, capable of navigating in unpredictable real-world environments with little human feedback, are a reality today [1]. Autonomous vehicle control imposes very strict security requirements on the wireless communication channels that are used by a fleet of vehicles [2]. This is necessary in order to ensure reliable connectivity [3]. Moreover, the Intelligent Vehicle Grid technology, introduced in [4], allows the car to become a formidable sensor platform, absorbing information from the environment, other cars, or the driver and feed it to other vehicles and infrastructure so as to assist in safe navigation, pollution control, and traffic management. The vehicle grid essentially becomes an Internet of Things (IoT) for vehicles, namely, the Internet of Vehicles (IoV) that is capable of making its own decisions when driving customers to their destinations [5].

The connected autonomous vehicles (CAVs) that use the wireless vehicle-to-vehicle (V2V) communication have become essential for the operation of a modern vehicle [6]. Wireless communications, however, are vulnerable to a wide range of attacks [7, 8]. An RF jamming attack consists of radio signals maliciously emitted to disrupt legitimate communications. Jamming attacks are a big threat to any type of wireless network. With the rise in safety-critical vehicular wireless applications, this is likely to become a constraining issue for their deployment in the future. A subcategory of jamming attacks is the denial of service (DoS) attacks, which are targeting the availability of network services. Of special interest are the mobile jammers, which impose an added strain on vehicular networks (VANETs). The accurate prediction of the behavior of the jammer such as its speed becomes critical for providing a swift reaction to an attack.

In this work, we propose a novel metric that captures the relative speed between the jammer (Jx) and the receiver (Rx). We also propose the Relative Speed Estimation Algorithm (RSEA) that is a completely passive estimation method that uses pilot-based received signals at the receiver to, firstly, estimate the channel between the transmitter-receiver and jammer-receiver and, secondly, the jamming signal and thirdly,

to estimate the relative speed between the jammer-receiver using the RF Doppler shift properly. This is the first work in the literature, according to our knowledge, that proposes an algorithm for speed estimation of malicious RF jammers.

1.1. Problem Statement. In addition to RF jamming, wireless communication between a transmitter (Tx) and a receiver can be impaired by unintentional interference and multiple access control (MAC) protocol collisions. Jammers can exhibit arbitrary behavior in order to disrupt and thwart communication with a form of DoS attack [9]. In the general case, RF jamming reduces the receiver signal to interference and noise ratio (SINR), a problem that can be addressed with classic communication algorithms. However, in several applications, it is critical to detect accurately the presence of a jammer, i.e., the precise reason behind the reduction in SINR, the packet delivery ratio (PDR), and more importantly, the nature of the attack. Consequently, it is difficult to determine whether the reason for the SINR reduction is an intentional jamming attack or unintentional interference. The challenge in detecting an RF jamming attack is that the information that is available for the jammer is typically minimal and it can be derived from the useful signal possibly mixed with other types of arbitrary interference in the area. By estimating the relative speed between a legitimate vehicle and a jammer, we can conclude if a high interference scenario has been provoked intentionally with the form of a DoS attack by an attacker that approaches the victim or has been provoked unintentionally by an area with significant RF interference. Specifically, if the estimated relative speed metric is around zero, we can infer that the jammer is moving at the same speed with the receiver. On the other hand, if the estimated relative speed has a high value, we can conclude that the jammer is moving at a quite different speed than that of the receiver. Of particular interest is the higher level behavior of a jammer, like its motion/movement relative to the Tx-Rx pair.

1.2. Our Solution. Using the jamming signal at the receiver, we estimate the relative speed metric (Δu) that is based on the difference or sum between the velocities of the jammer and the receiver. This passively estimated metric also includes information regarding the angle of projection (AOP) of the jammed signal. Our scheme uses only the signal at the receiver under the presence of a jammer to characterize the behavior/motion of the jammer (if the Jx is approaching or moving away from the Rx) using the RF Doppler shift. We also adopt a pilot-based method for the channel estimation between Tx-Rx since it is suitable for fast varying channels, like VANETs, because the channel is directly estimated by training symbols or the pilot tone that are known a priori to the receiver.

The contributions of the paper are threefold:

(i) A completely passive pilot-based scheme is proposed that is based on RF communication between Tx-Rx being interfered by a jammer in the area. However, we do not apply the proposed RSEA for estimating only the speed of the Tx [10]. We try from this point-to-point communication to gather as much information as possible regarding jammer's behavior, such as all the combined multipath channels among Tx, Rx, Jx, jammer's relative speed value, and the jamming signal.

(ii) In addition, the proposed relative speed metric uses novel physical location features because it includes the AOP of the jammer.

(iii) The effective usage of the estimated relative speed for a future jamming detection algorithm is outlined.

It has to be highlighted that the proposed RSEA can also be applied to any form of the jamming signal.

The rest of this paper is organized as follows. Section 2 presents the related work, whilst Section 3 analyzes the network topology, the system model analysis, and the wireless channel model. Section 4 presents the location-aware relative speed metric, and Section 5 analytically describes the proposed RSEA. Section 6 presents the experimental evaluation of the proposed RSEA and provides comparison between different scenarios. Section 7 justifies the experimental behavior of the proposed relative speed metric and describes real applications that the metric can be used. Finally, Section 8 concludes the paper and gives some directions for future work.

2. Related Work

2.1. RF Jamming. RF jamming has been extensively studied in the context of classical 802.11 networks without accounting for the particularities of car-to-car communications. Besides the differences in PHY design of 802.11p compared to other 802.11 amendments, the propagation conditions of VANETs are fundamentally different due to the highly dispersive and rapidly changing vehicular environment. A lot of different jamming attacks have been studied in VANETs [11]. The two most important categories of jamming attacks are the constant jamming and the reactive jamming. Constant jamming transmits randomly generated data on the channel without checking the state of the channel (idle or not). The reactive jamming happens only when the attacker senses activity on the channel. In [12], the authors observe that constant, periodic, but also reactive RF jammer can hinder communication over large propagation areas, which would threaten road safety. Reactive jamming attacks reach a high jamming efficiency and can even improve the energy efficiency of the jammer in several application scenarios [13, 14]. Also, they can easily and efficiently be implemented on commercially available off-the-shelf (COTS) hardware such as USRP radios [15–17]. But, more importantly, reactive jamming attacks are harder to detect due to the attack model, which allows the jamming signal to be hidden behind transmission activities performed by legitimate users [16, 18, 19].

A different category of attacks is the pilot-based attacks against OFDM and OFDMA signals [20]. These attacks seek to manipulate information used by the equalization algorithm to cause errors to a significant number of symbols. However, we do not evaluate this type of attack because the point of interest of this paper is the DoS attacks that are targeting the availability and not the integrity of packets. In

order to be robust against pilot tone jamming attacks, OFDM and OFDMA systems must randomize their subcarrier locations and values. For the mitigation of this type of RF jamming attacks, optimal power allocation with user scheduling techniques is proposed [21], utilizing also the technique of uncoordinated frequency hopping (UFH) [22]. UFH implies the communication between transmitter and receiver through a randomly chosen frequency channel unknown for both agents. In [23], the authors highlight the secrecy level of wireless networks under UFH, showing the harmful security effect of broadband eavesdropper adversaries capable of overhearing in multiple frequencies. In order to stop such eavesdroppers, the authors propose the use of broadband friendly jammers that cause interference on eavesdroppers. The goal is to cause as much interference as possible to eavesdroppers that are located in unknown positions, while limiting the interference observed by the legitimate receiver. The information about the location and speed of friendly jammers is crucial for the above UHF schemes.

The effects of RF jamming can be alleviated using cooperative relaying schemes to where the vehicles outside of the jamming area serve as relays to help forward the received control channel signal to the victim vehicles through another jamming-free service channel [24]. However, the jamming scenarios that are used in this paper are limited since the location of the jammer is assumed to be known in advance (either being an RSU or a moving node). The antijamming V2V communication in CAV networks through power selection in conjunction with channel selection is analyzed in [25]. Specifically, a brain-inspired cognitive dynamic system (CDS) is applied to study V2V communications, and the general structure of cognitive risk control (CRC) is tailored to analyze and address the jamming problem in CAV networks. After that, the power control is carried out first using the reinforcement learning method, the result of which is then examined by the task-switch control. However, the mobility of vehicles and the vehicle speeds are not considered in the channel model and the complicity of the proposed method is questionable too. By analyzing these articles, we can conclude that the jammer's speed is a crucial metric for all the techniques that try to address the jamming problem in RF communications in VANETs.

2.2. Localization. A lot of work has covered matters of localization, which is a fundamental challenge for any wireless network of nodes, in particular when nodes are mobile. In [26], the relative positions and velocities (PVs) are estimated up to a rotation and translation of an anchor-less mobile network, given two-way communication capability between all the nodes. A least-squares-based dynamic ranging algorithm is proposed, which employs a classical Taylor series-based approximation to estimate pairwise distance derivatives efficiently without the usage of Doppler shifts. However, this approach requires the existence of a cluster of nodes with predefined initial locations. On the contrary, the proposed RSEA algorithm does not require any initial information for the location of vehicles. In [27], the authors propose a dual-level travel speed calculation model, which is established under different levels of sample sizes. Wireless sensor networks (WSNs) are widely used to maintain the location information and rely on the tracking service only when their location changes. In the proposed approach in [28], the problem of tracking cooperative mobile nodes in wireless sensor networks is addressed with the calculation of Doppler shifts of the transmitting signal in combination with a Kalman filter (by performing a constrained least-squares optimization when a maneuver is detected). In [29], the authors suggest a method for joint estimation of the speed of a vehicle and its distance to a roadside unit (RSU) for narrowband orthogonal frequency-division multiplexing (OFDM) communication systems. Spatial filtering and a maximum-likelihood (ML) algorithm are developed for distance estimation. The vehicle speed is calculated using a kinematics model based on the estimated distance and angle of arrival (AOA) values. Comparing the aforementioned methods with our proposed speed estimation method, it is obvious that the RSEA is applicable to a VANET without any extra infrastructure such as WSNs or complex calculations like Kalman filters and without the need for deployment of RSUs for traffic recording. The localization of a smart jammer that is trying to hide his precise location has proved to be a difficult issue for the majority of the aforementioned works since position verification models are susceptible to statistical errors. The survey paper [30] notes the need for applying data fusion at the PHY layer of the 802.11p protocol of wireless access in vehicular environment (WAVE) signals with upper layers for a vehicle positioning, a method that our scheme is using.

2.3. Speed Estimation. Another group of papers proposes speed estimation systems that alert drivers about driving conditions and help them avoid joining traffic jams using multiclass classifiers. ReVISE in [31] proposes a multiclass SVM approach that uses features from the RF signal. The proposed experimental testbed must be established in a specific part of the road and is completed by two stable access points and two monitor points. However, it is doubtful whether it can be applied to a scenario with more than one vehicle in the specific area such as the scenario we are considering. Using a similar method, MUSIC [32] is a subspace-based AOA estimation algorithm that exploits the eigenstructure of the covariance matrix of the received signals on a multisignal classifier using a uniform circular array (UCA) antenna as extra hardware.

Covariance-based speed estimation schemes have also been used for the estimation of the maximum Doppler spread, or equivalently the vehicle velocity that is useful for improving the performance of handoff algorithms [33]. Specifically, the authors in [33] propose a velocity estimator based on spectral moments of in-phase and the quadrature-phase component or the squared envelope of the received signal. The proposed method has the least sample variance as compared to other covariance-based methods. However, all the covariance-based speed estimators do not assume shadowing in the channel model and the improvement of

their performance comes at expense of more computational complexity and therefore an added delay in computation time. Such models are not easily applicable to a frequently changed V2V wireless channel with many vehicles and obstacles where a lot of shadowing and scattering effects exist. Only the authors in [10] propose a velocity estimator that uses the statistics of the instantaneous frequency (IF) of the received signal to estimate the velocity and takes also into account the distribution of the scattered component of the received signal and is also robust to path loss and shadowing. The only restrictive assumption of this method for being applied in a VANET environment is that, in order to estimate the velocity, prior estimation of directivity parameter of the incoming waves is needed. The authors in [34] proposed an algorithm that employs a modified normalized autocovariance of received signal power to estimate the speed of mobile nodes. The simulation results indicate that this algorithm is reliable to estimate the mobile speed with corresponding maximum Doppler shift up to 500 Hz. However, a great challenge of fast-moving communications such as V2V is the high Doppler shifts due to the relative motion between communicating vehicles.

