Jammer Localization in the Internet of Vehicles: Scenarios, Experiments, and Evaluation

Ahmed Hussain*
Qatar University
Doha, Qatar
ahmed.hussain@qu.edu.qa

Nada Abughanam*
Qatar University
Doha, Qatar
nada.abughanam@qu.edu.qa

Savio Sciancalepore
Eindhoven University of Technology
Eindhoven, Netherlands
s.sciancalepore@tue.nl

Elias Yaacoub
Qatar University
Doha, Qatar
eliasy@ieee.org

Amr Mohamed
Qatar University
Doha, Qatar
amrm@qu.edu.qa

ABSTRACT

The Internet of Vehicles (IoV) paradigm aims to improve road safety and provide a comfortable driving experience for Internet-connected vehicles, by transmitting early warning and infotainment signals to Internet-connected vehicles in the network. The unique characteristics of the IoV, such as their mobility and pervasive Internet connectivity, expose such networks to many cyberattacks. In particular, jamming attacks represent a considerable risk to their performance, as they can significantly affect vehicles' functionality, possibly leading to collisions in dense networks. This paper presents a new scheme enabling the detection and localization of jamming attacks carried out within an IoV network. We consider several scenarios, e.g., where the Internet-connected vehicles and the jammer are statically positioned, as when parked on a street, moving in the same direction and with variable speeds, and moving in opposite directions. We leverage the physical-layer characteristics of the received signals, particularly the Received Signal Strength (RSS), and devise a solution minimizing the jammer localization error based on a set of antennas deployed on the vehicle. Specifically, we compute the power emitted by the jammer and received by the arrays of omnidirectional antennas and we use such values to estimate the location of the jammer in the previous-cited scenarios. Through an extensive simulation campaign, we provide a thorough study of our algorithm, evaluating the effect of several system and channel parameters on the measurement error. The results obtained for all scenarios show a significant localization accuracy, i.e., ranging from 0.23 meters to 13 meters, depending on the channel conditions.

CCS CONCEPTS

• **Networks** → *Network properties*; • **Mobile and wireless security**; • **Security and privacy** → **Systems security**;

*Both authors contributed equally to this research.

IoT '22, November 7–10, 2022, Delft, Netherlands

ACM ISBN 978-1-4503-9665-3/22/11…$15.00
https://doi.org/10.1145/3567445.3567463

KEYWORDS

Jammer Localization, Internet of Vehicles, Jamming, Physical-Layer Security, Vehicular Communications, Wireless Communications

ACM Reference Format:
Ahmed Hussain, Nada Abughanam, Savio Sciancalepore, Elias Yaacoub, and Amr Mohamed. 2022. Jammer Localization in the Internet of Vehicles: Scenarios, Experiments, and Evaluation. In *Proceedings of the 12th International Conference on the Internet of Things (IoT '22), November 7–10, 2022, Delft, Netherlands.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3567445.3567463

1 INTRODUCTION

Intelligent transportation systems have grown in popularity in both business and academics in recent years, and manufacturers are developing vehicles to become more intelligent and interconnected in various ways [22]. These advancements will lead to some of the most significant improvements to mobility and transportation in the next few years [17]. They are primarily motivated to enhance road safety and driving conditions and offer vehicle entertainment services. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, first standardized within the so-called Vehicular Ad-Hoc Network (VANET) scenario, are todays enriched to build the Internet of Vehicles (IoVs) paradigm, where Internet-connected vehicles exchange information among them and with the public Internet network. Like any wireless network, IoVs are prone to external and internal cyberattacks [29]. In this context, jamming attacks enable the adversary to disrupt ongoing communications occurring on the wireless channel, by simply injecting a powerful signal targeting the communication frequency. Jamming attacks can severely affect the quality and quantity of messages exchanged between vehicles. Low-cost Software Defined Radios (SDRs) such as HackRF One [5], equipped with open-source software such as GNU Radio [27], can be easily used to facilitate jamming attacks [28] This is achieved by scanning the wireless spectrum, identifying a particular bandwidth to be jammed, and finally transmitting a hindering signal increasing the interference at the receiver, causing frequent disconnections, and preventing the receiver from correctly decoding packets until the channel is idle again [23]. The messages exchanged within a IoVs network could contain invaluable data. For example, they can include the occurrence of an accident, road blockage ahead, and many other data that could be useful to the

driver [39]. Several jamming strategies are discussed in the literature [33], e.g., constant jamming, deceptive jamming, random jamming, and reactive jamming. Moreover, a few contributions addressed jamming mitigation and localization [7, 8], and some of them use the RSS to determine the jammer's location by estimating the distances between several nodes and the jamming source [9]. However, localizing a jammer in the Internet of Vehicle (IoV) scenario is challenging. Indeed, jammers can be either statically placed, e.g., on parked cars or infrastructure elements, or dynamically move in the area, e.g., when placed on a moving car. Thus, a solution for jamming localization in the IoV scenario should be able to distinguish between static and moving jamming by design, as well as to possibly track the jammer to take it down.

Contribution. In this paper, we provide the following contributions:

- We analyze adversarial jamming attacks carried out within a IoV scenario. In this setting, we propose a simple yet effective methodology to localize a constant jamming attack, leveraging one or multiple smart vehicles.
- We utilize physical-layer properties, namely, the RSS of the signal at the receiver(s), and propose a strategy that minimizes the jamming localization error based on a set of antennas deployed on the vehicle's body.
- The RF power received by one or more vehicles equipped with arrays of omnidirectional antennas is estimated and used to determine the position of the jammer.
- We investigate several different scenarios taking into account realistic and extreme conditions, as well as complex and harsh operating environments, i.e., where the vehicles and jammer are statically positioned, moving with the same speed and direction, moving with variable speeds, and moving in opposite directions.
- We conduct an extensive simulation campaign to prove the effectiveness of the proposed approach, encompassing the path-loss model with different shadowing (σ) and environment values (γ), different number of vehicles, and different channel sampling frequencies, resulting in a localization error ranging from 0.23 meters to 13 meters, depending on the channel conditions.
- Finally, we prove that it is possible to localize a jammer in the IoV scenario, even when mobile, with remarkable accuracy.

