Received: 7 February 2023 | Revised: 24 April 2023 | Accepted: 26 April 2023

DOI: 10.1049/sil2.12225

IET Signal Processing

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Physical layer security analysis using radio frequency-fingerprinting in cellular-V2X for 6G communication

Hina Ayaz[1] | Ghulam Abbas[2] | Muhammad Waqas[3] | Ziaul Haq Abbas[2] | Muhammad Bilal[4] | Ali Nauman[5] | Muhammad Ali Jamshed[6]

[1]Faculty of Computer Science and Engineering, GIK Institute of Engineering Sciences and Technology, Topi, Pakistan

[2]Tele Communications and Networking (TeleCoN) Research Center, GIK Institute of Engineering Sciences and Technology, Topi, Pakistan

[3]Computer Engineering Department, College of Information Technology, University of Bahrain, Bahrain, Bahrain

[4]Department of Computer Engineering, Hankuk University of Foreign Studies, Hankuk, Republic of Korea

[5]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan-si, Republic of Korea

[6]James Watt School of Engineering, University of Glasgow, Glasgow, UK

Correspondence

Muhammad Ali Jamshed, James Watt School of Engineering, University of Glasgow, Glasgow, UK.
Email: muhammadali.jamshed@glasgow.ac.uk

Ali Nauman, Department of Information and Communication Engineering, Yeungnam University, Gyeongsan-si, Republic of Korea.
Email: anauman@ynu.ac.kr

Abstract

It is anticipated that sixth-generation (6G) systems would present new security challenges while offering improved features and new directions for security in vehicular communication, which may result in the emergence of a new breed of adaptive and context-aware security protocol. Physical layer security solutions can compete for low-complexity, low-delay, low-footprint, adaptable, extensible, and context-aware security schemes by leveraging the physical layer and introducing security controls. A novel physical layer security scheme that employs the concept of radio frequency fingerprinting (RF-FP) for location estimation is proposed, wherein the RF-FP values are collected at different points with in the cell. Then, based on the estimated location, the nearest possible road-side unit for sending the information signal is located. After this, the effects on secrecy capacity (SC) and secrecy outage probability (SOP) in the presence of multiple eavesdropper per unit time are analysed. It has been shown via simulations that the proposed RF-FP scheme increases SC by up to 25% for the same signal-to-noise ratio (SNR) values as those of the benchmarks, while the SOP tends to decrease by up to 30% as compared to the benchmark scheme for the same SNR value. Thus, the proposed RF-FP-based location estimation provides much better results as compared to the existing physical layer security schemes.

KEYWORDS

radio links, security of data

1 | INTRODUCTION

1.1 | Motivation

The rapid advancements in wireless communication and the rapid expansion in urbanisation have paved the way for new frontiers in the domain of cellular communication. Sixth Generation (6G) technology is considered to be a new candidate in this line of advancement. 6G has promised to overcome the shortcomings of Fifth Generation (5G) and Beyond 5G (B5G) by exploiting the terahertz (THz) range. One of the features provided by 6G is to reduce latency, that is, reduce the delay in time by 1/100 of a millisecond. 6G is estimated to provide the highest data rates, that is, 1 Tbps, along with much better support for machine to machine communication, energy efficiency, network reliability, and the use of artificial intelligence (AI) and machine learning (ML) for optimal connectivity [1, 2].

Studies conducted by Ericsson and Qualcomm [3, 4] investigated the potential of using 6G networks for V2X communication. The first study found that 6G networks can support reliable and low-latency vehicle-to-everything (V2X) communication with AI and ML enabling more advanced applications. The second study found that 6G networks can significantly improve the accuracy and reliability of cooperative perception in V2X communication, which could enhance safety and efficiency. Additionally, the studies propose a novel framework for edge computing in V2X communication that enables faster and more efficient data processing, reducing latency, and enhancing reliability. [5–7].

However, these advancements open up new security threats as the advantages of such large-scale coverage can be utilised at the eavesdropper end too. As in the case of vehicular communication, there can be multiple eavesdroppers, and with 6G providing ultra-massive connectivity implies that most of the devices that are within range can be potential eavesdroppers. This includes a pedestrian, a Wi-Fi router, and a relay node [8]. The security techniques for 6G are also up to date with AI techniques and algorithms, which provide much better results. Still, most of the deep learning and AI techniques both require pre-processed data for analysis and mostly rely on the back end for heavy computation [9]. Other techniques employ IRS to redirect the signal so that an eavesdropper will not be able to listen to an information signal between the sender and the receiver [10, 11].

With the advent of B5G and 6G, maintaining security and privacy in wireless communications has become increasingly challenging due to their seamless connectivity. This presents design and simulation challenges that must be addressed. The use of physical layer security (PLS) techniques has the potential to effectively prevent various forms of eavesdropping attacks, including both passive and active types. As a result, it is highly advantageous for current multimedia and infotainment applications in vehicular communication. The next subsection presents related work in PLS techniques in cellular-V2X for 6G communication.

1.2 | Related work

Many researchers have presented a number of PLS schemes using various technologies, such as multiple-input-multiple-output (MIMO), millimetre wave, radio frequency (RF), and non-orthogonal multiple access.

Most of the literature on vehicular networks focus on using some form of computational offloading to first analyse and then provide results, which is helpful in the long run for better optimization. Furthermore, the need for less computationally expensive methods, such as channel state information (CSI) and optimal beamforming, for location estimation should be utilised before the actual message dissemination to reduce the possibility of eavesdropping in vehicular communication, given that it is highly mobile and time-constrained and requires a minimum delay in the physical world [11, 12].

The issue of creating and simulating secret and confidential communications systems across noisy and fading channels has been addressed from several different perspectives. These methods and approaches can be broadly divided into two main categories, that is, traditional approaches and information-theoretic approaches. The traditional method concentrates on the analytical derivations of performance measures associated with the PLS, whereas information-theoretic methods concentrate on the fundamental bounds of performance measurements [4]. A summary of the existing security challenges within VANETs, along with some of the existing approaches and solutions, are outlined in Table 1.

The authors in ref. [13] have discussed the potential aspects of PLS in 6G networks. One of the features that is taken into account is the security requirement for the massive connectivity of mobile devices. This context may benefit from the use of massive cell-free MIMO and intelligent reconfigurable surfaces (IRS) to provide secure communication.

The authors in ref. [14] have provided details regarding the use of IRS in vehicular communication. In the context of smart radio, IRS offers a fresh approach for boosting network secrecy in vehicles. IRS can enhance the desired signals or suppress unwanted signals by adaptively altering the phase shift of the reflecting elements [11, 15]. This is done by manipulating the reflected signal's addition to the non-IRS reflected signal at the receiver in a positive or negative manner.