In [35], an algorithm that estimates the speed of a mobile phone by matching time-series signal strength data to a known signal strength trace from the same road is introduced. The drawback of the correlation algorithm is the observation that the signal strength profiles along roads remain relatively stable over time, which is not so realistic for a VANET. Although the results are more accurate than previous techniques that are based on handoffs or phone localization, this method requires the travelers to have their mobile phones open during their travel. This is a limiting factor for a smart jammer, who has its phone inactive to remain undetected, in comparison with our proposed speed estimation method that can detect smart jammers. In [36], a method for the estimation of speed for mobile phone users using known WiFi signal-to-noise ratio (SNR) data from the past and time-domain features like mean, maximum, and autocorrelation is proposed. However, in a frequently changing environment such as a V2V channel, it is almost impossible that the SNR values remain constant. For this reason, the proposed RSEA algorithm does not require any training data about SNR or other PHY layer data, whilst in [37], two novel autocorrelation- (ACF-) based velocity estimators are used, without requiring knowledge of the SNR of the link. The drawback of both speed estimation techniques is that there is some dependence of velocity on estimator performance and there is also a limit to the velocity up to 185 km/h. On the contrary, our proposed speed estimation method can estimate quite large relative speeds without any speed limit.

In all the prior works, speed estimators that have been proposed include training procedures in order to estimate traffic congestion or other transportation performance metrics using sensor measurements. However, the speed estimation problem from a security perspective has been not widely investigated. Only, in [38], the authors try to estimate the AOA of the specular line of sight (LOS) component of signal received from a given single antenna transmitter using a predefined training sequence. The results show the optimality of the training-based ML-AOA estimator in the case of a randomly generated jamming signal. However, the drawback of this ML-AOA estimator is that this superior performance is subject to the availability of a perfect CSI and the knowledge of jammer's strategy which is unlikely in a realistic system. Finally, the authors in [39] introduced a new algorithm to estimate the mobile terminal speed at base station (BS) in cellular networks. This helps BS in estimating the channel Doppler shift, using measured received signals at the BS. The performance of the proposed algorithm is modeled in a Terrestrial Trunked Radio (TETRA) network, and the simulation has shown acceptable results for a wide range of velocities and jammers. However, using this algorithm, the estimated Doppler shift depends on the carrier frequency which is much smaller in a cellular network (i.e., 396 MHz) compared to a VANET (i.e., 5.9 GHz). In contrast, in the speed estimation approached by this paper, the carrier frequency of a VANET is used without any impact on the performance of the speed estimation procedure.

Recently, extensive works present video-based speed estimation techniques using a single camera [40, 41]. Furthermore, speed estimation techniques are used by applications for traffic counting that are based on wireless magnetic sensor networks (WMSNs). The authors in [42] propose a system for traffic speed estimation which can effectively eliminate the geomagnetic background interference. A morphological filter is designed for removing the interference and extracting the magnetic signatures of vehicles. However, all the aforementioned works require specific infrastructure or sensor such as camera, RAdio Detection And Ranging (RADAR), Light Detection And Ranging (LIDAR), magnetic sensors, and Visible Light Detection and Ranging (ViLDAR) that built upon sensing visible light variation of the vehicle's headlamp [43]. All these sensors have a pretty high cost. In contrast, our proposed method of speed estimation uses only the wireless signal at the Rx for the estimation of the relative speed metric Δu between Jx and Rx without any need for extra infrastructure. Last, a recent research [44] explores a novel technique which could estimate the speed of a vehicle by analyzing its influence on surrounding wireless signals from roadside wireless infrastructures, such as WiFi. To achieve this goal, in this paper, it is proposed and formulated a model to characterize the relationship between the phase and amplitude measurements and the vehicle speed. Based on the model, a method is developed that can detect the vehicle and estimate its speed accordingly using the frequency domain information involved in the spectrogram. However, this model estimates vehicle's speed by analyzing the influence of the vehicle on surrounding wireless signals using two static roadside WiFi devices. In contrast, our proposed method estimates the relative speed between two moving vehicles that can be assumed as transmitter and receiver that interchange pilot signals using the V2V wireless communication without the need of any additional infrastructure.

The great majority of the works have used covariance-based speed estimators. Some of them do not take into

account the shadowing effect of VANETs, others need initially sampling of the SNR links for a training procedure, and last some need perfect knowledge about the directivity of transmitted waves in order to estimate the receiver's speed improving handover algorithms between transmitter and receiver under a typical microcellular system. However, this type of network is assumed to be relatively stable in contrast to a VANET where the V2V channel yields more rapid and more severe fading than cellular networks. All the remaining state-of-the-art papers for speed estimation use extra hardware infrastructure, WSNs, or RSUs for traffic recording and therefore for position or speed verification. Moreover, the speed estimation approaches that use RSUs are not applicable for estimating the speed of a jammer as indication of jamming in the area because a smart jammer may change its travel behavior (i.e., speed and direction) in order to look like a legitimate vehicle and remain undetected. Our proposed technique is the first in the literature, to the best of our knowledge, that uses only the unicast communication between two moving vehicles Tx and Rx for the prediction of the jammer's speed and for future detection of a jamming attack without any initial knowledge about the location of vehicles or the channel conditions. Our method uses this point-to-point communication between Tx-Rx to gather as much information as possible regarding jammer's behavior, such as all the combined multipath channels among Tx, Rx, Jx, jammer's relative speed value, and jamming signal. The proposed system is dynamic and can be applied to any road topology for the jammer's speed estimation. Moreover, there has been no prior work that combines a feature of the physical location, except of the AOA at the receiver, such as the AOP of the Jx with its speed, in order to estimate relative speeds of two moving vehicles (jammer-receiver) during a jamming attack, using the channel Doppler shift value.

3. System Model and Preliminaries

3.1. Network Topology. We consider unicast V2V communication between transmitter and the receiver and a point-to-point V2V communication between a single jammer and the receiver. This simple scenario in a rural area is used for the initial verification of our system without high interference of other vehicles. In this area, a static obstacle already exists that impacts the communication between Tx-Rx and Jx-Rx.

The jammer transmits wireless packets/signals that may form a reactive jamming signal. We assume that the Tx-Rx pair of vehicles in our model moves at a constant speed for a period of time. This approach allows the modeling of platoons of vehicles that are formed by maintaining a constant distance with each other [2]. We assume that the jammer moves with a constantly increasing speed with the ultimate goal to approach the receiver and intervene in the effective communication zone of the Tx-Rx pair. AS it can be seen in the network topology of Figure 1, the distances between Jx-Rx in the y-axis and in the x-axis are $dy_{(\mathrm{Jx-Rx})}$ and $dx_{(\mathrm{Jx-Rx})}$, respectively, together with the actual distance between Jx-Rx $d_{(\mathrm{Jx-Rx})}$, which is the hypotenuse of the rectangular triangle that is formed. The motion of the vehicles in Figure 1 is characterized by the speed

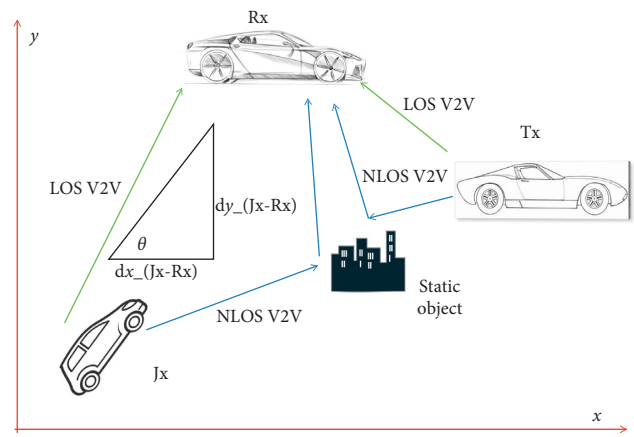

Figure 1: The network topology in which the orange vehicle is the jammer that approaches the Tx-Rx pair from a AOP (θ) angle. This figure also includes the multipath fading effects by a static object.

vectors ($\vec{u}_{\mathrm{Rx}}, \vec{u}_{\mathrm{Jx}}, \vec{u}_{\mathrm{Tx}}$). Only $\vec{u}_{\mathrm{Rx}}, \vec{u}_{\mathrm{Tx}}$ have the same direction, which is the direction of the x-axis. The jammer approaches the Tx-Rx with an AOP (θ). So, the speed vector of the jammer is projected in the axis of the motion of vector $\vec{u}_{\mathrm{Rx}}$ with an AOP (θ) Figure 2(a). In this figure, we also notice that the AOP (θ) is not equal to zero. Moreover, the angle that is formed between the speed vector of the jammer $\vec{u}_{\mathrm{Jx}}$ and the wireless signal that travels between the Jx and the Rx is called the angle of departure (AOD) and is denoted as ϕ in Figure 2. In Figure 2(a), the line of sight (LOS) component between Jx-Rx has a AOD (ϕ) equal to zero, while the non-line of sight (NLOS) component between Jx-Rx has a AOD (ϕ), which is different to zero in Figure 2(b).

3.2. System Overview. In our system model, K known pilot symbols that compose the symbol vector $\vec{x}_{\mathrm{pilot}} = [x_{\mathrm{pilot}}(1), \ldots, x_{\mathrm{pilot}}(K)]^T = [1, \ldots, 1]^T$ are being sent over consecutive K time instants from the transmitter to the receiver. At the same time, the jammer simultaneously transmits over consecutive K time instants K jamming symbols to the receiver that composes the symbol vector $\vec{s} = [s_1, \ldots, s_K]^T$. So we consider the received vector at the receiver $\vec{y} = [y(1)y(2), \ldots, y(K)]^T$, which consists of the combined symbols that the Rx receives from the transmitter and the jammer at K consecutive time instants. Therefore, for every time instant $n \in (0, K]$, the receiver signal $y(n)$ is the summation of the pilot symbol sent by the transmitter $x_{\mathrm{pilot}}(n)$ and the symbol sent by the jammer s_n. Using pilots, the LOS channel and the $N-1$ NLOS channels between Jx – Rx are estimated by the receiver. The receiver can also define the specific value of parameter N, which is the total number of multipath rays. The wireless channel is assumed to be constant for the duration of the transmission of the K pilot symbols from Tx to Rx.

3.3. Attacker Model. We consider jammers that aim to block completely the communication over a link by emitting interference reactively when they detect packets over the air, thus causing a DoS attack. The jammers minimize their

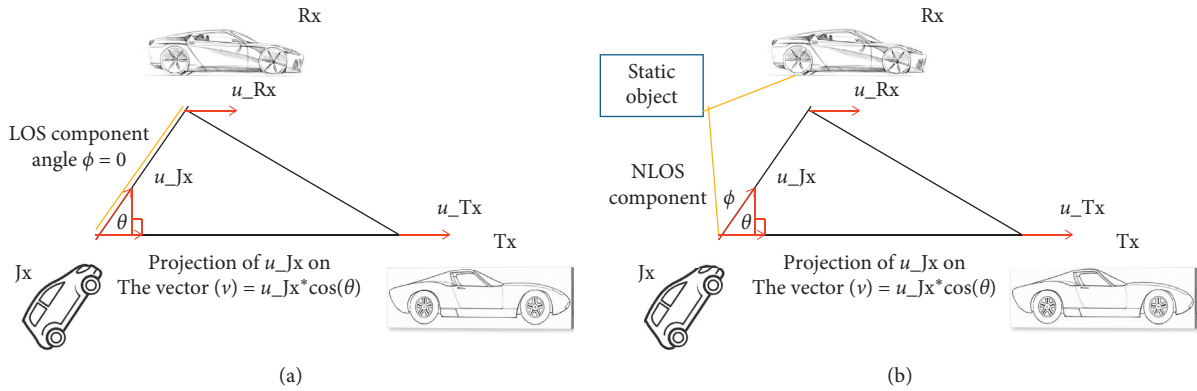

FIGURE 2: Illustration of projections of velocities u_{Jx} on the vector $\overrightarrow{v}$. Two-dimensional scheme. (a) LOS ray of Jx-Rx communication with $\phi = 0$, $\theta \neq 0$. (b) NLOS ray of Jx-Rx communication with $\phi \neq 0$, $\theta \neq 0$.

activity to only a few symbols per packet and use minimal, but sufficient power, to remain undetected. We assume that the jammer is able to sniff any symbol of the packet over the air in real time and react with a jamming signal that flips selected symbols at the receiver with high probability (see [45]).