Paper Organization. The remainder of this paper is organized as follows: Section 2 discusses the system and the threat model. Section 3 illustrates the scenarios and localization methodology proposed in this paper. In Section 4, we explain and evaluate the performance of the proposed methodology. Section 5 addresses the relevant related work and compares our proposal with existing solutions. Finally, Section 6 wraps up the findings and results presented in this paper and illustrates future work.

2 SYSTEM AND THREAT MODEL

Figure 1 depicts the scenario presented in this work. We assume an IoV scenario, with Internet-connected vehicles communicating and exchanging different types of messages while moving in a given area. We also assume that a powerful jammer is deployed on a moving vehicle, to disrupt all types of communications between vehicles on a particular frequency (e.g., f = 2.4GHz, which is the frequency that IoVs operate at). However, as the communications between vehicles and Base Station (BS) of the cellular network use other frequencies (e.g., frequencies between 1920 and 1980 MHz to uplink data and frequencies between 2110 and 2170 MHz to downlink data), they are assumed not to be affected by the jamming activity. In addition, we assume that the adversary is hiding in plain sight, i.e., on a busy highway during rush hour. Depending on the vehicle position, it might (not) be directly in the line of sight with the jammer. We assume a constant jammer that constantly emits a powerful Additive White Gaussian Noise (AWGN) signal. We assume that this signal mainly blocks all communications between other vehicles, and hence, disables any form of communication on the frequency f between the surrounding vehicles located within the jamming radius. Furthermore, we emphasize that jamming affects only the communications among the vehicles operating on this particular frequency, and it does not affect the communications of the vehicles with the BS of the cellular network. Indeed, being Internet-connected, i.e., through a cellular network connection, the vehicles still can use the Internet connection to deliver information to an Internet-available server, in charge of performing the localization task. Note that, although feasible, using an SDR to jam the WiFi channels and the cellular network at the same time would require more complex and expensive hardware, not always feasible for an adversary. If the jammer targets several frequencies, e.g., GPS, to prevent the vehicle from knowing its current position, we assume that the vehicle can retrieve the last recorded coordinates

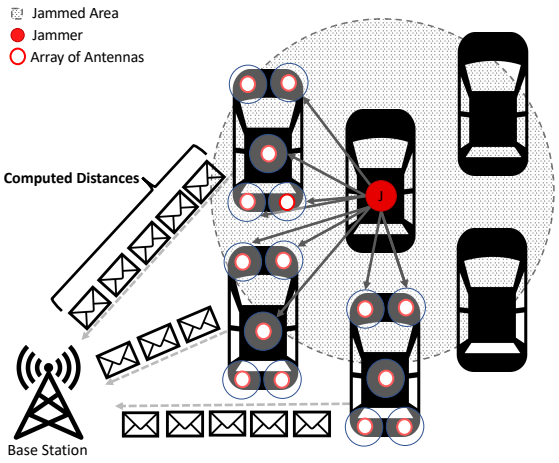


Figure 1: The scenario assumed in this work. An adversary carries out a jamming attack in an IoV network, to disrupt the vehicles' communications over the wireless channel. Thanks to the availability of the Internet connection, several vehicles collaborate to detect the jamming and perform a channel measurement through several deployed arrays of antennas, estimating the distance from the jamming vehicle. Once the distances are computed by each vehicle, it is then transmitted to the base station to be delivered to the server to perform the localization.

Table 1: Notations used throughout the paper.

Notation	Description
f_0	Channel Central Frequency.
N	Number of channel readings/samples.
$\mathcal{P}_t$	Power Transmitted.
$\mathcal{G}$	Grid Size.
σ	Logarithmic Standard Deviation of the Shadowing.
γ	Path-loss Exponent.
$\mathcal{RS}$	Receiver Sensitivity.
$\mathcal{L}$	Vehicles Coordinates.
$\mathcal{A}$	Jamming Vehicles Coordinates.
$\mathcal{T}$	Time Step.
$\mathcal{C}$	Number of Vehicles.
$\mathcal{S}$	Number of Simulations.

and provide them to the Internet-connected server. We aim to localize the mobile jammer by deploying several arrays of antennas on a smart vehicle. In brief, such arrays of antennas can utilize the power emitted by the jammer to estimate its location.

Path-loss Model. In this work, we adopt the well-known path-loss model, as depicted in Eq. 1. Such a model is used to estimate the power $P_{RX}(d_i)$ received by each omnidirectional array of antennas at a distance d_i from the source (i.e., the jammer), so as to estimate d_i based on the received power. P_{TX} represents the transmission power of the jammer, $P_L(d_0)$ represents the path loss at the reference distance d_0 (i.e., the length of the path) computed by leveraging the Free Space model [6, 12], γ is the path loss exponent, and X_g defines the attenuation due to the flat fading, modeled as a Gaussian random variable with zero mean and standard deviation σ.

$$P_{RX}(d_i)[dBm] = P_{TX} - P_L(d_0) - 10 \cdot \gamma \cdot log_{10}\frac{d_i}{d_0} - X_g \quad (1)$$

Finally, we summarize the notation used in this paper in Table 1.

3 SCENARIOS AND JAMMER LOCALIZATION

In this section, we discuss our localization logic and describe the considered scenarios.