In ref. [16], the researchers have looked into the effects on secrecy outage probability (SOP) of a single-antenna IRS system with the presence of a single eavesdropper. To be more precise, simulations were conducted to construct and validate analytical expressions of SOP. The authors have found that the use of IRSs can significantly enhance secrecy performance. In the presence of a realistic phase shift model, the SOP degrades, but only slightly. Here, the devices are considered static.

The security of vehicular networks that employ IRS is investigated in refs. [11, 17]. The study supports the possibility of enhancing security using IRS in both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication environment, and their simulation results show that PLS is highly influenced by the placement of IRS. The security is also affected by the quantity of the number of the reflecting elements per IRS.

The authors in ref. [18] have utilised radio frequency fingerprints (RF-FP) for identifying vehicles through dedicated

TABLE 1 Security challenges in VANETs.

Types of security threats	Existing state of the art solutions
Confidentiality	ID-based approach
	Key-based approach
Non-repudiation	Communication-based approach
	Trust-based approach
Data integrity	Behaviour-based approach
	ML-based approach
Availability	Hybrid approach

short-range communication (DSRC). Their proposed mechanism utilises RF-FP to identify IEEE 802.11p protocol-based DSRC. According to the authors, it is a more robust approach to resist identity attack and spoofing. They achieved this by extracting hardware characteristics that are formed by the differences in electronic components of different vehicle devices in highly mobile environments. Their proposed scheme extracts the preamble field features of physical layer frames as device fingerprints and uses the random forest algorithm and sequential detection method to authenticate and distinguish different devices. The results from their experiments and simulations demonstrate that their proposed scheme achieves identification accuracy rates of over 99% for DSRC modules in low-speed line of sight (LOS) and non-line of sight (NLOS) experimental states.

The use of RF-FP for identification of long-term evolution V2X (LTE-V2X) systems is discussed in ref. [19], where the authors propose a method for RF-FP extraction. To overcome the challenge of extracting transmitter RF-FP in the presence of wireless channel and receiver noise, they first estimated the wireless channel without RF-FP. Then, they removed the impact of the wireless channel based on the channel estimation and obtained the initial RF-FP features. Finally, they performed RF-FP denoising to improve the quality of the initial RF-FP. According to the authors, their proposed RF-FP extraction scheme achieves high identification accuracy and is robust to vehicle speed variations.

A secure computational offloading from smart vehicles is discussed in ref. [20]. The authors have presented a technique for resolving the security and authentication concerns for vehicles in VANET. The approach they proposed greatly contributes to ITS network by authenticating vehicles in VANET and detecting various cyber-attacks like distributed denial of service attacks (DDoS). In their methodology, harmful messages are filtered using deep learning-based algorithms, while access control to the cars is provided using identity-based encryption. The identity-based encryption uses deep learning algorithm for security to detect malicious messages with an accuracy of 99.72%.

The researchers in [21] examined two essential aspects for PLS of a wireless vehicular communication network: outage probability and SOP in 6G networks. Two IRS-based vehicle network scenarios have been examined by the authors. The signal-to-noise ratio at various receiver sites has been calculated using a number of analytical formulas. The study demonstrates that a vehicle's network secrecy metrics may be improved. This is accomplished by adjusting the source power, the eavesdropper's distance, and the quantity of IRS cells. It has been shown that IRS-based vehicular networks may be created by analysing the size and positioning of IRSs (in terms of the number of IRS cells) in order to improve their performance. Additionally, the effects of user disturbance and heavy traffic can be considered when evaluating this study.

In ref. [22], PLS is viewed as a potential candidate for securing a network and releasing 6G from conventional complexity-based security strategies. The authors have suggested the use of physical unclonable functions and wireless fingerprinting/localization, in combination with traditional security methods, to improve authentication and key agreement. It also highlights the potential for THz communications for the wiretap channel and for secrete key generation protocols to harness entropy in the frequency domain.

Visible light communication (VLC) is a promising candidate of 6G paradigm and has been used in [23] along with an IRS to provide security at the physical layer. To protect VLC at the physical layer, the authors have integrated watermarking and jamming primitives in the watermark blind physical layer security (WBPLS) algorithm. They assert that their solution makes use of IRS to enhance the communication's security features. They have calculated IRS phases using an optimization framework to optimise the WBPLS jamming interference pattern over a specified area in the room.

A reactive detection approach is considered in ref. [24], which is largely taken into account for the existing detection approaches in order to reduce the cost of communication. In contrast, for the 6G-V2X network where communication resources are relatively profuse, proactive exploration-based security methods should be beneficial for an upgraded level of security. A detection approach based on proactive anomaly detection and prevention of cyber-threats in connected cars has been proposed by refs. [24, 25].

A brief summary of the existing research in the area of physical layer security for vehicular networks is provided in Table 2.

1.3 | Contributions

Despite several earlier studies assumed a quasi-static node placement strategy for the ease of analysis, it has been demonstrated that the mobility of nodes lowers the effectiveness of security for vehicular nodes [11, 27–29]. However, the use of RF-FP for a real time scenario in a 6G Cellular V2X network can greatly improve the security at the physical layer by early location detection to provide a more secure means of V2X communication by leveraging the unique characteristics of the wireless signals transmitted by vehicles and mitigating the risk of eavesdropping and other attacks.

In this research, we observe the effects of RF-FP-based location estimation in order to visualise and take advantages of its benefits, that is, to improve secrecy capacity (SC) and SOP in a VANET-based scenario. The positioning of the potential eavesdropper vehicle with respect to that of the sender and the receiver is also observed, and a temporary perimeter is set around both the sending and receiving vehicles for potential eavesdropper's detection by location estimation per unit time. This temporary location identification helps in sending the information signal in a secure manner. To the best of our knowledge, the concept of RF-FP has not been utilised before in 6G-based physical layer security in C-V2X. The main contributions of the paper are as follows:

- We introduce the use of RF-FP for vehicle tagging, that is, location estimation and identification per unit time for 6G C-V2X. The RF-FP of every vehicle is unique, which helps to

TABLE 2 Summary of the existing state of the art in the physical layer security for vehicular networks.