The jammer is designed to start transmitting upon sensing energy above a certain threshold in order for a reactive jamming attack to succeed. We set the latter to −86 dBm as it is empirically determined to be a good trade-off between jammer sensitivity and false transmission detection rate, when an ongoing 802.11p transmission is assumed. So, the symbol vector $\overrightarrow{s}$ that reaches at the Rx from the Jx after K time instants has the same length as the pilot symbol vector that reaches the Rx from the Tx after K time instants, provided that the jammer transmits only when senses a transmission from the transmitter. Each one of the K scalar values depends on the used power by the jammer. The jammer continuously transmits with the same transmission power, with the purpose of overloading the wireless medium thus representing a DoS attack [46]. This work assumes that the jammer continuously transmits the same jamming symbol to the receiver forming a *simplified jamming signal* of the form $\overrightarrow{s} = [f, \ldots, f]^T$ with length K and f a random unknown value to the receiver. Furthermore, the proposed RSEA can operate with a different form of the jamming signal. This is possible when the Tx sends more pilot symbols to the Rx than the sum of the different unknown jamming symbols being sent by the jammer.

Recall that the main goal of this paper is to show how we can estimate the speed of a noncooperative malicious attacker that can eventually be used as extra useful information for the design of RF jamming detection schemes [47].

3.4. Channel Model. Multipath is the propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths. The multipath scenario illustrated in Figure 1 includes a static obstacle in order for the multipath effects to be considered in the communication between Tx-Rx and Jx-Rx. So, it exists the LOS component of the wireless signal being sent by the Jx and Tx and also the NLOS component. In the NLOS component, the AOP (θ) is not equal to zero and the AOD (ϕ) between the speed vector of the jammer and the NLOS ray is also not equal to zero (see Figure 2(b)). The phenomena of reflection, diffraction, and scattering due to the multipath give rise to additional radio propagation paths beyond the direct optical LOS path between the radio transmitter and receiver.

In our work, we adopt the Rician fading model, which is a channel model that includes path loss and also Rayleigh fading [48]. When a signal is transmitted, the channel adds Rician fading. The Rician fading model is particularly appropriate when there is a direct propagating LOS component in addition to the faded component arising from multipath propagation.

The Rician channel at time instant t is defined with the help of multiple NLOS paths, which is similar to the Rayleigh fading channel but with the addition of a strong dominant LOS component. Parameter q defines the channel between Tx − Rx with $q = 1$ and the channel between Jx − Rx with $q = 2$. We define a complex Gaussian random variable ζ_G that is uniform over the range $[0, 2\pi]$ and is fully specified by the variance σ_q^2. The Rician fading channel can be defined with the help of this random variable as

$$h_q[t] = \sqrt{\frac{k}{k+1}}\sigma_q e^{j(2\pi/\lambda)\left(f_c + f_{d,\max}\cos\phi_q\right)\tau_q}\delta\left(t - \tau_q\right) + \sqrt{\frac{k}{k+1}}\zeta_G. \tag{1}$$

In the above equation, f_c is the carrier frequency, $f_{d,\max}$ is the maximum Doppler shift, ϕ_q is the incidence AOD between the vector of speed $\overrightarrow{u}_{\text{Jx}}$ with the vector of the jamming signal, $\tau_q = d/c$ is the excess delay time for the LOS ray that travels between the two communicating nodes in channel h_q, d corresponds to the distance between the two communicating nodes, and t is the current time instant. The first term corresponds to the specular LOS path arrival and the second to the aggregate of the large number of reflected and the scattered paths. Parameter k is the ratio of the energy in the specular path to the energy in the scattered paths; the larger the k is, the more deterministic the channel is [49]. Finally, $(\gamma_q = \sqrt{k/k+1}\,\sigma_q)$ in (1) is the amplitude associated with the LOS path, which is known at the receiver. Rician channel model is often a better model of representing fading compared to the Rayleigh model.

The channel response $\overrightarrow{y}$ after K consecutive symbols sent by the jammer and the transmitter is as follows:

$$\overrightarrow{y} = \sum_{l=0}^{N-1} \left(h_1[l]\ \overrightarrow{x}_{\text{pilot}}[N-l] + h_2[l]\ \overrightarrow{s}\ [N-l] \right) + \overrightarrow{w}. \tag{2}$$

In above equation, the $\overrightarrow{y}$ is a $K \times 1$ column vector. Moreover, $\overrightarrow{x}_{\text{pilot}}$ is the symbol vector that the Rx receives from the Tx after K consecutive time instants and $\overrightarrow{s}$ is the symbol vector that the Rx receives from the Jx after K consecutive time instants again. The symbol vectors ($\overrightarrow{x}_{\text{pilot}}[N-l]$, $\overrightarrow{s}\ [N-l]$) have the same values, as defined above, for the l different paths of the respective channels, where $\forall l \in (0, N-1]$. The $\overrightarrow{w}$ represents the additive white Gaussian noise (AWGN) with zero mean. We assume also that the jammer and the transmitter send at very close time instants their symbols at the receiver, so that h_1, h_2 channels can remain stable for sending K symbols. Moreover, N is the overall multipath rays in the area. For the estimation of this parameter, we use the GEMV simulator [50]. For describing the modeled area, GEMV uses the outlines of vehicles, buildings, and foliage. Based on the outlines of the objects, it forms R-trees. R-tree is a tree data structure in which objects in the field are bound by rectangles and are hierarchically structured based on their location in space. Hence, GEMV employs a simple geometry-based small-scale signal variation model and calculates the additional stochastic signal variation and the number of diffracted and reflected rays based on the information about the surrounding objects. We must note that the wireless RF communication of the Tx-Rx pair and the Jx-Rx pair is taking place in a specific frequency band, according to the existing standard for automotive systems [51].

3.5. Transmission in the MAC/PHY Layer. We assume single carrier communication at the PHY. The 802.11p MAC also provides prioritized Enhanced Distributed Channel Access (EDCA) and can support applications by providing different levels of quality of service (QoS). In our model, only the 802.11p MAC EDCA AC[0] channel with higher priority is used for the pilots. The pilot beacons from the Tx to the Rx are transmitted with high probability of successful delivery, increasing the accuracy of the proposed RSEA at the same time. Any type of collisions at the wireless channel resulting from competing traffic is addressed by the MAC EDCA backoff mechanism for distances smaller than the carrier sensing (CS) range of 1000 m. So we assume that our speed estimation algorithm has a correct reaction and for high interference situations from other vehicles.

4. Location-Aware Relative Speed Metric

One of the main novel ideas of this work is that we take into account the physical location of the Jx and Rx nodes and the direction of their motion when calculating the relative speed metric. In the general case, the Rx does not move in the same direction as the Jx (see Figure 1). For this case, Δu includes the AOP (angle θ) of the Jx between Jx and Rx. The geometry-aware metric takes into account the distance $\mathrm{d}y_{(\text{Jx–Rx})}$ and the distance $\mathrm{d}x_{(\text{Jx–Rx})}$. So a rectangular triangle is formed by the sides $\mathrm{d}x_{(\text{Jx–Rx})}, \mathrm{d}_{(\text{Rx–Jx})}, \mathrm{d}y_{(\text{Jx–Rx})}$. As it can be seen from Figure 1, the distance $\mathrm{d}_{(\text{Jx–Rx})}$ is the hypotenuse of the rectangular triangle, which means that $\cos(\theta) = \mathrm{d}x_{(\text{Jx–Rx})}/\mathrm{d}_{(\text{Jx–Rx})}$. So, the speed of the Jx (source) with respect to the Rx speed, while the Jx and the Rx are moving in the same direction, is the relative speed between the two vehicles moving towards each other and is equal to the sum of their individual speed vectors $\Delta\overrightarrow{u}_{\text{line}} = \overrightarrow{u}_{\text{Jx}} + \overrightarrow{u}_{\text{Rx}}$. Moreover, $\overrightarrow{v} = \overrightarrow{u}_{\text{Tx}}/\|u_{\text{Tx}}\|$ is the unit length vector pointing from the Jx to the Tx. The relative speed of the Jx and the Rx can be defined as the following dot product:

$$\Delta u = \overrightarrow{v}\,\Delta\overrightarrow{u}_{\text{line}}. \tag{3}$$

To represent all the speed vectors of Figure 1 in two dimensions (x, y), we project the vector $\overrightarrow{u}_{\text{Jx}}$ on the unit length vector $\overrightarrow{v}$. $\overrightarrow{v}$ is in the direction of x-axis (see Figure 2). The projected vector is $\overrightarrow{u}_{\text{Jx}}\cos(\theta)$. On the other hand, $\overrightarrow{u}_{\text{Rx}}$ is already a vector in the direction of the x-axis (see Figure 2), which has the same direction as the projection of $\overrightarrow{u}_{\text{Jx}}$. This allows the calculation of the relative speed between Jx – Rx using the two vectors ($\overrightarrow{u}_{\text{Jx}}\cos(\theta)$, $\overrightarrow{u}_{\text{Rx}}$) that have the same direction with the vector $\overrightarrow{v}$.

In (3), if we use the projection vector $\overrightarrow{u}_{\text{Jx}}\cos(\theta)$ and the $\overrightarrow{u}_{\text{Rx}}$ vector, we get the final version of our metric, which is given by

$$\Delta u = \left| \overrightarrow{u}_{\text{Jx}} \left(\frac{dx_{(\text{Jx–Rx})}}{\mathrm{d}_{(\text{Jx–Rx})}} \right) + \overrightarrow{u}_{\text{Rx}} \right| = \left| \overrightarrow{u}_{\text{Jx}}\cos(\theta) + \overrightarrow{u}_{\text{Rx}} \right|. \tag{4}$$

This is the Δu metric in the direction of $\overrightarrow{v}$. The addition is justified by the fact that the vectors $\overrightarrow{u}_{\text{Jx}}\cos(\theta)$, $\overrightarrow{u}_{\text{Rx}}$ have the same direction. In the above equation, $\overrightarrow{u}_{\text{Jx}}$, $\overrightarrow{u}_{\text{Rx}}$ are the speed vectors of the Jx and the Rx, respectively. According to our model, if the Jx approaches the receiver, $\cos(\theta)$ increases. As the $\overrightarrow{u}_{\text{Rx}}$ remains constant and the $\overrightarrow{u}_{\text{Jx}}$ is constantly increasing, (4) is an increasing function and its maximum value indicates a nearby jamming attack.

As Δu increases, the jammer approaches the receiver and when Δu decreases, the jammer is moving away from the Tx and the Rx. If the Jx and the Rx are located on the same road, an actual straight line and the vectors $\overrightarrow{u}_{\text{Jx}}$, $\overrightarrow{u}_{\text{Rx}}$ have the same direction, then our metric is the sum between Jx – Rx speed vectors ($\overrightarrow{u}_{\text{Jx}} + \overrightarrow{u}_{\text{Rx}}$). Otherwise, if the vectors $\overrightarrow{u}_{\text{Jx}}$, $\overrightarrow{u}_{\text{Rx}}$ have opposite directions, our metric is estimated by the difference ($\overrightarrow{u}_{\text{Jx}} - \overrightarrow{u}_{\text{Rx}}$).

Taking into account the direction of the Jx relative to the direction of the Rx, the general form of the above metric is as follows:

$$\Delta u = \left| \overrightarrow{u}_{\text{Jx}}\cos(\theta) \pm \overrightarrow{u}_{\text{Rx}} \right|. \tag{5}$$

It is crucial to point out that the above metric is the actual value of the relative speed that will be used in the subsequent sections to model the Doppler shift between the jammer and the receiver.