Distance Estimation. We adopt the inverse of the path loss model (Eq. 2) to estimate the distance between the jammer and the receiving antennas deployed on the vehicle(s). To this aim, we define the path loss $P_L(d_i)$ as the signal attenuation experienced by each antenna when receiving a wireless message transmitted by a source located at distance d_i from the jammer, i.e., $P_L(d_i) = P_{TX} - P_{RX}(d_i) - P_L(d_0)$.

$$d_i = d_0 \cdot 10^{\frac{PL(d_i)}{\gamma 10}} \quad (2)$$

Localization. We combine the distances $[d_1, ..., d_n]$ obtained from the ranging procedure (as computed by Eq. 2) to create an estimated position for the jammer $[x_J, y_J]$. We begin by linearizing the problem, using one antenna $[x_n, y_n]$ and its corresponding distance to the jammer (d_n) as a reference and subtracting it from the $n-1$ equations, generating a system of $n-1$ equations in the form of $Az = b$, generating the matrices (A and b) in Eq. 3.

$$A = -2 \cdot \begin{pmatrix} (x_1 - x_n) & (y_1 - y_n) \\ (x_2 - x_n) & (y_2 - y_n) \\ \vdots & \vdots \\ (x_{n-1} - x_n) & (y_{n-1} - y_n) \end{pmatrix}$$

$$z = \begin{pmatrix} x \\ y \end{pmatrix} \quad (3)$$

$$b = \begin{pmatrix} x_n^2 + y_n^2 - y_1^2 - x_1^2 + d_1^2 - d_n^2 \\ x_n^2 + y_n^2 - y_2^2 - x_2^2 + d_2^2 - d_n^2 \\ \vdots \\ x_n^2 + y_n^2 - y_{n-1}^2 - x_{n-1}^2 + d_{n-1}^2 - d_n^2 \end{pmatrix}$$

The jammers' position can be calculated by solving the system of equations $A \cdot z = b$, using the Linear Least Square (LLS) method [8, 38], as indicated in the Eq. 4.

$$z = [x_J, y_J]^T = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T b \quad (4)$$

In summary, the steps required for collecting samples and localization are the following.

(1) Each vehicle computes an estimate of the distance between its current location and the jammer, based on the power of the received signals at its antennas.
(2) The vehicles transmit the estimated distances to a nearby BS or Road Side Unit (RSU), namely, the infrastructure element, on a frequency/channel that is not affected by the jamming.
(3) The infrastructure element forwards the messages to a localization server over the Internet.
(4) The localization server uses its computational capabilities to combine all the received readings and build a system of equations, solve the system of equations, and estimate the jammers' location.

Once the jammer is localized, the authorities are notified of the location of the jammer and take any desired action, such as physically taking it down or blocking the traffic in the area.

Scenarios. In the following, we introduce the scenarios considered in our work. For each scenario, in each simulation run, we selected the grid size ($\mathcal{N}$) based on the total number of vehicles generated, multiplied by a fixed factor of 5. For instance, with 3 vehicles, we have a grid size of $15m^2$ (3 vehicles × 5 meters squared). The main idea is to test an area larger than the distribution of the vehicles.

Scenario 1: Stationary Vehicles and Jammer. This scenario is considered as the most basic one, as we assume that the vehicles ($\mathcal{L}$) and Jamming Adversary ($\mathcal{A}$) are stationary, i.e., not moving. This could occur when vehicles are queued in a jam-packed highway during rush hour, or when they are parked in a parking lot. We consider this scenario as the baseline one, whose results are to be compared with the other (more challenging) scenarios.

Scenario 2: Vehicles and Jammer Moving with the Same Direction and Speed. In this scenario, we assume that $\mathcal{L}$ and $\mathcal{A}$ are moving in the same direction and speed. $\mathcal{A}$ is assumed to be located within the same traffic lane or radius of $\mathcal{L}$, and continuously moving. The position for both vehicles ($\mathcal{A}$ and $\mathcal{L}$) is incremented by a constant value at each time step to mimic movement. For this scenario, we considered the speed of 50 kilometers/hour as the constant value. We emphasize that the specific value of the speed is not relevant for this scenario, since we consider that the vehicles are moving at the same speed and direction.

Scenario 3: Vehicles and Jammer Moving at Variable Speeds. As described in scenario 2, we assume $\mathcal{L}$ and $\mathcal{A}$ are moving in the same direction. However, in this scenario, the speed varies with time for both $\mathcal{L}$ and $\mathcal{A}$. We consider that there is a speed change probability of 0.5 at each time step, i.e., $\mathcal{L}$ or $\mathcal{A}$ change their moving speed. The initial speed for all vehicles is randomly generated, with a value between 50 and 80 kilometers/hour. The speed of $\mathcal{L}$ increases by 3-4 kilometers/hour, while the speed of $\mathcal{A}$ increases by 1-2 kilometers/hour over time.

Scenario 4: Vehicles and Jammer Moving in Opposite Directions. The final scenario assumes that $\mathcal{L}$ and $\mathcal{A}$ are moving in opposite directions at the same speed, as could be the case in a two-way street. The position of $\mathcal{L}$ is shifted in a given direction by a constant value, while the position of $\mathcal{A}$ is shifted in the opposite direction by the same constant value. As mentioned before, such a constant value depends on the speed of the vehicles, considered in this scenario as 50 kilometers/hour.