Scheme	Year	Proposed methodology	6G component	Dynamic env.	VANET
Cui miao et al. [26]	2019	Use of IRS signal diminishing features to cancel the leaked signal at the eavesdropper's end	IRS	×	×
Cheng et al. [12]	2020	Federated learning-based traffic pattern identification and disaster management	No	✓	✓
Makarfi et al. [11]	2020	Use of IRS as a relay to redirect the information signal and observe the effects on SC and SOP	IRS	✓	✓
Makarfi et al. [11]					
Ali et al. [17]	2020	Use of IRS to observe the effects of SC and SOP for a V2V and a V2I scenario	IRS	✓	✓
Zhou et al. [20]	2021	A secure computational offloading from smart vehicles, along with identity-based encryption method with a deep learning algorithm for security to detect malicious messages	×	✓	✓
Soderi et al. [23]	2022	Use of VLC for integration of the watermarking and jamming primitives in the WBPLS algorithm.	VLC and IRS	✓	✓
Kavaiya et al. [21]	2022	The use of power adjustment to improve SOP for a vehicular network	IRS	✓	✓
RF-FP location estimation					
(Proposed)	2023	Analysing SOP and SC by using RF-FP location detection	6G C-V2X	✓	✓

identify different vehicles when they establish communication with the base station (BTS). The RF-FP information is stored in the cloud database for future reference. We assume that the cloud database is maintained at the BTS, where the RF-FP values are collected at different locations within the cell.

- We have considered angular distance of the potential eavesdropper vehicles with respect to that of the legit communicating vehicles. The use of angular distance, that is, the distance of the legit as well as the potential eavesdropper vehicle can help us better optimise how the information signal should be sent, that is, between the legit communicating vehicles. To measure the angular distance between the vehicles, we employ the Haversine equation.
- We consider an urban scenario for our proposed scheme. The presence of multiple eavesdroppers within the communication range having distance less than 4 m is considered. Since the traffic in an urban scenario is dense and the traffic is also heavy, keeping this in view, the presence of multiple eavesdropper is potentially very high.
- To minimise eavesdropping while maintaining the seamless end-to-end service, it is important to regulate the amount of transmit power. This approach can limit the signal range and contribute to power optimization indirectly.
- We have analysed the effects of location estimation per unit time on SC and SOP. Since the vehicles are in motion and constantly change their position, the location has to be constantly monitored. This has a significant impact on SC and SOP, per unit time, for which we varied the signal-to-noise ratio (SNR) values between vehicles.
- To benchmark our results, we have compared our proposed scheme with the existing NNakagami fading channels in ref. [30]. The NNakagami fading channels, which include the Rayleigh and Nakagami-m fading channels, are more versatile and general for practical mobile applications. Therefore, we explore the NNakagami fading channel secrecy performance of the mobile vehicular networks model.
- The results of the simulation indicate that there is a significant improvement in SC and SOP by using RF-FP for location estimation. The SC increases by 25%, which leads to a corresponding increase in the overall performance of the system. Moreover, the simulation results also show that the SOP decreases by 30%, which is a significant improvement even for very small values of SNR, that is, 5 dBm. This suggests that the proposed RF-FP-based location estimation scheme is robust and effective and has the potential to improve the performance of the system even in challenging scenarios where the SNR is low. Overall, the simulation results provide a strong evidence in favour of the efficacy of the RF-FP-based scheme in improving the performance of the system.

1.4 | Paper organisation

The rest of the paper is organised as follows. Section 2 presents an overview of the system model and the problem formulation. Section 3 details the proposed scheme, followed by simulation results in Section 4. Finally, the conclusion is laid out in the subsequent sections. Table 3 lists the symbols and notations used throughout the paper.

2 | SYSTEM OVERVIEW, MODEL, AND PROBLEM FORMULATION

For our model, we consider a 6G C-V2X environment, where the BTS as well as the RSUs are assumed to be 6G enabled and are fully connected with each other as shown in Figure 1. The signal receiving range of the RSU is considered to be up to 800 m. Since we are utilising 6G network technology for communication, we assume that as soon as a vehicle enters within the range of an RSU or a BTS, its RF-FP of the unique

TABLE 3 List of notations.

Notation	Definition
C	Secrecy capacity
D	Destination
d	Distance between $\{P, I, E\}$ w.r.t. S and D
d_{S-D}	Distance from S to D in metres
E	Eavesdropper
G_i	Gain where $i = \{S, D, E\}$
I	Infrastructure, that is, BTS/RSU
L	Path loss factors due to attenuation, interference, shadowing
n_i	Noise value where $i = \{D, E\}$
P	Pedestrian
P_i	Power where $i = \{S, D, E\}$
Ph	Channel coefficient at S and D
Pr	Probability
RF-FP$_n$	Radio frequency fingerprinting where $n = \{V, P, I\}$
S	Source
T_i	Transmit power where $i = \{S, D, E\}$
V	Vehicles where $\{S, D, E\}$
$\mathcal{W}_i$	Additive white Gaussian noise where $i = \{S, D, E\}$
X_j	Information signal to be exchanged
(x_i, y_i)	Coordinates of the vehicles
y_i	Received signal strength where $i = \{S, D, E\}$
$\mathrm{Z}_{\mathrm{sop}}$	Instantaneous SOP
Δt	Instantaneous time
δ^{th}	Threshold value
λ	Wavelength of the signal in metres
γ_i	Signal-to-noise ratio where $i = \{D, E\}$
θ	Central angle between two points on a sphere

form is stored with the BTS in the form of a table, which is further stored in a cloud database. The information can be shared on demand. For our model, we consider V2V, V2I, and V2P scenarios, that is, when a vehicle wants to communicate directly with another vehicle or it wants to communicate with the infrastructure (BTS or RSU) or with a nearby pedestrian. The vehicle that initiates communication is defined as the source represented by S, and the receiver that can be a pedestrian, infrastructure, or another vehicle is represented by D, where $D = \{V, P, I\}$, respectively. The distance between the source and destination is represented by d_i where $i \in d = \{d_V, d_P.d_I\}$, respectively.

We also consider an urban scenario for our model, where we take into account multiple eavesdroppers in the vicinity of the legit communicating vehicles. The transmit signal strength for calculation of RF-FP is given as follows:

$$T_S = T_D / \left(G_S * G_D * (\lambda/(4 * \pi * d))^2 * L\right), \tag{1}$$

where T_S is the transmitted power from the transmitter (in watts), T_D is the received power at the receiver (in watts), G_S is the gain of the transmitter antenna, G_D is the gain of the receiver antenna, λ is the wavelength of the signal (in metres), d_{S-D} is the distance between the transmitter and receiver (in metres), and L is the path loss factor, which accounts for the attenuation of the signal due to atmospheric conditions and other environmental factors. For ease of simplicity of the equation, we have not added the other path loss factors and shadowing.