5. Proposed Estimation Scheme

5.1. Estimation of the Combined Pilot/Jamming Signal. The channel between two nodes with jamming is captured in (2). For the proposed RSEA, a pilot-based method for channel estimation is used. So, the signals that Rx receives from the Tx and the jammer interfere additively. In (2), if we differentiate the one LOS component from the other $N-1$ NLOS components, we have the following equation:

$$\overrightarrow{r}_{\text{LOS}} = h_1^{\text{LOS}}\,\overrightarrow{x}_{\text{pilot}}[N] + h_2^{\text{LOS}}\,\overrightarrow{s}\,[N], \tag{6}$$

where the channel values $h_1^{\text{LOS}} = h_1[0], h_2^{\text{LOS}}[2] = h_2[0]$ and the symbol vectors $\overrightarrow{x}_{\text{pilot}}[N]$, $\overrightarrow{s}\,[N]$ represent the unique LOS component of the total N multipath values. If the NLOS multipath components are added,

$$\overrightarrow{y} = \overrightarrow{r}_{\text{LOS}} + \sum_{l=1}^{N-1}\left(h_1[l]\,\overrightarrow{x}_{\text{pilot}}[N-l] + h_2[l]\,\overrightarrow{s}\,[N-l]\right) + \overrightarrow{w}. \tag{7}$$

In (7), the received vector $\overrightarrow{y}$ is the convolution between h_1 and the pilot symbol vector $\overrightarrow{x}_{\text{pilot}}$ and the convolution between h_2 and the jamming symbol vector $\overrightarrow{s}$. Moreover, the $K \times 1$ column received vector $\overrightarrow{y}$ for the K received values for every time instant during which the receiver collects every pilot that is sent from the transmitter is given by

$$\overrightarrow{y} = \begin{bmatrix} r_{\text{LOS}}[1] + \sum_{l=1}^{N-1}\left(h_1[l] + h_2[l]s_1[N-l]\right) \\ r_{\text{LOS}}[K] + \sum_{l=1}^{N-1}\left(h_1[l] + h_2[l]s_K[N-l]\right) \end{bmatrix} + \begin{bmatrix} w_1 \\ \dots \\ w_K \end{bmatrix}. \tag{8}$$

To estimate the channel between Tx-Rx(h_1), the channel between Jx-Rx(h_2), and the jamming symbol vector $\overrightarrow{s}$, the best we can do is to estimate the combined vector parameter:

$$\overrightarrow{z} = \begin{bmatrix} \sum_{l=0}^{N-1}\left(h_1[l]x_{\text{pilot}}[N-l] + h_2[l]s_1[N-l]\right) \\ \sum_{l=0}^{N-1}\left(h_1[l]x_{\text{pilot}}[N-l] + h_2[l]s_K[N-l]\right) \end{bmatrix}. \tag{9}$$

Vector $\overrightarrow{z}$ has the above form for the short time that is required by the receiver to collect all the K symbols of the pilot vector. Recall that for a short time duration, the wireless channel is assumed constant. So for all the K values of vector $\overrightarrow{z}$ in (9), the parameters $h_1[l], h_2[l], x_{\text{pilot}}[N-l]$ remain constant and only the jamming symbols may change depending on the form of the jamming symbol vector sent by the jammer. We use a MMSE estimator [52], which finds a better estimate from least squares (LS), in order the K values of $\overrightarrow{z}$ to be estimated:

$$\widehat{\overrightarrow{z}} = \left(\overrightarrow{x}_{\text{pilot}}^{H} C_w^{-1}\,\overrightarrow{x}_{\text{pilot}}\right)^{-1}\overrightarrow{x}_{\text{pilot}}^{H} C_w^{-1}\,\overrightarrow{y}, \tag{10}$$

where C_w is the covariance matrix of the noise vector $\overrightarrow{w}$. Vector $\overrightarrow{z}$ in (10) has K components each having N unknown multipath channel components. So, both the h_1, h_2 channels can be estimated and also the K values of the jamming signal $\overrightarrow{s}$ can be estimated too.

If the *simplified jamming signal* is used $\overrightarrow{s} = [f, \dots, f]^T$, in which the jammer continuously sends the same jamming symbol, which is unknown to the Rx, we have $2N$ unknown values for the two channels h_1, h_2 with K equations in (9) and one unknown value for the jamming symbol f. So if the condition $K > 2N + 1$ is valid, we can see that each one of the channel values h_1, h_2 out of N multipath values can be estimated with the elimination method for the solution of the linear system with K equations and $2N$ unknown values in (9). The values of the wireless channels h_1, h_2 remain constant for each value of vector $\overrightarrow{z}$. Moreover, the above linear system can also be solved with a completely irregular form of the jamming signal provided that the length of the pilot symbol vector $\overrightarrow{x}_{\text{pilot}}$ being sent from the Tx to the Rx is larger than the sum of the number of the unknown jamming symbols with the value of parameter (which is the double number of overall multipath rays in the area for the estimation of both h_1, h_2 channels) $2N$. We only utilize the LOS component of the vector $\overrightarrow{z}$ for the estimation of the relative speed metric using Doppler shift. So, the useful part from vector $\overrightarrow{z}$ that we need for the relative speed estimation through the Doppler shift is $\overrightarrow{r}_{\text{LOS}} = \left(\begin{bmatrix} h_1^{\text{LOS}} + h_2^{\text{LOS}}s_1 \\ \dots \\ h_1^{\text{LOS}} + h_2^{\text{LOS}}s_K \end{bmatrix}\right)$. If we only want to estimate the $h_1^{\text{LOS}}, h_2^{\text{LOS}}$ values of vector $\overrightarrow{r}_{\text{LOS}}$ without the multipath values, the above conditions for the solution of the linear system in (8) can be simplified to $K > 3$ for the *simplified jamming signal* form.

5.2. Proposed Algorithm. The proposed RSEA is presented in Algorithm 1. First, the Tx specifies the number of multipath rays N in the area that the GEMV propagation model is used, as explained in subsection 3.4. Then, the RSEA is used for every time step with the transmission of a pilot that consists of $K = 2N + 2$ symbols. In line 4 of the algorithm, the combined channel between the Tx and the Rx, with the intervention of the Jx, is estimated from the vector $\overrightarrow{y}$ using a MMSE estimator. Depending on the jamming signal, the inequality that must be valid for the RSEA system to be resolvable for all the N multipath values is different. In the final 10th line of the RSEA, the relative speed value is estimated. A component $\hat{r}_{\text{LOS}}[1]$ of the estimated vector of the combined LOS channels $\widehat{\overrightarrow{r}}_{\text{LOS}}$ (each one of the K components of $\overrightarrow{r}_{\text{LOS}}$ has the same combined channel values) can be combined with the ray-optical baseband complex number $(a_1 + b_1 j)s_1$, which is the jamming signal that the *Rx* finally receives from the Jx. Specifically, the subtraction of the channel h_1^{LOS} component from the $\hat{r}_{\text{LOS}}[1]$ value can be set equal to the ray-optical baseband complex number $(a_1 + b_1 j)s_1$. The complex number $(a_1 + b_1 j)s_1$ characterizes the baseband form of the narrowband wireless channel. This narrowband wireless channel is a function of the relative speed Δu between the jammer and receiver and the Doppler shift between the two moving objects.

(1) N% It is specified by the Tx for the specific area using the GEMV propagation model.
(2) **for Every time step** (t^{RSEA}) A pilot signal with $K = 2N + 2$ symbols being sent from Tx to Rx **do**
(3) N% It is respecified by the Tx for the specific area using the GEMV propagation model.
(4) $\widehat{\overrightarrow{z}} \leftarrow \mathrm{MMSE}\,(\overrightarrow{y}, C_w^{-1})$
(5) $\overrightarrow{r}_{\mathrm{LOS}} \leftarrow \left(\begin{bmatrix} h_1^{\mathrm{LOS}} + h_2^{\mathrm{LOS}} s_1 \\ \cdots \\ h_1^{\mathrm{LOS}} + h_2^{\mathrm{LOS}} s_K \end{bmatrix}\right)$ %LOS components
(6) **if** $((K > 2N + 1))$ % and $\overrightarrow{s}$ has the *simplified jamming signal* form **then**
(7) $\widehat{\overrightarrow{r}}_{\mathrm{LOS}} \leftarrow \left(\begin{bmatrix} h_1^{\mathrm{LOS}} + h_2^{\mathrm{LOS}} s \\ \cdots \\ h_1^{\mathrm{LOS}} + h_2^{\mathrm{LOS}} s \end{bmatrix}\right)$ % The $\overrightarrow{r}_{\mathrm{LOS}}$ and $\overrightarrow{z}$ values can be estimated.
(8) $\hat{r}_{\mathrm{LOS}}[1] - h_1^{\mathrm{LOS}} = (a_1 + b_1 j)\, s$
(9) **end if**
(10) $\widehat{\Delta u}$ Estimation % estimated relative speed value from (8)
(11) **end for**

Algorithm 1: Relative Speed Estimation Algorithm (RSEA).

5.3. Channel Model with Doppler Shift. In this subsection, we describe in more detail the wireless LOS combined channel model $h_1^{\mathrm{LOS}} + h_2^{\mathrm{LOS}}$ between Tx-Rx and Jx-Rx. The proposed relative speed value Δu can be estimated using only the LOS combined channel models. The tracked LOS components also show fading characteristics, likely due to the ground reflection which cannot be resolved from the true LOS. For this reason, we choose the same model for the LOS component as for the discrete components. Small-scale fading characteristics do not affect significantly the communication between Tx and Rx, as compared to NLOS conditions and, therefore, the Δu estimation procedure. So central to this paper is the introduction of the proposed metric Δu in the channel model of (1), taking into account the path loss value at the receiver. This path loss value only depends on the distance between the communicating nodes and usually gets small values for a narrowband wireless channel. Let us consider the channel model such as defined by the Rx for a ray transmitted between two nodes as [53]

$$\sum_{q=1}^{2} h_q^{\mathrm{LOS}}(t, \tau_q) = \sum_{q=1}^{2} \gamma_q po_q e^{j(2\pi/\lambda)\left(f_c + f_{d,\max}\cos\phi_q\right)\tau_q} \delta(t - \tau_q). \tag{11}$$

In the above equation, q defines the channel between Tx − Rx with $q = 1$ and the channel between Jx − Rx with $q = 2$, γ_q is the amplitude associated with the LOS path, po_q represents the free space propagation loss [54], λ is the wavelength, f_c the carrier frequency, $f_{d,\max}$ is the maximum Doppler shift that depends on the Δu metric such as in (3), ϕ_q is the incidence AOD between the vector of speed $\overrightarrow{u}_{\mathrm{Jx}}$ and the vector of the jamming signal, $(\tau_q = d/c)$ is the excess delay time that the ray travels between the two nodes, and t is the current time instant. We assume the LOS case for the communication between the jammer and the receiver, as can be seen in Figure 2(a). The LOS ray between the Jx and the Rx has the same direction with the speed vector of the jammer. As a consequence, the AOD is equal to zero ($\cos\phi_q = 1$, in (11)). The observed frequency at the receiver is $f' = f_c(1 + (\Delta u/c)\cos\phi_q)$, which depends on the relative speed Δu of the two vehicles (jammer and receiver) that we defined in the previous subsection. The baseband channel model for a ray transmitted between two nodes with the intervention of a jammer therefore becomes

$$\sum_{q=1}^{2} h_q^{\mathrm{LOS}}(t, \tau_q) = \sum_{q=1}^{2} \gamma_q po_q e^{j(2\pi/\lambda) f_c \left(1 + (\Delta u/c)\cos\phi_q\right)\tau_q} \delta(t - \tau_q). \tag{12}$$

We can see that the Doppler shift Δf Hz that is observed in the Rx can be equal to [55]

$$\Delta f = \frac{\Delta u f_c \cos\phi_q}{c}. \tag{13}$$

And the maximum Doppler shift is as follows:

$$f_{d,\max} = \frac{\Delta u}{c}. \tag{14}$$

Now, let τ_q be the time that is required for a signal to travel the distance d. Then, we can rewrite h_2^{LOS} from (12) as

$$h_2^{\mathrm{LOS}}(t, \tau_2) = \gamma_2 po_2 e^{j(2\pi/\lambda) f_c (1 + (\Delta u/c)) d/c} \delta\left(t - \left(\frac{d}{c}\right)\right). \tag{15}$$