4 PERFORMANCE EVALUATION

We considered the four reference real-life scenarios described in the previous section, where jamming attacks are carried out within a randomly constructed vehicular network. We emphasize that, in each simulation, the vehicles (including the jammer) are deployed in random positions to ensure the effectiveness and fairness of the proposed localization scheme. We adopted the new Tesla Model S 2021 as our smart vehicle with the following dimensions: length = 4.907 meters, width = 1.964 meters, and height = 1.445 meters [1]. We assume that the antennas are installed and distributed on the vehicle body in five different locations, namely, the front (2 antennas), top (1 antenna), and back (2 antennas). The distance between the antennas deployed in the front is 1.964 meters. Similarly, the antennas on the back have the same distance. At the same time, the top antenna is at a distance of 2.672 meters with respect to the other antennas. The type of antennas used is assumed to be omnidirectional. The simulations were carried out on an Alienware Aurora Ryzen Edition, with an AMD Ryzen 9 3950X 16-core processor running at 3.49GHz, and 64GB RAM memory. We used MATLAB 2021a to run all the simulations. Table 2 summarizes the parameters used in the simulations. Note that some parameters are taken from reference papers in the jamming literature [8, 18]. To test the effectiveness of the proposed scheme, we ran 10,000 simulations per scenario, where in each scenario the channel is sensed 500 times (N), and for all the scenarios, we report our results together with the 95% confidence interval.

Algorithm 1: Scenario 3 simulation algorithm for estimating the Jammer position when γ is fixed.

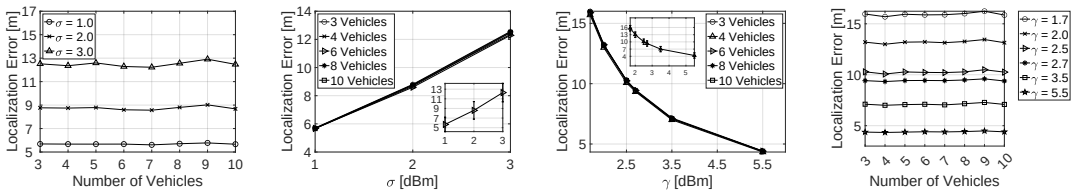
Input: $\mathcal{L}, \mathcal{A}, \mathcal{T}, \gamma, C, \mathcal{S}$;
Result: Estimated Jammer Position (x_J, y_J);

$\mathcal{A} \leftarrow \emptyset$;
$\mathcal{L} \leftarrow \emptyset$;
$\gamma \leftarrow 5.5$;
$\mathcal{A} \leftarrow$ *generateCoordinatesSet(1)*;
$\mathcal{L} \leftarrow$ *generateCoordinatesSet*($\mathcal{S}$);
// For each value of sigma
for $i \leftarrow 1$ **to** $|\sigma|$ **do**
  // For each timestep
  for $j \leftarrow 1$ **to** $|\mathcal{T}|$ **do**
    // For each number of simulations
    for $k \leftarrow 1$ **to** $|\mathcal{S}|$ **do**
      // Generate a random number between 1 and 4
      $r \leftarrow$ `randi(4, 1)`;
      // Increasing the car/jammer speed logic
      if $r > 2$ **then**
        car_speed $\leftarrow$ j + r;
        jammer_speed $\leftarrow$ j;
      else
        car_speed $\leftarrow$ j;
        jammer_speed $\leftarrow$ j + r;
      end
      // Jammer location estimation
      $(x_J, y_J) \leftarrow$ `JammerLocalizerV2X(`$l_{k,1}$`, (`$l_{k,2}$ `+ car_speed), `$a_{k,1}$`, (`$a_{k,2}$ `+ jammer_speed), `γ`, `σ_i`);`
    end
  end
end

Table 2: Simulation Parameters.

Notation	Value
f_0	2.4 GHz
N	500
$\mathcal{P}_t$	45 dBm
$\mathcal{G}$	5 × Number of Vehicles
σ	[0.1, ..., 3]
γ	[1.7, ..., 5.5]
$\mathcal{RS}$	-60 dBm
$\mathcal{T}$	10
C	[3, ..., 10]
$\mathcal{S}$	10,000

Simulation results are obtained for all four scenarios, with the second, third, and fourth considered more challenging due to their mobility factor, which could also be more representative or actual IoVs scenario. Furthermore, we considered different physical surrounding environments, e.g., by increasing the noise level and the attenuation of the propagated signal from the jammer due to the



(a) (b) (c) (d)

Figure 2: Simulation results for scenario 3. (a) represents the localization error as a function of the localization vehicles when $\sigma \in [1, 2, 3]$. Similarly, (b) shows the localization error as a function of σ (c) depicts the localization error as a function of γ (d) illustrates the localization error as a function of the localization vehicle when $\gamma \in [1.7, 2, 2.5, 2.7, 3.5, 5.5]$.

environmental effects. We first evaluated the jammer location estimation error while varying the number of used vehicles for localization. Moreover, we evaluated different values of σ and γ. to mimic different channel conditions. Specifically, as described in Algo. 1, the jammer localizer function (`JammerLocalizerV2X(`$l_{k,1}$`, (`$l_{k,2}$ `+ car_speed), `$a_{k,1}$`, (`$a_{k,2}$ `+ jammer_speed),` γ`,` $\sigma_{i\in\{0.1,\ldots,3\}}$`)` perform samples acquisition for a predefined number of times (N = 500). Then, the algorithm estimates the distances for each sample using the formula in Eq. 2. The distances are then assumed to be sent to the BS (or RSU) to perform the localization as illustrated in Eq. 3 and 4. The algorithm summarized above and detailed in Algo. 1 is adapted to work also in the other scenarios, with minor changes to the localization logic. In each simulation, the vehicles are uniformly and randomly distributed across the grid, as well as the jammer.