The received signal strengths at the source S, destination D, and eavesdroppers E are as follows:

$$y_S = G_{S,D}.P_S + \mathcal{W}_S, \tag{2}$$

$$y_D = G_{D,S}.P_D + \mathcal{W}_D, \tag{3}$$

$$y_E = G_{E,S}.P_E + \mathcal{W}_E. \tag{4}$$

where y_S is the received signal at source with power P_S. Similarly, y_D and y_E are received signals at the destination and eavesdropper, respectively, with powers P_D and P_E. G is the channel gain between the communicating vehicles, and $\mathcal{W}_i$ is the additive white Gaussian noise, where $i = \{S, D, E\}$.

SC is the rate at which two vehicles can communicate securely in the presence of an eavesdropper. Since the vehicles are considered in motion, the instantaneous SC is given as follows:

$$C = MAX\left\{\ln\left(1 + \gamma_D\right) - \ln\left(1 + \gamma_E\right), 0\right\}. \tag{5}$$

The average SC is the average of the secrecy capacity [30]. Here, γ_D and γ_E are the signal-to-noise ratio at D and E, respectively. In Equation (5),

$$\gamma_D = \sqrt{G_D P}h_D X + n_D, \tag{6}$$

and

$$\gamma_E = \sqrt{G_E P}h_E X + n_E, \tag{7}$$

where n_E and n_D are noises and are of the type 0 and $N_0/2$, respectively. Ph_D and Ph_E are the channel coefficients at S and D, respectively.

SOP is the maximum amount of information that can be exchanged under the threat of eavesdropping and it should not fall below a preset threshold value, which might compromise the information [11]. The instantaneous SOP is given as follows:

$$\mathcal{Z}_{sop} = \Pr\left(C\left(\gamma_D, \gamma_E\right) < \delta_{th}\right), \tag{8}$$

where $\mathcal{Z}_{sop}$ is the instantaneous SOP, Pr is the probability, and δ^{th} is the threshold value [30].

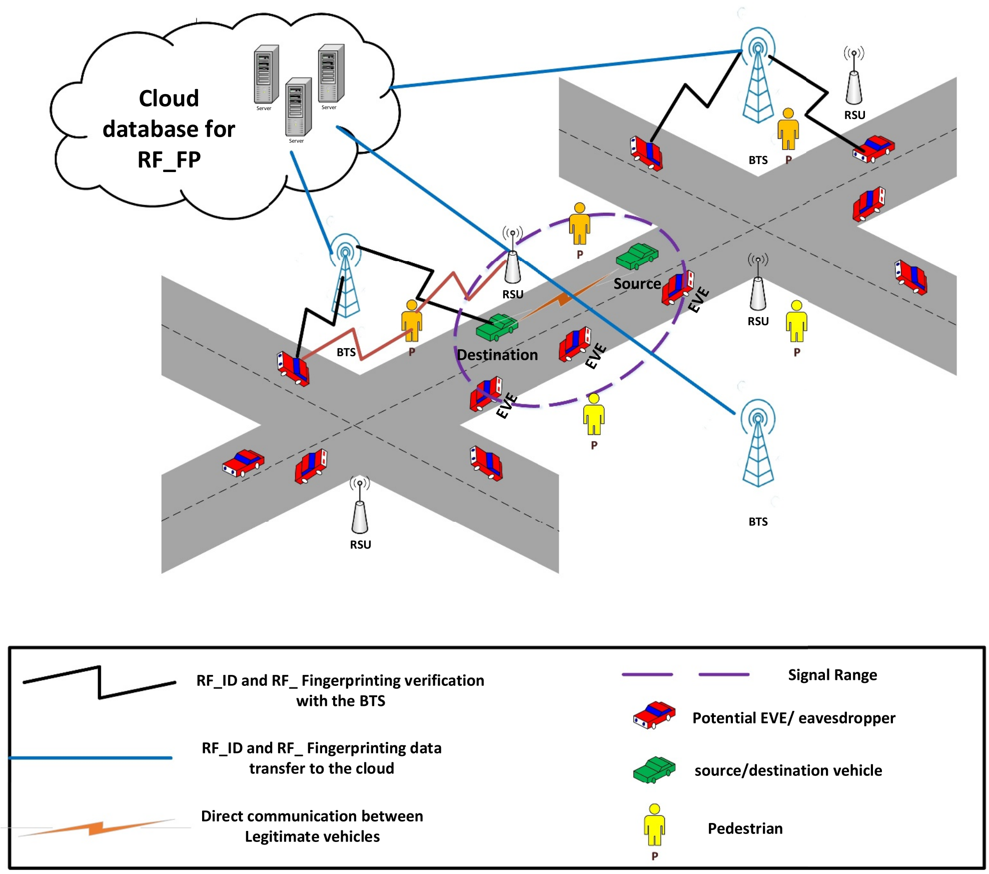
Cloud database for RF_FP
Server
Server
Server
BTS
RSU
P
BTS
P
RSU
Source
Destination
EVE
EVE
EVE
P
RSU
P
P
BTS
RSU
RF_ID and RF_ Fingerprinting verification with the BTS
RF_ID and RF_ Fingerprinting data transfer to the cloud
Direct communication between Legitimate vehicles
Signal Range
Potential EVE/ eavesdropper
source/destination vehicle
Pedestrian
P

FIGURE 1 System model for a C-V2X network with Source S with BTS and RSU that are connected to a cloud for RF-FP tagging for location estimation of the legit vehicles along with that of the potential eavesdroppers.

3 | THE PROPOSED SCHEME

From the above laid out scenario for a 6G C-V2X-based network from a PLS perspective, we utilise FR-FP for location estimation before the actual message can be communicated. Here, we try to locate the instantaneous position of the legit vehicles as well as that of the eavesdroppers, which are the potential threats. The procedural flowchart of the proposed scheme is given in Figure 2.

A point wise explanation of each step is as follows.

3.1 | RF-FP collection

In this step, the proposed algorithm collects a set of RF fingerprints from various locations in the area where the two vehicles are located. Each RF fingerprint should contain information about the signal strength of different wireless access points (WAPs), that is, BTS/RSU sources in the area. In this way, the unique RF-FP associated with every vehicle is exchanged with the nearest RSU or BTS. We store the RF fingerprints in the cloud database, along with their corresponding locations. Next, we determine the time at which the location estimation is required. We then obtain the RF fingerprint of each vehicle at that time by scanning for nearby WAPs or other RF sources and measuring their signal strength. This step is performed for every vehicle that is entering in the cell. The value is stored and tagged in a cloud database for the identification of the vehicle in future. It is assumed that the cloud database is connected to all the BTSs. It is also assumed that a temporary table is constructed in the cloud for the identification of the RF-FP values associated with each vehicle.