In the above equation, we use a $f_c = 5.9$ GHz, which is the band dedicated to V2V communication. The channel $h_2^{\mathrm{LOS}}(t, \tau_2)$ is also the channel of a baseband signal in (15) and if $((\Delta u/c) \gg 1)$ has the following form:

$$h_2^{\mathrm{LOS}}(t, \tau_2) = \gamma_2 po_2 e^{j(2\pi/\lambda)\left(f_c (\Delta u/c)\right)(d/c)} \delta\left(t - \left(\frac{d}{c}\right)\right). \tag{16}$$

To get our final signal model, we replace the path loss parameter po_2 with the following equation:

$$po_2 = G_{0,p}\left(\frac{d_{\mathrm{ref}}}{d}\right)^{n_p}, \tag{17}$$

where $G_{0,p}$ is the received power at a reference distance d_{ref}, which is a standard value at about 100 m, n_p is the path loss

exponent, which is equal to 2 for the pure LOS links, and d is the distance that the transmitted ray travels between the two communicating nodes. So, po_2 only depends on the distance d that the ray travels. We denote $\Delta t = t_i^{\mathrm{RSEA}} - t_{i-1}^{\mathrm{RSEA}}$ as the time interval between the current time instant and the preceding one, in which the RSEA is reapplied (t_{i-1}^{RSEA}). Furthermore, if $h_2^{\mathrm{LOS}}(t, \tau_2)$ represents the channel between the Rx-Jx pair, the distance between the two nodes after the time interval Δt is $d = \Delta u \Delta t$, when the jammer approaches the receiver. Substituting (17) into (16), h_2^{LOS} can be rewritten as

$$h_2^{\mathrm{LOS}}(t, \tau_2) = \gamma_2 G_{0,p}\left(\frac{d_{\mathrm{ref}}}{\Delta u \Delta t}\right)^2 e^{j(2\pi/\lambda)(f_c(\Delta u/c))\tau_2}\delta\left(t - \left(\frac{d}{c}\right)\right). \tag{18}$$

In the above equation, the only unknown parameter is Δu at time t. Reorganizing (18), we have the following equation:

$$h_2^{\mathrm{LOS}}(t, \tau_2) = \gamma_2 G_{0,p}\left(\frac{d_{\mathrm{ref}}^2}{\Delta u^2 \Delta t^2}\right)\delta\left(t - \left(\frac{d}{c}\right)\right) \cdot (\cos(\omega_2) + j\sin(\omega_2)), \tag{19}$$

where $\omega_2 = (2\pi/\lambda)(f_c(\Delta u/c))\tau_2$. In the above equation, the only unknown parameter is Δu.

For the LOS channel betweenTx − Rx, we know that the receiver moves with the same speed as the transmitter, such as a platoon of vehicles with two members. The above means that the Doppler phenomenon is nonexistent. Following (16) for the formulation of the channel h_1^{LOS} without the existence of Doppler phenomenon, we can see that this channel only depends on the path loss component and the complex amplitude associated with the LOS path. The path loss component po_1 and the complex amplitude variable γ_1 can be estimated by the receiver. So the h_1^{LOS} can be represented by a complex number:

$$h_1^{\mathrm{LOS}}(t, \tau_1) = \gamma_1 po_1 e^0 = a_{Tx-Rx} + b_{Tx-Rx} j. \tag{20}$$

Reformulating the combined value of the LOS channels (h_1^{LOS}, h_2^{LOS}) in (12) by combining equations (20), (19), we have the following equation:

$$\sum_{q=1}^{2} h_q^{\mathrm{LOS}}(t, \tau_{qi}) = \gamma_1 po_1 + \gamma_2 G_{0,p}\left(\frac{d_{\mathrm{ref}}^2}{\Delta u^2 \Delta t^2}\right)\delta\left(t - \left(\frac{d}{c}\right)\right) \cdot (\cos(\omega_2) + j\sin(\omega_2)). \tag{21}$$

5.4. Relative Speed Estimation. At this point, we have an estimate of the baseband channel h_2^{LOS} between Jx − Rx, which can be represented with a complex number. The final baseband signal that reaches at the receiver after the intervention of the jammer can be represented as $(a_1 + b_1 j)s$. From Algorithm 1, we know that the jamming symbols of the symbol vector $\overrightarrow{s}$ is part of the vector $\overrightarrow{r}_{\mathrm{LOS}}$. So, if from the estimated combined value $\widehat{r}_{\mathrm{LOS}}$ we subtract the channel h_1^{LOS}, which can be estimated by the receiver, the value ($\widehat{r}_{\mathrm{LOS}} - h_1^{\mathrm{LOS}} = h_2^{\mathrm{LOS}} s$) can be set equal to the baseband received signal at the receiver:

$$\widehat{r}_{\mathrm{LOS}} - h_1^{\mathrm{LOS}} = (a_1 + b_1 j)s. \tag{22}$$

From the above equation, also

$$h_2^{\mathrm{LOS}} s = (a_1 + b_1 j)s. \tag{23}$$

Reusing the (19) from the previous section, the ray-optical baseband complex number $(a_1 + b_1 j)$ can be set equal to

$$(a_1 + b_1 j)s = \gamma_2 G_{0,p}\left(\frac{d_{\mathrm{ref}}^2}{\Delta u^2 \Delta t^2}\right)\delta\left(t - \left(\frac{d}{c}\right)\right) \cdot (\cos(\omega_2)\mathrm{Re}(s) + j\sin(\omega_2)\mathrm{Im}(s)), \tag{24}$$

where $\omega_2 = (2\pi/\lambda)(f_c(\Delta u/c))\tau_2$. The jamming signal $\overrightarrow{s}$ is estimated by the receiver from Algorithm 1. So the $\mathrm{Re}(s)$, $\mathrm{Im}(s)$ are known values to the receiver. From the above equation, we can calculate the desired parameters a_1, b_1:

$$\frac{a_1}{\left(\gamma_2 G_{0,p}\left(\left(d_{\mathrm{ref}}^2 \delta(t - (d/c))/\Delta u^2 \Delta t^2\right)\right)\right)} = \cos\left(\left(\frac{2\pi}{\lambda}\right)\left(f_c \frac{\Delta u}{c}\right)\tau_2\right), \tag{25}$$

$$\frac{b_1}{\left(\gamma_2 G_{0,p}\left(d_{\mathrm{ref}}^2 \delta(t - (d/c))/\Delta u^2 \Delta t^2\right)\right)} = \sin\left(\left(\frac{2\pi}{\lambda}\right)\left(f_c \frac{\Delta u}{c}\right)\right)\tau_2\Big). \tag{26}$$

From (25) and (26) and with the use of the Euler identity, we have the following equation:

$$\cos\left(\left(\frac{2\pi}{\lambda}\right)\left(f_c \frac{\Delta u}{c}\right)\right)\tau_2\Big)^2 + \sin\left(\left(\frac{2\pi}{\lambda}\right)\left(f_c \frac{\Delta u}{c}\right)\right)\tau_2\Big)^2 = 1. \tag{27}$$

In (27), there is only one unknown variable Δu. So, we can calculate Δu as

$$\widehat{\Delta u} = \sqrt[4]{\frac{G_{0,p}^2 \gamma_2^2 d_{\mathrm{ref}}^4 \delta(t - (d/c))^2}{\Delta t^4 \left(a_1^2 + b_1^2\right)}}. \tag{28}$$

From the above equation, we can see that the estimated $\widehat{\Delta u}$ value depends only on the excess delay time $\tau_2 = d/c$ that is caused by the Doppler phenomenon and not on the actual value of Doppler shift.

6. Performance Evaluation

6.1. Evaluation Setup. Our evaluation scenario is conducted on the outskirts of the city of Aachen, representing a real-world environment while assuming that this is a rural area. Our experimental setup considers unicast data transmissions in a network consisting of three nodes: a transmitter, a receiver, and a jammer, and V2X broadcast communication for 10 interfering vehicles outside of the CS range between the Tx and the Rx (distance more than 1000 m). Two different moving RF jamming attack scenarios are evaluated. Analyzing RF Jammer Behavior 1 VI-C, the Tx-Rx pair (see Figure 1) travels with a constant speed of approximately 50 Km/h and with constant distance of

approximately 20 m, as a platoon of vehicles. The Jx is also moving on a side road with zero initial speed and accelerates to a maximum speed of 60 Km/h in order to approach the Tx-Rx pair. In RF Jammer Behavior 2 VI-D, the transmitter and the receiver travel with constant speed of approximately 48 Km/h when the jammer approaches the crossroads, as illustrated in Figure 3, with accelerating speed and a maximum limit of 50 km/h.

Our experiments are conducted using the Veins-Sumo simulator [56] with the simulation parameters presented in Table 1 such as the initial distance between the jammer and the pair of Rx-Tx, d_{Jx-Rx}; the distance that separates the receiver from the transmitter throughout the course of the simulation d_{Tx-Rx}; the closest distance in which the jammer arrives relative to the Tx-Rx pair as well as the power of all the transmitted signals $P_{Tx,Jx}$; the time interval Δt after RSEA is reapplied; and the specific value of the parameter N, which is the number of the multipath rays. Last, the standard reference distance d_{ref} is used for the estimation of the LOS path loss component.

As illustrated in Figure 3, there is a time interval Δt_{eff}, in which the transmitter can effectively communicate with the receiver. It starts with the "*Start of Communication Zone*" and ends with the "*Start of the Effective Zone*" of the Jx. After the start of the effective zone of the Jx, the jammer is located at distances smaller than 30 m away from the receiver and it can completely jam the communication between the Tx and the Rx by constructing a "*black hole*." All the evaluation parameters are summarized in Table 2.

During the performance evaluation, we test our proposed RSEA with different SINR values for two real-life scenarios. When the jamming vehicle is approaching the Tx-Rx pair, the SINR is given by

$$\text{SINR} = \frac{\left\| h_1 \overrightarrow{x}_{\text{pilot}} \right\|^2}{\left\| h_2 \overrightarrow{s} \right\|^2 + \sigma_n^2}. \tag{29}$$

The SINR level is measured by the receiver at the PHY layer. In the above equation, the noise power σ_n^2 is the noise power. Moreover, the mean absolute error (MAE) between the real Δu value and the estimated is calculated for both scenarios. This is the difference between the actual relative speed metric Δu with the estimated relative speed metric $\widehat{\Delta u}$:

$$\text{MAE} = \frac{1}{ns} \left| \Delta u_i - \widehat{\Delta u_i} \right|, \tag{30}$$

where i is an integer number that identified with the current time instant in which the real and the estimated Δu variable have a specific value and $ns = 10$ is the number of measurements for the specific speed value. The MAE value gets its optimal zero value when the real Δu is identified with the estimated. We assume this optimal value as a reference point for the MAE (%) calculations for the rest of the paper.

6.2. Speed Estimator Comparison. All state-of-the-art recent papers from 2014 onwards for speed estimation, along with the proposed one, are summarized and compared under specific conditions in Table 3. These articles fall into some specific categories. Some of the papers use RSUs installed on the side of the road that can detect a vehicle and estimate its speed by analyzing the influence of the vehicle on surrounding wireless signals from roadside wireless infrastructures (see [27, 29, 44]). In the same category belong the articles that require static nodes with specific magnetic sensors to collect the earth magnetic field and estimate the speed of a vehicle by calculating the similarity of vehicle signatures between these static nodes (see [42]). Last, recent papers such as [43] use ViLDAR systems to estimate a vehicle's speed using received light power (intensity) variations of a vehicle's headlamps as transmitter and static

Figure 3: Graphical representation of the Δt_{eff} from the Tx – Rx pair between the communication zone and effective zone of the Jx.

Table 1: Simulation parameters.

Evaluation parameters in veins simulator	Values
$d_{Tx,Rx}$	20 m
[CW [min], CW [max]]	[3, 7]
Vehicle's transmission range	130–300 m
Initial d_{Jx-Rx}	300 m
CS range of 802.11p protocol	1000 m
Interfering vehicles outside of CS range Tx – Rx	10
d_{Jx-Rx} at "black hole"	25 m
$P_{Tx,Jx}$	100 mW
Minimum sensitivity (P_{th})	−69 dBm to −85 dBm
f_c	5.9 GHz
Doppler shift for $\Delta u = 120$ km/h	± 655.5 Hz
d_{ref}	100 m
Δt	2 s
N	4

Table 2: Evaluation scenario parameters.