We start our analysis by considering the impact of the shadowing effect on the localization accuracy, considering the variance σ of the path-loss model in the range 0.1 dBm $\leq \sigma \leq$ 3 dBm, the path-loss exponent in the range of 1.7 dBm $\leq \gamma \leq$ 5.5 dBm, and a number of deployed vehicles (C) in the range ($3 \leq C \leq 10$). Figure 2 (a) shows the localization error as a function of the number of vehicles used for localization where the value of σ is set to 1, 2, and 3, respectively. The localization error is computed as the Euclidean distance between the actual location of the jammers and the location predicted through our solution. The findings consider the average value of the 10,000 simulation runs and 500 jamming signal measurements. First, note that the number of vehicles does not impact on the localization accuracy. At the same time, when increasing the shadowing value (σ), the localization error increases, even when increasing the number of localization vehicles. Indeed, as the shadowing value increases, the received power fluctuates more and is attenuated further due to the obstacles located between the jammer and the localization vehicle, leading to less accurate localization. Figure 2(b) illustrates the localization error as a function of different σ values. It can be seen that when increasing the σ value, the localization error increases. However, increasing the number of vehicles participating in the jammer localization procedure reduces the error. The low rate is due to the increasing sigma value, which increases the signal attenuation. Additionally, instead of using 10 vehicles to perform the localization, 8 vehicles are sufficient to estimate the jammer location accurately. Similarly, Figure 2 (b) shows a similar behavior such that using 6 vehicles is sufficient to estimate the jammer

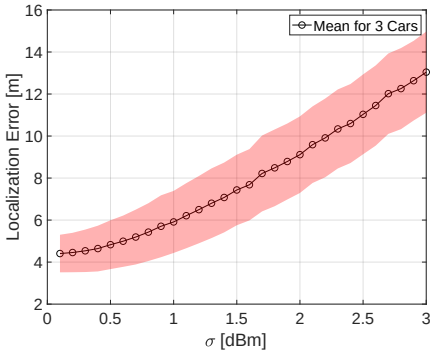


Figure 3: Confidence Interval of the Localization Error as a function of σ (0.5 dBm $\leq \sigma \leq$ 3 dBm) when using 3 vehicles and γ is 5.5. The error bound is less when $\sigma \leq 1$. When $\sigma > 1$, the error bound increases.

location. Figure 2 (c) depicts the localization error as a function of γ with a certain number of vehicles. Despite increasing the γ value, the localization error decreases regardless of the number of vehicles used. Figure 2 (d) represents the localization error as a function of the number of vehicles with different γ values. It is clearly shown that the localization error significantly decreases with the increase of the value of γ. Figure 3 shows the confidence interval of the localization error as a function of σ when using 3 vehicles. The error is the least when σ is ≤ 1, and it increases with the increase of σ. Tables 3, 4, and 5 address the results obtained for each of the considered scenarios. We considered using 3 and 10 vehicles in each scenario, i.e., the minimum and the maximum number of vehicles used in all scenarios. In scenarios 1, 2, 3, and 4, performances do not change when using 3 or 10 vehicles. For example, the margin of error between using 3 and 10 is 0.34 meters in scenario 1 when γ is set to 5.5 and σ is 3. Such margin is sufficient and negligible to localize the jammer accurately without using 10 vehicles. Another example is scenario 3, where a mobile scenario is considered, the jammer and localization vehicles are moving at different speeds, and apart from each other in a harsh/complex environment (γ = 5.5), the localization error difference between using 3 and 10 vehicles is 0. Further, in scenario 4, the maximum

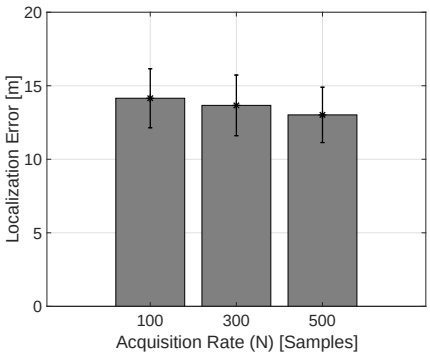


Figure 4: Localization error as a function of the acquisition rate (N) when γ = 5.5, σ = 3, and C is set to 7 in scenario 1. When increasing the number of times the channel is read (N), the less the localization error.

Table 3: Localization error as a function of γ when σ = 0.32, and σ when γ = 5.5 associated with the minimum and maximum number of vehicles in scenario 1.

Number of Vehicles	γ	Error [m]	σ [dBm]	Error [m]
3	2.00	13.73	1.00	6.01
3	3.50	7.36	2.00	9.48
3	5.50	4.61	3.00	13.37
10	2.00	13.80	1.00	5.97
10	3.50	7.48	2.00	9.15
10	5.50	4.66	3.00	13.03

Table 4: Localization error as a function of γ when σ = 0.32, and σ when γ = 5.5 associated with the minimum and maximum number of vehicles in scenario 2.

Number of Vehicles	γ	Error [m]	σ [dBm]	Error [m]
3	2.00	13.82	1.00	5.96
3	3.50	7.42	2.00	9.26
3	5.50	4.60	3.00	13.35
10	2.00	13.85	1.00	6.00
10	3.50	7.45	2.00	9.21
10	5.50	4.58	3.00	13.32

localization error is 0.23 meters when γ is set to 5.5 and σ is 3. Thus, this proves that the localization accuracy remains similar in harsh environments, even when increasing the number of vehicles used. Finally, in Fig. 4, we evaluated the effect of the number of samples available for localization on the jammer estimation accuracy. We observe that increasing the number of samples acquired on the channel improves the localization accuracy, reducing the localization error. Indeed, the higher the number of samples, the higher the chance that the estimator finds a better local minimum point, reducing the final estimation error.

Table 5: Localization error as a function of γ when σ = 0.32, and σ when γ = 5.5 associated with the minimum and maximum number of vehicles in scenario 4.