3.2 | Location estimation

We compare the measured RF fingerprints to those in the database and determine the most similar fingerprints. We then use the locations associated with the most similar fingerprints to estimate the location of each vehicle. We have used Haversine, that is, $haversine(\theta) = \sin^2(\theta/2)$, as a distance measuring method to determine the distance between S and D. The algorithm returns the estimated location before establishing communication.

3.3 | Establishing communication

In order to establish communication between the legit communicating vehicles, the estimated distance calculated in

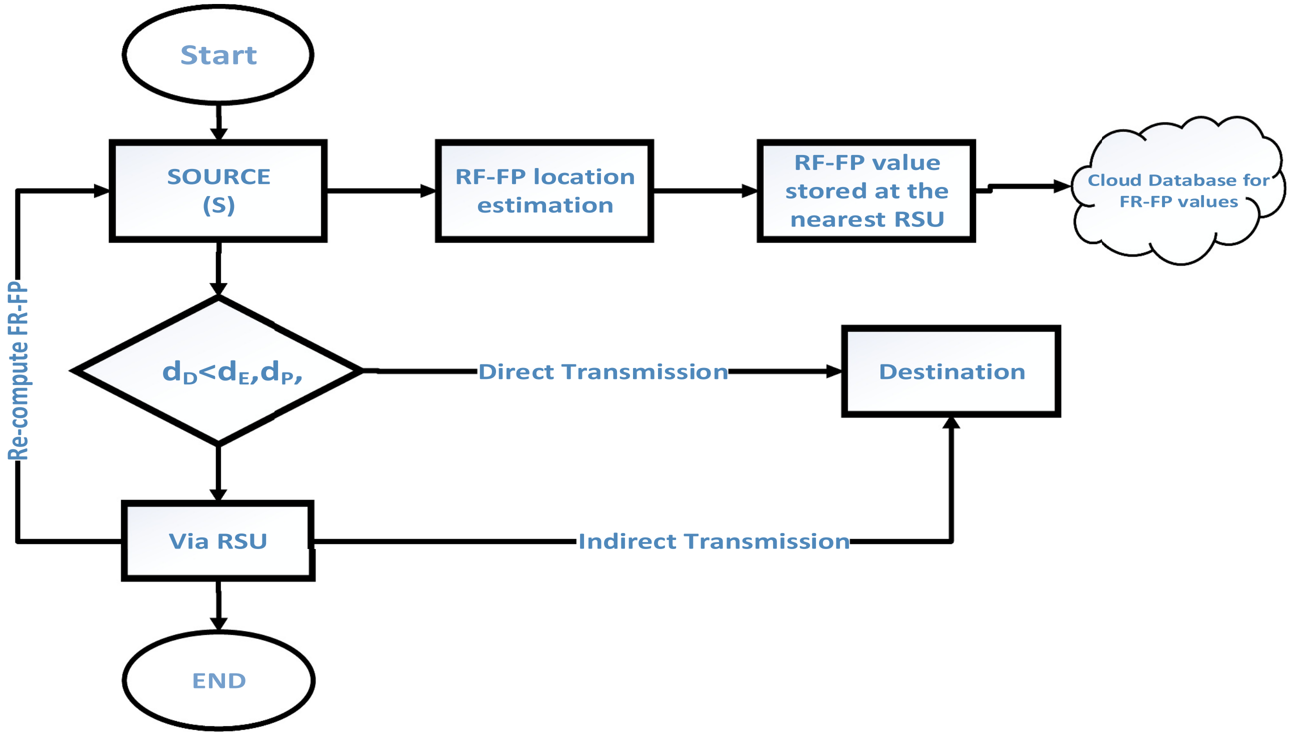

FIGURE 2 Procedural flowchart of the proposed RF-FP location estimation scheme.

Step II (location estimation) is evaluated, that is, to check whether it is less than 4 m. If true, then the RF-FP of the S and D is shared with the source and destination. Then, the distance d_V of the nearby vehicles that are potential eavesdropper is also calculated at time Δt, where $V = \{S, D, E\}$. The algorithm keeps track of S and D, as well as calculates d_i where $i = \{P, I, E\}$ w.r.t. S and D.

3.4 | Transmission

In this step, the information can be transmitted in two ways, either directly or indirectly, depending on the location of the eavesdropper w.r.t. Legit communicating vehicles. If the distance of eavesdroppers, that is, d_E is greater than that of S and D, then the information is decimated directly or if the distance of the potential eavesdropper is more than half a wavelength, then it cannot eavesdrop on the information being exchanged. Otherwise, if there exists some potential unauthorized vehicle(s) that is not the intended destination, then an indirect path via the nearest RSU is taken to share the message.

3.5 | Re-compute RF-FP

In this step, if further information needs to be exchanged between S and D, then Step I to Step III are recomputed for the next Δt. Finally, SC and SOP are calculated for analysis. The steps of our proposed scheme are given in Algorithm 1.

Algorithm 1 : RF-FP location estimation for analysing SC and SOP in VANETs

```
Start
Step #I RF-FP Collection:
  Collect $RF - FP_n$ from various points in the cell
  Store all the $RF - FP_n$ at the cloud database of BTS
  Share $RF - FP_n$ with the RSU with in the cell
    where $n = \{V, P, I\}$.
Step # II Location Estimation ($LE$):
  Determine the time $\Delta t$
at which LE is required $b/w$ $S$ and $D$
  Retrieve coordinates $(x_i, y_i)$ of $S$ & $D$
  Calculate the angular distance $b/w$
    $S$ & $D$
  Using $haversine(\theta) = \sin^2(\theta/2)$.
Step # II: Establish Communication:
  if $\delta d_{D,S} < 8$ m
  Share $RF - FP_S$ & $RF - FP_D$ values $b/w$ the legit
Vehicles
  Calculate $d_V$ at $\Delta t$
    where $V = \{S, D, E\}$
  Calculate $d_P$ & $d_I$ w.r.t $S$ and $D$
    where $P = pedestrian$ & $I = BTS/RSU$
keep track of $S$ and $D$
Tag the destination $d_i$
Step # III: Transmission:
     if $d_E > (d_S$ & $d_D)$
```

```
        then
            Send $X_j$
              else
            Send $X_j \mapsto$ RSU near $D$
          Send $X_j \mapsto D$
          Send RSU $\mapsto D$
Step# IV Re-compute RF-FP
     Repeat Step I-Step III for NEXT $X$
      Calculate SC and SOP for both the cases
End
```

4 | PERFORMANCE EVALUATION

Simulations for SC and SOP are conducted for the proposed RF-FP-based location estimation scheme. For simulations, we have used MATLAB 2020 b. The vehicles as well as the pedestrian are randomly deployed. The BTS/RSUs are kept 800 m apart for C-V2X to function properly. The distance between the communicating entities is kept between 1 and 4 m. The SNR values are fluctuated between −10 dBm and 30 dBm, and the instantaneous time is kept up to 60 s. The threshold value for SOP is 2 bits/hertz. The distance between the legitimate vehicles, that is, S and D, is varied between {3–6} metres, while that of the eavesdropper vehicles with respect to S, E is varied between {3–8} metres, respectively. Table 4 presents the list of the parameters used for simulations.