Independent parameters	RF Jammer 1	RF Jammer 2
Tx-Rx velocity	50 Km/h	48 Km/h
Jx velocity	60 Km/h	50 Km/h
Δt_{eff}	15.5 sec	18 sec
"Black hole" of communication	13.5 sec	18 sec
Time of Δu peak	23.4 sec	25 sec

Table 3: Method limitations.

Categories	[26]	[28]	[35]	([39])	[40]	[42]	[41]	[43]	[RSEA]
RSU, static sensors, static cameras	×	×		×	×	×	×	×	
Extra sensors on vehicles (UCA)		×							
Limitations (speed limit)	×		×					×	
Training data		×	×					×	

photodetectors as receiver through visible light communication (VLC). Moreover, some papers need static cameras located at the roads for the speed estimation procedure ([40, 41]). However, these methods require the deployment of many RSUs or additional hardware to estimate vehicle speed over a large section of the road, and therefore, the cost of the methods is high. The methods that use RSUs for estimating the speed of an RF jammer are not applicable additionally because a smart jammer may change its travel behavior (i.e., speed and direction) in order to look like a legitimate vehicle and thus remain undetected. Another category of papers uses specific hardware embedded in the vehicle such as UCA antennas, RADAR, and LIDAR for the speed estimation [29]. These techniques are also very expensive. Some papers need also big or medium training data for the speed estimation using either complicated kinematic models [27] or the autocorrelation between two time series of WiFi signals using different samples of SNR data [36]. Similarly, some papers must use a proper (relatively large) window size for collecting training data for performing speed estimation [44]. A last category of articles deals with some of the limitations that impose on the speed estimation process. Specifically, some of the papers assume moving vehicles with speed limits of up to 60 km/h which corresponds to relatively low sampling rates required for the WiFi hardware used [29, 44]. However, a great challenge of V2V communication is the high Doppler shifts due to the fast-moving communicating vehicles. Such corresponding limiting factors for a VANET may be the high computational time or the applicability of the method only to relevant static nodes such as applications for estimating speed directly from signal strength profiles of mobile phones.

Concluding, it is obvious that the proposed RSEA method is the only method in the state-of-the-art literature that estimates the relative speed of a jammer with a completely passive scheme that is based on RF communication between Tx-Rx with the interference of a jammer in the area, without extra cost for adding sensors or hardware. Moreover, we can conclude that the proposed method is the only method in the literature that combines the physical orientation of the vehicles in the considering jamming scenario with the relative speed Δu between Jx-Rx without extra sensors. Last, the proposed method is the only method that does not susceptible to high Doppler shift or relative speed values that are observed in V2V communication. It may be noted that, later in this section, the proposed RSEA will be evaluated on a wide range of jammer speed values.

6.3. Results of RF Jammer Behavior 1. In RF Jammer Behavior 1, we assume that the pair Tx-Rx moves with a high constant speed (50 Km/h) when the jammer accelerates with a higher maximum speed (60 Km/h), while transmitting a jamming signal with a *simplified* form to the receiver. The first figure of Figure 4(a) shows a comparison between the real Δu and the estimated value. Specifically, by observing the start time of the steep slope of SINR in Figure 5(b), we can conclude that it coincides with the start of the jamming attack, 15.5 sec. The main reason for the sharp decrease of the SINR in our experiment is the jamming attack and not the interference from the entire environment. In that case, the total received power at the Rx is also increased indicating the jamming attack. Moreover, in Figure 4(a), after 15.5 sec, for which Δu is above 20 rad∗m/s, the SINR in Figure 5(b) has also a steep slope. So, the effective zone of communication between Tx and Rx is approximately $\Delta t_{\text{eff}} = 15.5$ sec, whilst after that it is corrupted for 13.5 sec. So, the "black hole" in the communication range between the Tx and the Rx is during the time interval (15.5 sec–29 sec). After 29 sec, we have the end of the attack. For this time interval (15.5 sec–29 sec), the MAE of our proposed RSEA increases to 23% from the optimal MAE value (see Figure 6).

In Figure 4(a), we can see that Δu reaches a maximum value, approximately 32.5 rad∗m/s, at the time instant 23.4 sec. At this time, Jx is approaching the Tx-Rx pair in the main road, which is illustrated in Figure 3. The average MAE for the duration of RF Jammer Behavior 1 is approximately 13% worse than the optimal value.

6.4. Results of RF Jammer Behavior 2. For the second evaluation scenario, we assume that the pair Tx-Rx travels with constant speed (48 Km/h), which is almost the same as the maximum speed of the jammer (50 Km/h) (see Figure 5). The jammer continuously transmits a random jamming symbol to the receiver. The start time of the jamming attack is at 18 sec during which the SINR appears to be decreasing from 5 dB to zero while Δu starts to increase from 20 rad∗m/s to the "peak" value of Δu. The time that is needed for the Jx to approach the pair Tx-Rx is approximately $\Delta t_{\text{eff}} = 18$ sec. After that time, the jamming attack clearly has perfect results for 18 sec; from the 18 sec of the simulation until 36 sec, after that SINR increases more than 5 dB.

If the Δu slope is positive, the Jx approaches the Rx, whilst if it goes to zero, Jx is removed from the effective zone of communication between the Tx and the Rx. The "black hole" in the communication between the Tx and the Rx is around the time interval (18 sec–36 sec), during which the MAE value increases to approximately 18% from the optimal MAE value.

In Figure 5, we can see that the average MAE for the complete duration of RF Jammer Behavior 2 is

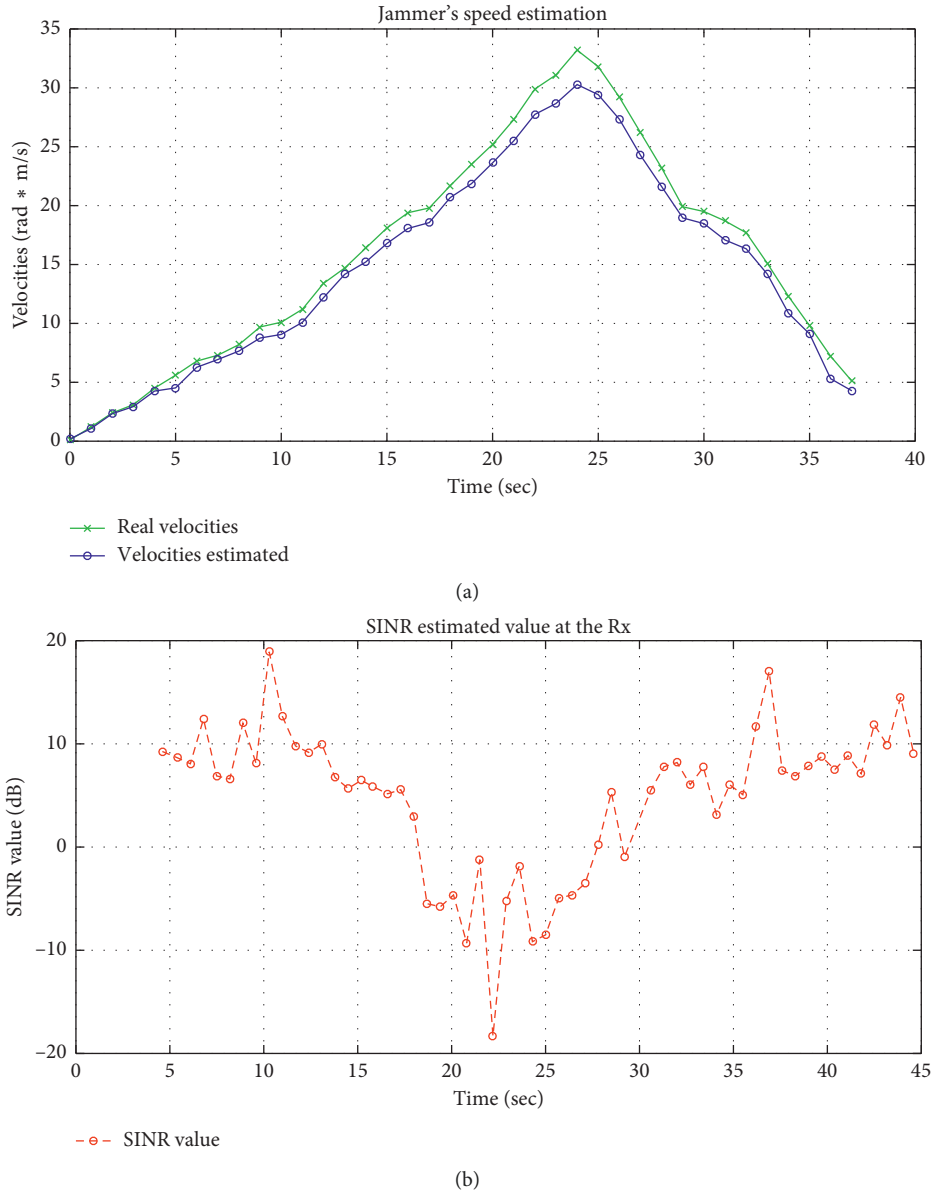

FIGURE 4: RF Jammer Behavior 1 results: RSEA with speed of Tx-Rx (50 Km/h) and Jx maximum speed (60 Km/h) and a *simplified* form of the jamming signal. (a) Δu vs. estimated $\widehat{\Delta u}$ to time. (b) SINR (dB) vs. time (sec).

approximately 10% worse than the optimal value, as it is shown also in Figure 6.

6.5. MAE Comparison between RF Jammer Behavior 1 and RF Jammer Behavior 2. The overall comparison of the MAE results between RF Jammer Behavior 1 (Jammer 1) and RF Jammer Behavior 2 (Jammer 2) is summarized in Table 4. Figure 6 shows that there is a quite small MAE, only 15% greater than the MAE value at the start and end of simulation. However, when the jammer approaches the receiver, the MAE shows an increase of about 23% from the optimal value for RF Jammer Behavior 1 and 18% for RF Jammer Behavior 2. The phenomenon of the larger MAE at the time of the jamming attack for RF Jammer Behavior 1 compared to that of RF Jammer Behavior 2 is attributed to the fast varying nature of the Δu metric because it changes with a higher rate, and thus, the channel between the Jx and the Rx changes frequently too. So, the longer the duration of the jamming attack lasts, the better the MAE results of the proposed RSEA are.

In order to test our previous results under more generic scenarios, the average MAE is estimated for different jammer speed values and different number of "hidden" nodes that are located at the edge of the CS range of the Tx – Rx pair. Specifically, we conducted several simulations, for a range of jammer speed values between $[47, 97]$ Km/h and number of "hidden" nodes between $[0, 50]$ nodes. For these parameters, the MAE value increases at approximately 20% from the reference zero MAE value with the maximum jammer speed value (see Figure 7(b)) and at approximately19.2% from the same reference value with the