Number of Vehicles	γ	Error [m]	σ [dBm]	Error [m]
3	2.00	12.61	1.00	6.04
3	3.50	6.76	2.00	9.28
3	5.50	4.18	3.00	13.37
10	2.00	12.51	1.00	5.91
10	3.50	6.76	2.00	9.10
10	5.50	4.17	3.00	13.14

5 RELATED WORK

This section summarizes the contributions in the current literature, cross-comparing such solutions with ours.

5.1 Jamming Localization

Several techniques to localize a jammer are discussed in the literature, using metrics such as Angle of Arrival (AoA), Phase of Arrival (PoA), Direction of Arrival (DoA), RSS, and Packet Delivery Ratio (PDR) [7]. Wang *et al.* [37] presented a mobile jammer localization and tracking scheme to track a mobile jammer in a multi-hop wireless network, based on four stages: a selection of initial monitoring nodes, the determination of cooperative nodes, triangulation localization, and the handover of the monitoring group. Pelechrinis *et al.* [25] presented a distributed jammer localization algorithm based on gradient descent. As the PDR is highest farther away from the jammer, each node selects the neighbor that has the lowest PDR as the locally optimal choice. In [40], the authors proposed a multi-jammer localization algorithm that is based on alternating iteration and Gravitational Search Algorithm (GSA). The proposed method first uses a region growth algorithm to estimate the number of jammers. Then it estimates the jammers' positions iteratively using a combination of alternating iteration and GSA without relying on the distance between nodes or the shape of the jamming area. Fan *et al.* [4] proposed an Antenna Identification and Localization of the Jammer (AILJ) method that is based on the network topology. A collection protocol first gathers information about the nodes, whereas an identification protocol then classifies the type of the jammers' antenna. The jammer's position is estimated via a range-free method depending on the antenna. The authors in [10] utilized RSS to locate an active jammer. The proposed scheme requires the nodes to increase the power transmission in the region where jamming is active until they can share measurement data associated with the estimated jammer position. Hussain *et al.* [8] proposed a jammer localization scheme where battery-free Radio-Frequency Identification (RFID) sensor tags harvest energy from the signal emitted by the jammer. The distances from different tags are then computed to estimate the actual jammer location based on the power received at each energy-harvesting node.

5.2 Jammer Detection and Localization in Mobile Environments

The authors in [26] illustrated a machine learning-based jamming detection approach for devices operating in the 802.11 networks.

Table 6: Comparison between the proposed and existing solution.

Ref.	IoVs	Localization Type	Omnidirectional Antenna	Number of Jammers	Jammer Movement – Mobile	Feature – RSS	Algorithm
[24]	✗	Range-based	✓	Single	✗	✗	Gradient Descent
[34]	✗	Range-based	✓	Single	✗	✓	Gradient Descent and Ascent
[15]	✗	Range-based	✓	Single	✗		LSQ, Adaptive LSQ
[16]	✗	Range-based	✓	Multiple	✗	✓	GA, GPS, SA
[41]	✗	Range-based	✓	Single	✓	✓	LS
[40]	✗	Range-based	✓	Multiple	✗	✓	Alternating iteration and GSA
[37]	✗	Range-based	✓	Single	✓	✓	Trilateration
[14]	✗	Range-free	✓	Single	✗	✓	CL, WCL and VFIL
[13]	✗	Range-free	✓	Multiple	✗	✗	VFIL
[36]	✗	Range-free	✓	Single	✗	✓	GSA
[35]	✗	Range-free	✓ and Directional	Single	✗	✓	CL, VFIL, and improved GSA
[32]	✗	Range-based	✓	Single	✗	✓	CrowdLoc
[31]	✗	Range-free	✓	Single	✗	✗	GCL
[30]	✗	Range-free	✓	Single	✗	✗	CJ
[2]	✗	Range-free	✓	Multiple	✗	✗	X-ray
[3]	✗	Range-free	✓	Single	✗		DCL
[20]	✗	Range-free	✓	Single	✗	–	PSO
[4]	✗	Range-free	✓ and Directional	Single	✗	✓	AILJ
[19]	✓	Range-free	✓	Multiple	✗	✗	FCM and PSO
[21]	✓	-	✓	Multiple	✗	✗	-
This Work	✓	**Range-based**	✓	**Single**	✓	✓	**LLS**

The authors considered a scenario where a static jammer is deployed in a Vehicular Ad Hoc Network (VANET). They utilize PDR and RSS, Channel Busy Ratio (CBR), and measured noise power to detect and identify the type of jammer. Several machine learning algorithms were used to perform classification. Kosmanos *et al.* [11] Proposed an algorithm for speed estimation of malicious jammers in VANETS. Their method estimates the channel between the transmitter-receiver and jammer-receiver based on the relative speed of the jammer and the receiver. Furthermore, they correctly determine the relative speed between the jammer and receiver utilizing the Doppler shift. Pang *et al.* [19] proposed a range-free approach to determine the number of deployed jammers and localize them. A multiclass detection problem is formulated, and Fuzzy C-Means (FCM) method is used to calculate the distance between coordinates and centroids and calculate the number of jamming attackers based on the coverage area. In [21], the authors presented an approach where the number of jammers in Vehicular Ad Hoc Networks (VANETs) is estimated. The dataset is divided into point sets using vehicles' moving features and jammers' spatial features, where the point sets are then grouped based on the distribution of points that are not jammed. Wei *et al.* [41] put forward a distributed mobile jammer tracking scheme to locate mobile jammers in multi-hop wireless networks. The proposed scheme consists of four main steps, including the selection of the monitoring node, measurement of the jamming signal, jammer localization, and handover of the monitoring group. To assess the effectiveness of the presented scheme, multiple simulations were performed for which the results verify the proposed scheme's effectiveness. Nevertheless, this method is only effective for jammers with an omnidirectional antenna, and not a directional antenna. In addition, the effectiveness of the scheme needs to be investigated for different mobility schemes.