In the next section, we examine the effects of using RF-FP location estimation on ASC and SOP over fading channels as well as Nakagami and 2-Nakagami.

4.1 | Average secrecy capacity

In this section, we evaluate the effects of FR-FP on ASC. To observe the results, we have increased the SNR values and kept the deployment of vehicles random. The source transmit power is kept between 5 and 15 W. This value is kept minimum to avoid signal leakage at the eavesdropper's end.

Figure 3 shows the impact of channel fading on ASC as the eavesdropper moves away from the legitimate vehicles. From the simulations, it is observed that by using uniform increase in distance of the eavesdropper, there is a great increase in ASC. The increase in the SNR values also helps to improve ASC as can be observed by the blue line with circles. In the other line that displays the effects on ASC with random deployment of eavesdropper, there is a sharp decrease in ASC since the eavesdroppers are less than 1 m apart from the legitimate vehicles. Moreover, the transmit power is also high enough for the eavesdropper to tap in the information signal. As there is an increase in the SNR value, the ASC is also performing better and is increasing. This is because of the increase in the SNR value at the eavesdropper end results in signal degradation. Moreover, the destination is nearer to the source as compared to the eavesdroppers. Thus, both the distance as well as the SNR value have a significant impact on ASC.

Figure 4 signifies the impact of having more than one eavesdroppers near the legitimate communicating vehicles. When the number of eavesdropper is more than one, then the angular distance of these vehicles with respect to S and D has a significant impact. With smaller values of SNR, ASC is

TABLE 4 Simulation parameters.

Parameters	Range of values
Vertical distance	1–8 m
No. of eavesdroppers within range	1–4
Min path loss values	0.68–30 dBm
No. of antennas	2
SNR values	−5–20 dBm
Distance b/w RSUs	800 m
Instantaneous time	60 s
SOP threshold values	2 bits/sec

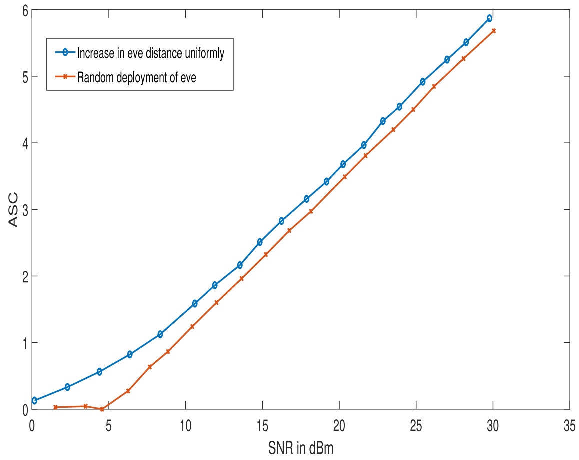

FIGURE 3 The impact of channel fading on the eavesdropper by minimising the source transmit power.

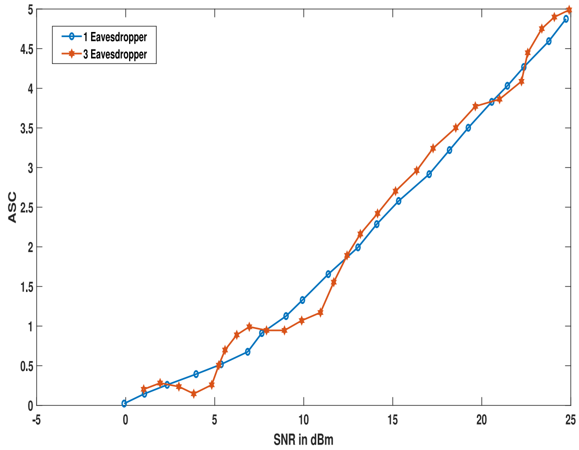

FIGURE 4 The effects of multiple eavesdroppers in the presence of legit communicating vehicles.

significantly reduced. The ASC, even in the presence of multiple eavesdroppers, can be improved by increasing the SNR values and controlling the source transmit power as it can be observed in Figure 4. The angular distance of the eavesdropper, whether it is a single eavesdropper or multiple, has a significant impact on ASC.

In Figure 5, we have used random deployment of multiple eavesdroppers with an increase in the SNR up to 20 dBm. It is observed that by using simply 2-Nakagami without location estimation does increase ASC significantly, and there is a general increase in ASC with an increase in the SNR. While with RF-FP and smaller SNR values, the ASC values of the proposed scheme are very less in comparison to that of 2-Nakagami [30]. This is happening as the number of eavesdropper vehicles are more than 3 near the source or the destination vehicle. Conversely, a great increase happens when the eavesdroppers are less and have a larger angular distance from the legit communicating vehicles. Once again, even for such a scenario, the increase in the SNR value for the eavesdropper significantly improves ASC in the proposed scheme. Thus, location estimation using RF-FP has a positive impact on ASC with the increased SNR value.

4.2 | Secrecy outage probability

In this section, we observe the impact of using RF-FP location estimation on SOP for different scenarios.

Figure 6 presents the effects of simply using the Nakagami and 2-Nakagami on SOP with an increase in SNR values. Both the types of Nakagami are almost overlapping with each other. Although at some points 2-Nakagami performs slightly better, it is not that significant enough. This happens due to the random deployment of the eavesdropper vehicles. Although the increase in the SNR value greatly improves SOP and reduces the outage probability even when the eavesdropper vehicle is in range, yet for smaller values of the SNR, the SOP is very high. Thus, just employing Nakagami fading at the eavesdropper end is not enough to improve SOP as it only provides better results for significantly larger SNR values. If the distance of the eavesdropper vehicle is less than 2 m even for larger SNR values, SOP tends to rise.