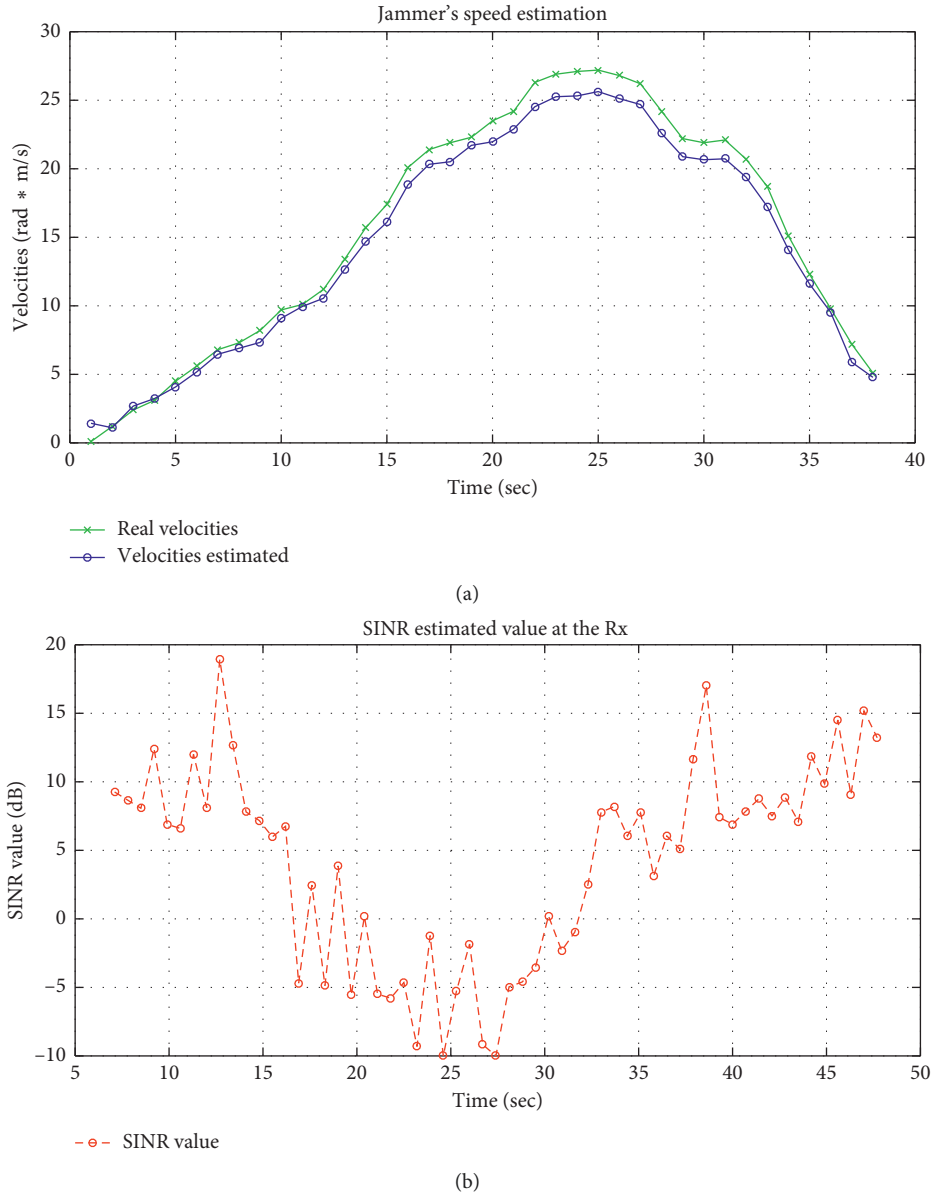

Figure 5: RF Jammer Behavior 2: RSEA with speed of Tx-Rx (48 Km/h) and Jx maximum speed (50 Km/h) and *simplified jamming signal* form. (a) Real Δu vs. estimated $\widehat{\Delta u}$ to time. (b) SINR (dB) vs. time (sec).

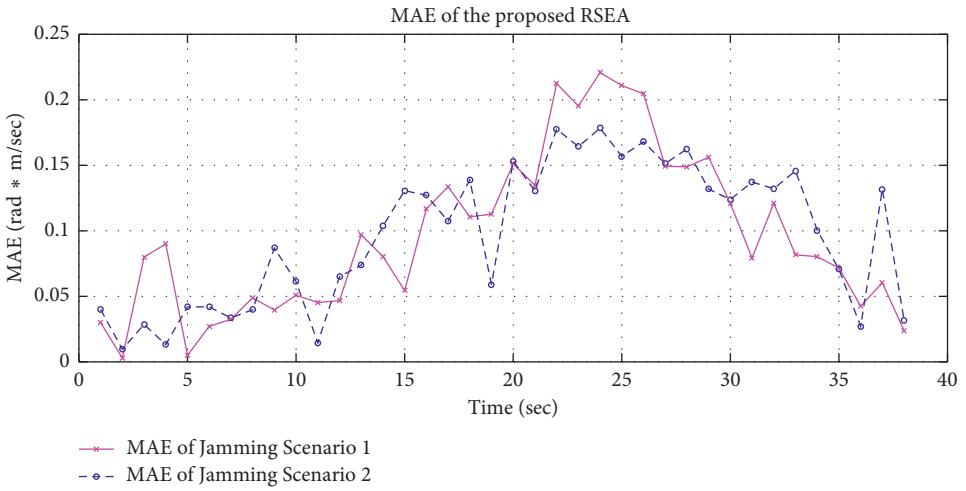

Figure 6: Instantaneous MAE comparison between RF Jammer Behavior 1 and RF Jammer Behavior 2 with *simplified jamming signal* form.

Table 4: RF Jammer Behavior comparison results of MAE (%) increase from the optimal zero MAE reference point.

Time intervals	MAE (Jammer 1)	MAE (Jammer 2)
"Black hole" of communication	23%	18%
Δt_{eff}	8%	6%
Overall simulation time	13%	10%

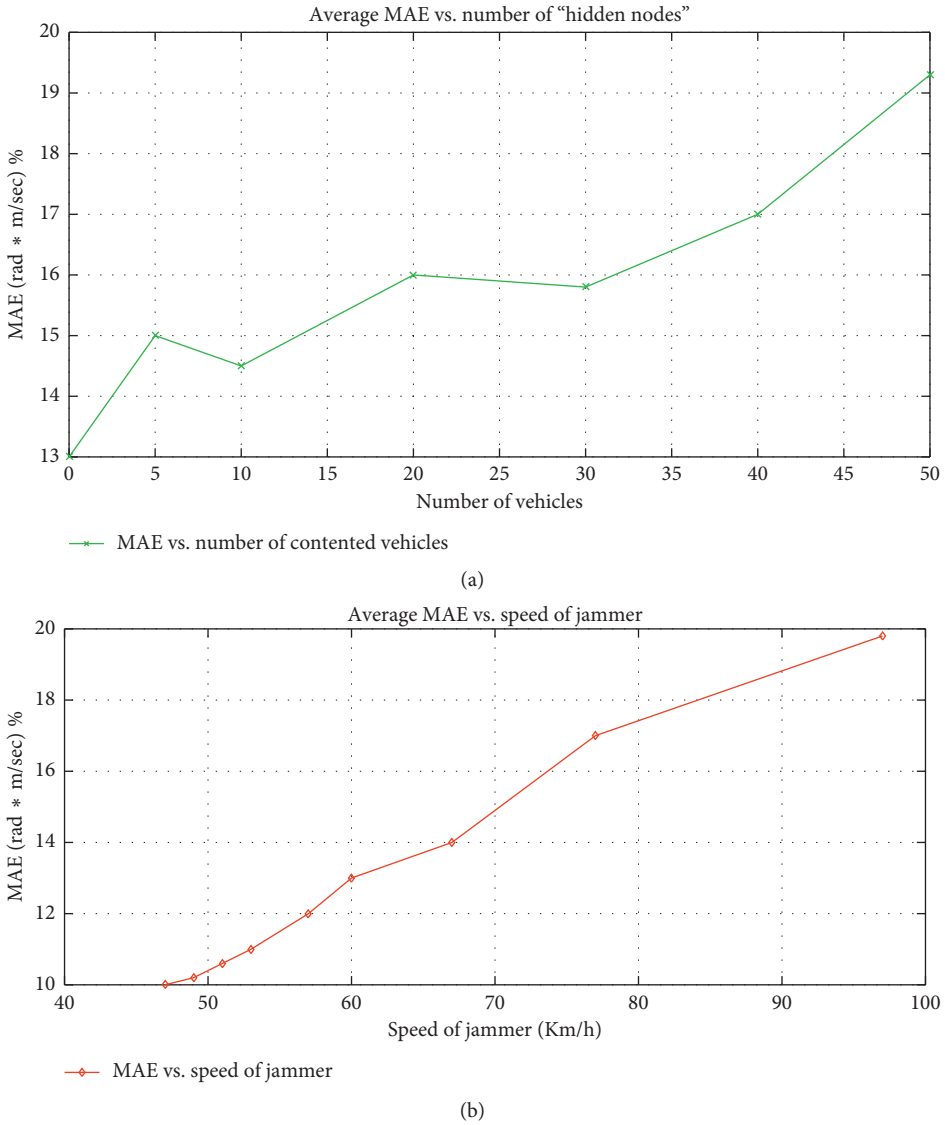

Figure 7: Average MAE (%) increase from the optimal zero MAE reference point with different evaluation parameters: the MAE of the proposed RSEA with different number of nodes for the contention window of the MAC back-off procedure for the wireless channel between Tx-Rx and different jammer's speed values. (a) Average MAE (%) vs. different number of "hidden" nodes. (b) Average MAE (%) vs. range of jammer's speed values (Km/h).

maximum number of "hidden" nodes, which is 50 nodes (see Figure 7(a)). For values greater than 67 km/h regarding the speed metric and 30 "hidden" nodes, the MAE was increasing with a higher rate. For smaller values of these two "side effect" values, the increase of MAE value is negligible. So these simulation results indicate that the back-off MAC/EDCA algorithm, using a safety-related high priority channel for the communication between Tx – Rx, does not affect considerably the performance of the speed estimation algorithm. The jammer's speed increase also affects but not significantly the proposed RSEA.

7. Discussion

In Section 6, we tested our proposed RSEA under different SINR values in order to represent realistic conditions. When there is a decreased steep slope of the SINR values, a jamming attack is conducted in the area. At the same time,

the relative speed value Δu, as defined in (4), presents an increased steep slope, indicating a jamming attack. Furthermore, when the jammer approaches the receiver, the MAE of the RSEA presents a significant increase due to the packet loss of the pilots sent by the Tx to Rx due to the presence of jammer. This results in the incorrect estimation of the stochastic V2V channel between Jx and Rx, increasing also the corresponding MAE of the Δu value.

V2X communication generally uses broadcast messages, but in this paper, we use unicast RF communication between two nodes in order to perform jammer's speed estimation. This type of communication is supported for advanced safety applications of autonomous vehicles by the Qualcomm's Cellular Vehicle-to-Everything (C-V2X) technology [57]. The target of this paper is to evaluate the performance of the RSEA for a pair of moving nodes with limited conditions, having as a future objective to be used in a real-life VANET scenario for more than one pair of nodes. Peer-to-peer networks in VANETs are studied lately in many other works [58–61], focusing mostly on social networks message exchange, cooperative caching, or unicast video streaming.

Relative speed estimation results from our proposed RSEA can be collected from a Trusted Central Authority (TCA) that exists in the area. Analyzing these collected data records, the TCA makes deductions based on the SINR value, notifies approaching vehicles, and even proposes jamming-free routes [62].

8. Conclusion and Future Work

In this paper, we presented an algorithm for estimating the combined value Δu of the relative speed between Rx and Jx in combination with the AOP of the Jx, during a jamming attack. A *simplified jamming signal* is sent to the receiver by the jammer that contains an unknown symbol to the receiver K times. The proposed relative speed metric can capture both the speed of the jammer and its direction relative to the Tx-Rx movement. By predicting the above value, we can understand jammer's behavior, for which Rx does not have any information except for the combined signal that is received from Tx and the interference caused by the attacker. Our proposed RSEA uses the physical metric of Δu from RF communication Tx − Rx in order to estimate the direction of the attacker. This metric is combined with the SINR value from the hardware (physical layer) in order for a real-life VANET scenario to be simulated. The MAE measured is being approximately only 10% worse compared to the optimal zero MAE value under different jamming attach scenarios.

As future work, we plan to combine RSEA with other metrics from the PHY layer or the network layer, such as SINR, for developing an accurate cross-layer jamming detection scheme. The detection scheme will be capable of dealing with more than one pair of nodes that communicate in a broadcast form. This combined metric can be also used as an extra feature in a machine learning approach (see [63]), in which the vehicles of the area can be classified as cooperative or malicious, thereby forming a trusted vehicular network. The usage of the relative speed metric can also reduce false alarms and can provide additional information about the future position of a Jx, such as the time that the attacker will approach the effective zone of communication. The above information extracted from our channel-based Jx-Rx analysis can decrease false alarms compared to jamming prediction schemes that are based only on the 802.11p PHY/MAC-related metrics (see the DJAVAN in [64]), concluding the physical geographical topology of the attacker. Last but not least, this metric is appropriate for a variety of jamming attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] G. Topham, "Self-driving cars could provide 62bn boost to uk economy by 2030," 2019, https://www.theguardian.com/technology/2019/apr/04/self-driving-cars-could-provide-62bn-boost-to-uk-economy-by-2030-brexit.

[2] M. Scribner, "Authorizing automated vehicle platooning," 2019, https://cei.org/content/authorizing-automated-vehicle-platooning-2019.