5.3 Comparison with Existing Solutions

Table 6 compares the work presented in this paper against existing contributions. We believe that the scenarios and adversarial model introduced here are unique and not addressed in the literature. None of the existing solutions considered moving jammers in IoV networks, and they neither used multiple arrays of antennas nor deploy them in a similar fashion, i.e., distributing them at an equal distance on the vehicle body. Having several antennas as a part of the vehicle body enables achieving higher localization accuracy. Further, such a choice provides a wider range of coverage to detect jamming. Unlike [41], in our localization scheme, we considered that the vehicle participating in the localization scheme is only responsible for computing the distance from the received RSS and transmitting the computed values on through the Internet channel, not affected by jamming. The Internet-connected server is in charge of performing the localization of the jammer vehicle, taking full advantage of the IoV paradigm. Such features make our contribution tailored to IoV scenarios and unique in the literature.

6 CONCLUSION AND FUTURE WORK

In this paper, we presented a jammer localization scheme for IoV networks. The proposed scheme can identify the location of the jammer by leveraging the power received at multiple antennas on multiple collaborating Internet-connected vehicles. We evaluated the performance of our scheme in several setups mimicking real-life scenarios, where the jammer and localization vehicles are stationary in one setup and mobile in the others. Particular attention was paid

to challenging mobile scenarios, with the results being thoroughly analyzed. For each scenario, extensive simulations were performed on randomly-deployed jammer and localization vehicles to obtain insights into the performance of our solution while varying the number of localization vehicles, path-loss exponent, shadowing values, and acquired samples. The obtained results show the effectiveness of the scheme described in the paper, reporting significant localization accuracy even in harsh environments, while using a little number of vehicles.

In the future, we will investigate the performance of our solution with real-life mobility models, as well as the suitability of our solution with multiple jammers. In addition, we will deploy the proposed solution in a real environment, and evaluate its performance in real-life scenarios.

ACKNOWLEDGMENTS

This publication was supported by Qatar University Graduate Assistantship. The findings achieved herein are solely the responsibility of the authors.