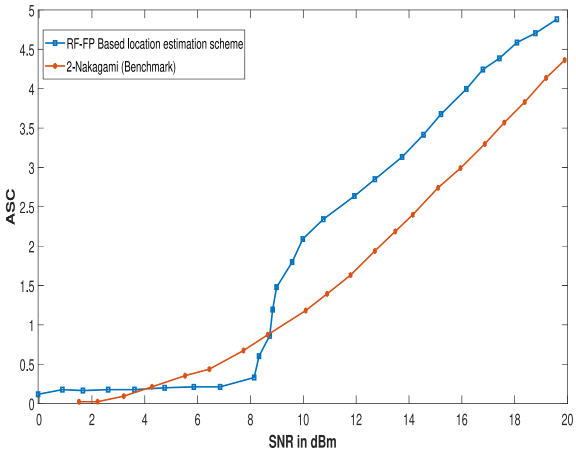

FIGURE 5 ASC with and without RF-FP-based location estimation before actual message dissemination with random eavesdropper deployment.

To reduce the SOP, we have introduced RF-FP for location estimation at the legit communicating vehicles, where it can be observed that in Figure 7 for very small SNR values, the outage probability is greatly reduced. For comparison, we have used 2-Nakagami without RF-FP location estimation with that of 2-Nakagami with RF-FP location estimation, respectively.

In Figure 7, it can be seen that the use of RF-FP for location estimation significantly improves SOP even for smaller SNR values. Conversely, 2-Nakagami improves SOP but for much larger SNR values. Furthermore, even in the presence of multiple eavesdroppers within the range, the RF-FP-based location estimation still outperforms the simple 2-Nakagami scheme. Therefore, using the RF-FP-based location estimation scheme before the actual message transmission can have a better impact on reducing SOP than relying solely on the simple 2-Nakagami scheme.

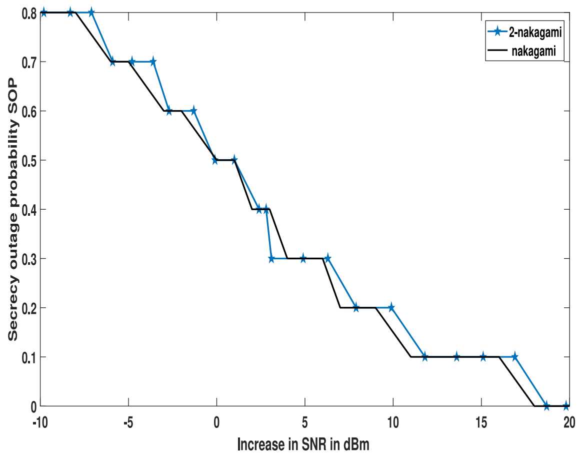

FIGURE 6 SOP without using RF-FP location estimation with multiple and random eavesdropper deployment for different SNR values.

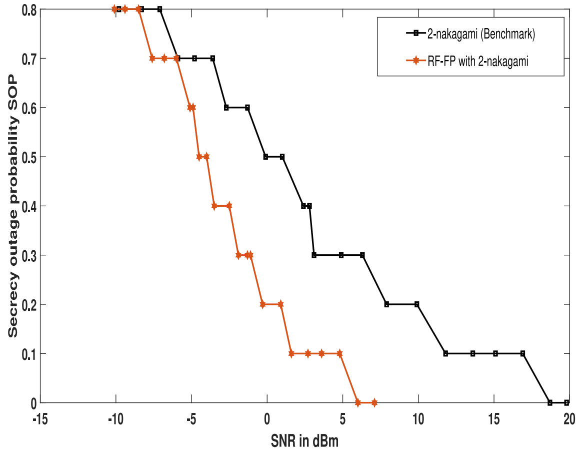

FIGURE 7 Impact of using RF-FP location estimation with multiple and random eavesdropper deployment for different SNR values on SOP.

4.3 | Critical discussion

From the results presented in the previous subsections, it can be observed that there are a number of factors that have a significant impact on SOP and ASC in a VANET environment. Although we are using 6G C-V2X for communication, it still needs optimization for using its full capacity.

The seamless connectivity and full coverage are just not available at the legit communicating vehicles, it is also available simultaneously to potential eavesdroppers. An eavesdropper can also use these features to negatively impact ASC and SOP. The secrete message can be easily tempered by any malicious user within a signal receiving range. The location estimation using RF-FP significantly improves the legit communication as it helps to optimise the amount of power needed to transmit the information signal.

For ease of computation, we have considered the interference to be a constant value, that is, 10 dBm. Since 6 G operates at higher frequencies and data rates as compared to VANETs and is more susceptible to interference, this can results in a number of shortcomings, namely, incorrect location estimation due to multi-path fading, limited coverage, reduced scalability. Since, it is important to note that in real-world scenarios, interference can be variable and have different effects on different parts of the communication system, by examining the impact of different types of interference, we can gain a more comprehensive understanding of how the system performs under different conditions. This knowledge can then be used to further optimise the performance of the proposed scheme. Our future work will identify potential problems, and develop strategies to mitigate interference.

5 | CONCLUSION AND FUTURE WORK

The anticipated emergence of new security challenges in 6G systems presents an opportunity for the development of adaptive and context-aware security protocols that leverage physical layer security solutions. This paper proposes a novel physical layer security scheme that utilises radio frequency fingerprinting for location estimation and identifies the nearest road-side unit for sending information signals. Simulation results show that the proposed RF-FP scheme increases SC by up to 25% and decreases secrecy SOP by up to 30% compared to benchmark schemes for the same SNR values. Overall, the proposed RF-FP-based location estimation offers much better results compared to existing physical layer security schemes. As a future work, we aim to improve SC and SOP by considering imperfect or no CSI along with the use of other scenario where multiple pedestrian can also be potential threats in an ultra dense traffic. Another possible future direction is to study the impact of interference and jamming on the performance of RF-FP location estimation. This could involve investigating how the proposed scheme performs in the presence of intentional or unintentional interference and developing countermeasures to mitigate the impact of such interference and also to analyse the effects of different types of interference on the SC and SOP.

AUTHOR CONTRIBUTION

Hina Ayaz: Conceptualisation, Formal analysis, Investigation, Methodology. **Ghulam Abbas**: Conceptualisation, Methodology, Project administration. Resources, Supervision, Writing, review and editing. **Ziaul Haq Abbas**: Project administration, Resources, Supervision, Writing, review and editing. **Muhammad Bilal**: Formal analysis, Project administration, Resources, Funding Acquisition, Writing, review and editing. **Ali Nauman**: Formal analysis, Software, Funding Acquisition, Writing, review and editing. **Muhammad Ali Jamshed**: Resources, Software, Writing, review and editing.

ACKNOWLEDGEMENT

This work received no external funding.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

Data are not available to this article.