[3] S. Santini, A. Salvi, A. S. Valente, A. Pescapè, M. Segata, and R. L. Cigno, "Platooning maneuvers in vehicular networks: a distributed and consensus-based approach," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 1, pp. 59–72, 2019.

[4] M. Gerla, E. K. Lee, G. Pau, and U. Lee, "Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds," in *Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT)*, March 2014.

[5] J. Jo and M. Gerla, "Internet of vehicles and autonomous connected car—privacy and security issues," in *Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, Canada, July-August 2017.

[6] Z. Chen and B. B. Park, "Preceding vehicle identification for cooperative adaptive cruise control platoon forming," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2019.

[7] Q. Abdul, A. Raja, G. D. Nandan, and S. Harish, "A novel mechanism of detection of denial of service attack (DoS) in VANET using malicious and irrelevant packet detection algorithm (MIPDA)," in *Proceedings of the International Conference on Computing, Communication & Automation*, pp. 414–419, Noida, India, May 2015.

[8] P. Basaras, I. Belikaidis, L. Maglaras, and D. Katsaros, "Blocking epidemic propagation in vehicular networks," in *Proceedings of the 2016 12th Annual Conference on Wireless On-Demand Network Systems and Services (WONS)*, pp. 1–8, IEEE, Cortina d'Ampezzo, Italy, January 2016.

[9] Y. Awais, L. Asim, R. F. Babiceanu, M. Leandros, and Y. Onaiza, "Architectural and information theoretic perspectives of physical layer intruders for direct sequence spread spectrum systems," *Computers and Security*, vol. 70, pp. 124–143, 2017.

[10] E. Zandi and G. Azemi, "IF-based velocity estimation of the mobile units in micro-cellular systems with non-isotropic scattering distribution," in *Proceedings of the 2009 IEEE 70th Vehicular Technology Conference Fall*, Anchorage, AK, USA, September 2009.

[11] S. Malebary and W. Xu, "A survey on jamming in vanet," *International Journal of Scientific Research and Innovative technology*, vol. 2, no. 1, 2015.

[12] 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, 2015.

[13] M. Pajic and R. Mangharam, "Spatio-temporal techniques for antijamming in embedded wireless networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, p. 2010.

[14] A. Wood, J. Stankovic, and G. Zhou, "DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *Proceedings of the 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, San Diego, CA, USA, June 2007.

[15] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: reactive jamming in wireless networks: how realistic is the threat?," in *Proceedings of the Fourth ACM Conference on Wireless Network Security*, Hamburg, Germany, June 2011.

[16] D. Nguyen, C. Sahin, B. Shishkin, N. Kandasamy, and K. R. Dandekar, "A real-time and protocol-aware reactive jamming framework built on software-defined radios," in *Proceedings of the 2014 ACM workshop on Software radio implementation forum—SRIF '14*, Chicago, IL, USA, August 2014.

[17] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of ieee 802.11 under jamming," in *Proceedings of the IEEE INFOCOM 2008—The 27th Conference on Computer Communications*, Phoenix, AZ, USA, April 2008.

[18] A. Marttinen, A. Wyglinski, and R. Jantti, "Statistics-based jamming detection algorithm for jamming attacks against tactical MANETs," in *Proceedings of the 2014 IEEE Military Communications Conference*, Baltimore, MD, USA, October 2014.

[19] M. Strasser, B. Danev, and S. Capkun, "Detection of reactive jamming in sensor networks," *ACM Transactions on Sensor Networks*, vol. 7, no. 2, pp. 1–29, 2010.

[20] T. C. Clancy, "Efficient ofdm denial: pilot jamming and pilot nulling," in *Proceedings of the 2011 IEEE International Conference on Communications (ICC)*, Kyoto, Japan, June 2011.

[21] S. D'Oro, E. Ekici, and S. Palazzo, "Optimal power allocation and scheduling under jamming attacks," *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1310–1323, 2017.

[22] K. Xu, Q. Wang, and K. Ren, "Joint ufh and power control for effective wireless anti-jamming communication," in *Proceedings of the 2012 Proceedings IEEE INFOCOM*, Orlando, FL, USA, March 2012.

[23] J. S. Sousa and J. P. Vilela, "Uncoordinated frequency hopping for secrecy with broadband jammers and eavesdroppers," in *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, London, UK, June 2015.

[24] P. Gu, C. Hua, R. Khatoun, Y. Wu, and A. Serhrouchni, "Cooperative anti-jamming relaying for control channel jamming in vehicular networks," in *Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference*, Singapore, December 2017.

[25] S. Feng and S. Haykin, "Cognitive risk control for anti-jamming v2v communications in autonomous vehicle networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9920–9934, 2019.

[26] R. T. Rajan, G. Leus, and A.-J. van der Veen, "Relative velocity estimation using multidimensional scaling," in *Proceedings of the 2013 5th IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, St. Martin, France, December 2013.

[27] J. Weng, R. Yuan, R. Wang, and C. Wang, "Freeway travel speed calculation model based on ETC transaction data," *Computational Intelligence and Neuroscience*, vol. 2014, Article ID 174123, 7 pages, 2014.

[28] B. Kusy, A. Ledeczi, and X. Koutsoukos, "Tracking mobile nodes using RF Doppler shifts," in *Proceedings of the 5th international conference on Embedded networked sensor systems—SenSys '07*, pp. 29–42, Sydney, Australia, 2007.

[29] A. E. Assaad, M. Krug, and G. Fischer, "Distance and vehicle speed estimation in OFDM multipath channels," in *Proceedings of the 2016 21st International Conference on Microwave, Radar and Wireless Communications (MIKON)*, Krakow, Poland, May 2016.

[30] E. Adegoke, J. Zidane, E. Kampert, C. R. Ford, S. A. Birrell, and M. D. Higgins, "Infrastructure Wi-Fi for connected autonomous vehicle positioning: a review of the state-of-the-art," *Vehicular Communications*, vol. 20, Article ID 100185, , 2019.

[31] N. Kassem, A. E. Kosba, and M. Youssef, "RF-based vehicle detection and speed estimation," in *Proceedings of the 2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, Yokohama, Japan, May 2012.

[32] W. Bo, "Realization and simulation of DOA estimation using MUSIC algorithm with uniform circular arrays," in *Proceedings of the 2006 4th Asia-Pacific Conference on Environmental Electromagnetics*, pp. 908–912, Dalian, China, August 2006.

[33] C. Tepedelenlioglu and G. B. Giannakis, "A spectral moment approach to velocity estimation in mobile communications," in *Proceedings of the 2000 IEEE Wireless Communications and Networking Conference. Conference Record (Cat. No.00TH8540)*, Chicago, IL, USA, September 2000.

[34] Y. R. Zheng and C. Xiao, "Mobile speed estimation for broadband wireless communications over Rician fading channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 1–5, 2009.

[35] G. Chandrasekaran, T. Vu, A. Varshavsky et al., "Vehicular speed estimation using received signal strength from mobile phones," in *Proceedings of the 12th ACM International Conference on Ubiquitous Computing—Ubicomp '10*, pp. 237–240, Copenhagen, Denmark, 2010.

[36] P. K. Pedapolu, P. Kumar, V. Harish et al., "Mobile phone user's speed estimation using WiFi signal-to-noise ratio," in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing—Mobihoc'17*, Chennai, India, July 2017.

[37] B. Kusy, A. Ledeczi, and X. Koutsoukos, "SNR-independent velocity estimation for mobile cellular communications systems," in *Proceeding of the IEEE International Conference on Acoustics Speech and Signal Processing*, pp. 29–42, Honolulu, HI, USA, April 2007.

[38] A. Abdelaziz, C. E. Koksal, and H. El Gamal, "On the security of angle of arrival estimation," in *Proceedings of the 2016 IEEE*

Conference on Communications and Network Security (CNS), pp. 109–117, Philadelphia, PA, USA, October 2016.

[39] J. A. Jahanshahi and S. A. Ghorashi, "Doppler shift estimation and jamming detection for cellular networks," *Australian Journal of Basic and Applied Sciences*, vol. 4, no. 12, pp. 6590–6597, 2010.

[40] M. G. Moazzam, M. R. Haque, and M. S. Uddin, "Image-based vehicle speed estimation," *Journal of Computer and Communications*, vol. 7, no. 6, pp. 1–5, 2019.

[41] O. Bourja, A. Maach, Y. Zennayi, F. Bourzeix, and T. Guerin, "Speed estimation using simple line," *Procedia Computer Science*, vol. 127, pp. 209–217, 2018.

[42] Z. Zhang, X. He, and H. Yuan, "An anti-interference traffic speed estimation system with wireless magnetic sensor networks," *IEEE Transactions on Industrial Informatics*, 2019.

[43] H. Abuella, F. Miramirkhan, S. Ekin, M. Uysal, and S. Ahmed, "ViLDAR—visible light sensing-based speed estimation using vehicle's headlamps," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 10406–10417, 2019.

[44] J. Wang, J. Tong, Q. Gao, Z. Wu, S. Bi, and H. Wang, "Device-free vehicle speed estimation with WiFi," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8205–8214, 2018.

[45] M. Spuhler, V. Lenders, and M. Wilhelm, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1593–1903, 2014.

[46] S. Munazza, K. A. Muazzam, K. U. Shafiq, and N. A. Saqib, "Detection and prevention of distributed denial of service attacks in VANETs," in *Proceedings of the 2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 970–974, Las Vegas, NV, USA, December 2016.

[47] 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.

[48] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, Cambridge University Press, Cambridge, UK, 2005.

[49] F. A. F. Edris, A. G. Elsid, and M. H. M. Nerma, "A study of channel estimation in fast fading environments," *International Journal of Scientific & Technology Research*, vol. 4, no. 8, 2015.

[50] M. Boban, J. Barros, and O. K. Tonguz, "Geometry-based Vehicle-to-Vehicle channel modeling for large-scale simulation," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4146–4164, 2014.

[51] R. Barrett, *Wi-fi in the Car: How to Meet the Concurrent Needs of Multiple Systems and Applications*, Cypress Semiconductor, San Jose, CA, USA, 2017, http://www.eenewseurope.com/design-center/wi-fi-car-how-meet-concurrent-needs-multiple-systems-and-applications-0.

[52] A. Sassi, F. Charfi, L. Kamoun, Y. Elhillali, and A. Rivenq, "A symbol-based estimation technique for inter-vehicular communication performance optimization," *IJCSI International Journal of Computer Science Issues*, vol. 10, 2014.

[53] G. M. Abdalla, M. A. Abu-Rgheff, and S.-M. Senouci, "An adaptive channel model for VBLAST in vehicular networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 328706, , 2009.

[54] A. Nima, B. A. Tabatabaie, and A. G. Dempster, "Dynamic path loss exponent and distance estimation in a vehicular network using doppler effect and received signal strength," in *Proceedings of the Vehicular Technology Conference Fall*, pp. 1–5, Ottawa, Canada, September 2010.

[55] J. Nuckelt, M. Schack, and T. Kürner, "Deterministic and stochastic channel models implemented in a physical layer simulator for Car-to-X communications," *Advances in Radio Science*, vol. 9, pp. 165–171, 2011.

[56] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2011.

[57] Qualcomm, Accelerating C-V2X commercialization, 2017, https://www.qualcomm.com/documents/path-5g-cellular-vehicle-everything-c-v2x.

[58] F. M. Amine and A. Ahmed, "ESSPR: an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network," *Telecommunication Systems*, vol. 66, no. 3, pp. 481–503, 2017.

[59] K. Neeraj and L. Jong-Hyouk, "Peer-to-peer cooperative caching for data dissemination in urban vehicular communications," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1136–1144, 2014.

[60] R. Cristiano, B. Azzedine, H. S. Ramos, and A. A. F. Loureiro, "A reactive and scalable unicast solution for video streaming over VANETs," *IEEE Transactions on Computers*, vol. 64, no. 3, pp. 614–626, 2015.

[61] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in *Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 228–233, IEEE, Santorini Island, Greece, May 2019.

[62] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET: a survey," *Procedia Computer Science*, vol. 45, pp. 592–601, 2015.

[63] O. Punal, I. Aktas, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: design and experimental evaluation," in *Proceeding of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, Sydney, Australia, June 2014.

[64] 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.