REFERENCES

[1] Auto Data. 2021. *Tesla model S Facelift 2021.* https://www.auto-data.net/en/tesla-model-s-facelift-2021-long-range-670hp-awd-42384 Accessed: November 2021.
[2] Tianzhen Cheng, Ping Li, and Sencun Zhu. 2011. Multi-jammer localization in wireless sensor networks. In *2011 Seventh International Conference on Computational Intelligence and Security*. IEEE, 736–740.
[3] Tianzhen Cheng, Ping Li, and Sencun Zhu. 2012. An algorithm for jammer localization in wireless sensor networks. In *2012 IEEE 26th international conference on advanced information networking and applications*. IEEE, 724–731.
[4] Jianhua Fan, Tao Liang, Tongxiang Wang, and Jianwei Liu. 2019. Identification and localization of the jammer in wireless sensor networks. *Comput. J.* 62, 10 (2019), 1515–1527.
[5] Great Scott Gadgets. 2014. HackRF One. Retrieved May 2022 from https://greatscottgadgets.com/hackrf/one/
[6] Andrea Goldsmith. 2005. *Wireless communications*. Cambridge university press.
[7] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing* 17, 4 (2014), 197–215.
[8] Ahmed Mohamed Hussain, Pietro Tedeschi, Gabriele Oligeri, Amr Mohamed, and Mohsen Guizani. 2022. Energy-Harvesting Based Jammer Localization: A Battery-Free Approach in Wireless Sensor Networks. In *2022 IEEE Global Communications Conference: IoT and Sensor Networks (Globecom 2022 IoTSN)*. Rio de Janeiro, Brazil.
[9] Furqan Jameel, Shurjeel Wyne, Georges Kaddoum, and Trung Q Duong. 2018. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Communications Surveys & Tutorials* 21, 3 (2018), 2734–2771.
[10] Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague. 2012. All your jammers belong to us—Localization of wireless sensors under jamming attack. In *2012 IEEE International Conference on Communications (ICC)*. IEEE, 949–954.
[11] Dimitrios Kosmanos, Antonios Argyriou, and Leandros Maglaras. 2019. Estimating the relative speed of RF jammers in VANETs. *Security and Communication Networks* 2019 (2019).
[12] Sinan Kurt and Bulent Tavli. 2017. Path-Loss Modeling for Wireless Sensor Networks: A review of models and comparative evaluations. *IEEE Antennas and Propagation Magazine* 59, 1 (2017), 18–37.
[13] Hongbo Liu, Zhenhua Liu, Yingying Chen, and Wenyuan Xu. 2011. Determining the position of a jammer using a virtual-force iterative approach. *Wireless Networks* 17, 2 (2011), 531–547.
[14] Hongbo Liu, X Wenyuan, Yingying Chen, and Zhenhua Liu. 2009. Localizing jammers in wireless networks. In *2009 IEEE International Conference on Pervasive Computing and Communications*. IEEE, 1–6.
[15] Zhenhua Liu, Hongbo Liu, Wenyuan Xu, and Yingying Chen. 2011. Exploiting jamming-caused neighbor changes for jammer localization. *IEEE Transactions on Parallel and Distributed Systems* 23, 3 (2011), 547–555.
[16] Zhenhua Liu, Hongbo Liu, Wenyuan Xu, and Yingying Chen. 2013. An error-minimizing framework for localizing jammers in wireless networks. *IEEE Transactions on Parallel and Distributed Systems* 25, 2 (2013), 508–517.
[17] Bernard Marr. 2021. *The 5 Biggest Connected And Autonomous Vehicle Trends In 2022.* https://www.forbes.com/sites/bernardmarr/2021/12/20/the-5-biggest-connected-and-autonomous-vehicle-trends-in-2022/ Accessed: January 2022.
[18] Jorge Miranda, Reza Abrishambaf, Tiago Gomes, Paulo Gonçalves, Jorge Cabral, Adriano Tavares, and J Monteiro. 2013. Path loss exponent analysis in wireless sensor networks: Experimental evaluation. In *2013 11th IEEE international conference on industrial informatics (INDIN)*. IEEE, 54–58.
[19] Liang Pang, Xiao Chen, Yong Shi, Zhi Xue, and Rida Khatoun. 2017. Localization of Multiple Jamming Attackers in Vehicular Ad hoc Network. *International Journal of Distributed Sensor Networks* 13, 8 (2017), 1550147717725698.
[20] Liang Pang, Xiao Chen, Zhi Xue, and Rida Khatoun. 2017. A novel range-free jammer localization solution in wireless network by using PSO Algorithm. In *International conference of pioneering computer scientists, engineers and educators*. Springer, 198–211.
[21] Liang Pang, Pengze Guo, Xiao Chen, Jiabin Li, and Zhi Xue. 2017. Estimating the number of multiple jamming attackers in vehicular ad hoc network. In *2017 6th International Conference on Computer Science and Network Technology (ICCSNT)*. IEEE, 366–370.
[22] William Pao. 2021. *Intelligent transportation trends to watch for in 2021.* https://www.asmag.com/showpost/32201.aspx Accessed: January 2022.
[23] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V Krishnamurthy. 2010. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications surveys & tutorials* 13, 2 (2010), 245–257.
[24] Konstantinos Pelechrinis, Iordanis Koutsopoulos, Ioannis Broustis, and Srikanth V Krishnamurthy. 2009. Lightweight jammer localization in wireless networks: System design and implementation. In *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*. IEEE, 1–6.
[25] Konstantinos Pelechrinis, Iordanis Koutsopoulos, Ioannis Broustis, and Srikanth V Krishnamurthy. 2016. Jammer localization in wireless networks: An experimentation-driven approach. *Computer Communications* 86 (2016), 75–85.
[26] Oscar Puñal, Ismet Aktaş, Caj-Julian Schnelke, Gloria Abidin, Klaus Wehrle, and James Gross. 2014. Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation. In *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*. IEEE, 1–10.
[27] GNU Radio. 2001. HackRF One. Retrieved May 2022 from https://www.gnuradio.org/
[28] Annamaria Sârbu and Dumitru Neagoie. 2020. Wi-Fi Jamming using Software Defined Radio. In *International conference Knowledge-Based Organization*, Vol. 26. 162–166.
[29] Muhammad Sameer Sheikh, Jun Liang, and Wensong Wang. 2019. A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors* 19, 16 (2019), 3589.
[30] Yanqiang Sun, Refik Molva, Melek Önen, Xiaodong Wang, and Xingming Zhou. 2011. Catch the jammer in wireless sensor network. In *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, 1156–1160.
[31] Yanqiang Sun and Xiaodong Wang. 2009. Jammer localization in wireless sensor networks. In *2009 5th International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE, 1–4.
[32] Yanqiang Sun, Xiaodong Wang, Melek Önen, and Refik Molva. 2011. CrowdLoc: wireless jammer localization with crowdsourcing measurements. In *Proceedings of the 2nd international workshop on Ubiquitous crowdsouring*. 33–36.
[33] Le Wang and Alexander M Wyglinski. 2011. A combined approach for distinguishing different types of jamming attacks against wireless networks. In *Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*. IEEE, 809–814.
[34] Qiping Wang, Xianglin Wei, Jianhua Fan, Tongxiang Wang, and Qin Sun. 2015. A step further of PDR-based jammer localization through dynamic power adaptation. (2015).
[35] Tongxiang Wang, Xianglin Wei, Jianhua Fan, and Tao Liang. 2018. Adaptive jammer localization in wireless networks. *Computer Networks* 141 (2018), 17–30.
[36] Tongxiang Wang, Xianglin Wei, Jianhua Fan, and Tao Liang. 2018. Jammer localization in multihop wireless networks based on gravitational search. *Security and Communication Networks* 2018 (2018).
[37] Tongxiang Wang, Xianglin Wei, Fei Hu, and Jianhua Fan. 2018. Mobile jammer localization and tracking in multi-hop wireless network. *Journal of Ambient Intelligence and Humanized Computing* (2018), 1–12.
[38] Wei Wang, Haoshan Shi, Pengyu Huang, Dingyi Fang, Xiaojiang Chen, Yun Xiao, and Fuping Wu. 2015. A grid-based linear least squares self-localization algorithm in wireless sensor network. *International Journal of Distributed Sensor Networks* 11, 8 (2015), 317603.
[39] Jan Wantoro and I Wayan Mustika. 2014. M-AODV+: An extension of AODV+ routing protocol for supporting vehicle-to-vehicle communication in vehicular ad hoc networks. In *2014 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*. IEEE, 39–44.
[40] Xianglin Wei and Tongxiang Wang. 2021. AIGSA-based multi-jammer localization in wireless networks. *Applied Soft Computing* 103 (2021), 107131.
[41] Xianglin Wei, Tongxiang Wang, Chaogang Tang, and Jianhua Fan. 2018. Collaborative mobile jammer tracking in multi-hop wireless network. *Future Generation Computer Systems* 78 (2018), 1027–1039.