ORCID

Muhammad Waqas https://orcid.org/0000-0003-0814-7544

Muhammad Ali Jamshed https://orcid.org/0000-0002-2141-9025

REFERENCES

1. Chen, S., et al.: Cellular Vehicle-To-Everything (C-V2x). Springer Nature (2023)
2. Bhattacharya, P., et al.: 6Blocks: 6G-enabled trust management scheme for decentralized autonomous vehicles. Comput. Commun. 191(2022), 53–68 (2022). https://doi.org/10.1016/j.comcom.2022.04.024
3. Ericsson, Telkomsel, Q.: Ericsson and Qualcomm Strengthen Collaboration on 5G-Based Fixed Wireless Access Technology Roadmap Development to Enhance Digital Experience in Indonesia (2023). https://www.ericsson.com/en/press-releases/2/2023/. Accessed on 13 April 2023
4. Jejdling, F., Others Ericsson mobility report: Ericsson. Stockholm (2020)
5. Dai, Y., Zhang, Y.: Adaptive digital twin for vehicular edge computing and networks. Journal Of Communications And Information Networks 7(1), 48–59 (2022). https://doi.org/10.23919/jcin.2022.9745481
6. You, X., et al.: & Others towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci. China Inf. Sci. 64, 1–74 (2021)
7. Bajracharya, R., et al.: Dynamic pricing for intelligent transportation system in the 6G unlicensed band. IEEE Trans. Intell. Transport. Syst. 23(7), 9853–9868 (2021). https://doi.org/10.1109/tits.2021.3120015
8. Nguyen, D., et al.: 6G Internet of Things: a comprehensive survey. IEEE Internet Things J. 9(1), 359–383 (2021). https://doi.org/10.1109/jiot.2021.3103320
9. Khan, W., et al.: Opportunities for Intelligent Reflecting Surfaces in 6G-Empowered V2X Communications (2022). *ArXiv Preprint ArXiv: 2210.00494*
10. Asim, A., Cada, M.: Enhancement of physical layer security in flying Adhoc networks by intelligent reflecting metasurfaces. International Journal Of Intelligent Systems And Applications In Engineering 11, 46–50 (2023)

11. Makarfi, A., et al.: Physical layer security in vehicular networks with reconfigurable intelligent surfaces. In: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), pp. 1–6 (2020)
12. Cheng, X., Huang, Z., Chen, S.: Vehicular communication channel measurement, modelling, and application for beyond 5G and 6G. IET Commun. 14(19), 3303–3311 (2020). https://doi.org/10.1049/iet-com.2020.0531
13. Mucchi, L., et al.: Physical-layer security in 6G networks. IEEE Open Journal Of The Communications Society 2, 1901–1914 (2021). https://doi.org/10.1109/ojcoms.2021.3103735
14. Zhu, Y., Mao, B., Kato, N.: Intelligent reflecting surface in 6G vehicular communications: a survey. IEEE Open Journal Of Vehicular Technology 3, 266–277 (2022). https://doi.org/10.1109/ojvt.2022.3177253
15. Ayaz, H., et al.: Improved rate of secret key generation using passive Reconfigurable intelligent surfaces for vehicular networks. Sustainability vol. 15(1), p. 342 (2022)
16. Yang, L., et al.: Secrecy performance analysis of RIS-aided wireless communication systems. IEEE Trans. Veh. Technol. 69(10), 12296–-12300 (2020). https://doi.org/10.1109/tvt.2020.3007521
17. Ai, Y., et al.: Secure vehicular communications through reconfigurable intelligent surfaces. IEEE Trans. Veh. Technol. 70(7), 7272–7276 (2021). https://doi.org/10.1109/tvt.2021.3088441
18. Chen, T., Hu, A., Jiang, Yu: Radio frequency fingerprint-based DSRC intelligent vehicle networking identification mechanism in high mobility environment. Sustainability 14(9), 5037 (2022). https://doi.org/10.3390/su14095037
19. Chen, T., et al.: Radio frequency fingerprints extraction for LTE-V2X: a channel estimation based methodology. In: 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), pp. 1–6. IEEE (2022)
20. Zhou, Z., et al.: A fine-grained access control and security approach for intelligent vehicular transport in 6G communication system. IEEE Trans. Intell. Transport. Syst. 23(7), 9726–9735 (2021). https://doi.org/10.1109/tits.2021.3106825
21. Kavaiya, S., Patel, D.: Restricting passive attacks in 6G vehicular networks: a physical layer security perspective. Wireless Network 29(3), 1–11 (2022). https://doi.org/10.1007/s11276-022-03189-1
22. Chorti, A., et al.: Context-aware security for 6G wireless: the role of physical layer security. IEEE Communications Standards Magazine 6(1), 102–108 (2022). https://doi.org/10.1109/mcomstd.0001.2000082
23. Soderi, S., et al.: VLC physical layer security through RIS-aided jamming receiver for 6G wireless networks. In: 2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), pp. 370–378 (2022)
24. Tang, F., et al.: Future intelligent and secure vehicular network toward 6G: machine-learning approaches. Proc. IEEE 108(2), 292–307 (2019). https://doi.org/10.1109/jproc.2019.2954595
25. Al-Khateeb, H., et al.: Proactive threat detection for connected cars using recursive Bayesian estimation. IEEE Sensor. J. 18(12), 4822–4831 (2017). https://doi.org/10.1109/jsen.2017.2782751
26. Cui, M., Zhang, G., Zhang, R.: Secure wireless communication via intelligent reflecting surface. IEEE Wireless Communications Letters 8(5), 1410–1414 (2019). https://doi.org/10.1109/lwc.2019.2919685
27. Porambage, P., et al.: The roadmap to 6G security and privacy. IEEE Open Journal Of The Communications Society 2, 1094–1122 (2021). https://doi.org/10.1109/ojcoms.2021.3078081
28. Makarfi, A., et al.: Reconfigurable intelligent surfaces-enabled vehicular networks: a physical layer security perspective." *ArXiv Preprint ArXiv:2004*.11288. (2020)
29. Dang, S., et al.: What should 6G be? Nature Electronics 3(1), 20–29 (2020). https://doi.org/10.1038/s41928-019-0355-6
30. Xu, L., et al.: Physical layer security performance of mobile vehicular networks. Mobile Network. Appl. 25(2), 643–649 (2020). https://doi.org/10.1007/s11036-019-01224-8

How to cite this article: Ayaz, H., et al.: Physical layer security analysis using radio frequency-fingerprinting in cellular-V2X for 6G communication. IET Signal Process. e12225 (2023). https://doi.org/10.1049/sil2.12225