

Hybrid PLS-ML Authentication Scheme for V2I Communication Networks

Hala Amin, Jawaher Kaldari, Nora Mohamed, Waqas Aman, Saif Al-Kuwari
Division of Information and Computing Technology, College of Science and Engineering,
Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar.
{haam51711, jaka51804, nomo51812, waman, smalkuwari}@hbku.edu.qa

Abstract—Vehicular communication networks are rapidly emerging as vehicles become smarter. However, these networks are increasingly susceptible to various attacks. The situation is exacerbated by the rise in automated vehicles complicates, emphasizing the need for security and authentication measures to ensure safe and effective traffic management. In this paper, we propose a novel hybrid physical layer security (PLS)-machine learning (ML) authentication scheme by exploiting the position of the transmitter vehicle as a device fingerprint. We use a time-of-arrival (ToA) based localization mechanism where the ToA is estimated at roadside units (RSUs), and the coordinates of the transmitter vehicle are extracted at the base station (BS). Furthermore, to track the mobility of the moving legitimate vehicle, we use ML model trained on several system parameters. We try two ML models for this purpose, i.e., support vector regression and decision tree.

To evaluate our scheme, we conduct binary hypothesis testing on the estimated positions with the help of the ground truths provided by the ML model, which classifies the transmitter node as legitimate or malicious. Moreover, we consider the probability of false alarm and the probability of missed detection as performance metrics resulting from the binary hypothesis testing, and mean absolute error (MAE), mean square error (MSE), and coefficient of determination R^2 to further evaluate the ML models. We also compare our scheme with a baseline scheme that exploits angle of arrival at RSUs for authentication. We observe that our proposed position-based mechanism outperforms the baseline scheme significantly in terms of missed detections.

I. INTRODUCTION

Vehicular communication networks (VCNs) are a type of communication system that enables wireless communication among vehicles and vehicles to roadside infrastructure. VCNs are designed to provide efficient and reliable communication in order to improve road safety, traffic efficiency, and the overall driving experience [1]. There are two main types of VCNs: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. V2V communication enables vehicles to communicate with each other and exchange information such as location, speed, and direction. This type of communication can be used to alert drivers to critical events on the road, such as an upcoming intersection or a vehicle stopped ahead [2]. V2I communication, on the other hand, enables vehicles to communicate with roadside infrastructure, such as traffic lights and sensors, in order to improve traffic flow and reduce congestion [3].

As a relatively recent type of networks, VCNs are vulnerable to cyberattacks, which can compromise the safety

and privacy of drivers and passengers [4]. Therefore, security in VCNs is crucial and needs to be ensured at the highest level. Authentication is one of the four main properties of security that need to be preserved in any secure system. Authentication verifies the identities of entities in VCNs, such as vehicles, infrastructure, and users before granting them access to the network. This helps to prevent unauthorized access and misuse of network resources. Authentication further provides secure access control, protects against impersonation attacks, safeguards sensitive data, and ensures trust in the system. Generally, authentication schemes were mainly studied at the higher layer of protocol stacks where predefined secrets (i.e., passwords, keys, signatures) are utilized for this purpose. The secrets are encrypted and decrypted via various cryptographic measures [5]. However, some instances in the literature reported breaching cryptographic measures through brute force attacks [6]. Therefore, alternative security mechanisms are now being evaluated. One such (promising) mechanism lies in the physical layer. Authentication at the physical layer is known as physical layer authentication (PLA) where the randomness in the characteristics of the physical layer is exploited. This randomness is mainly incurred in the wireless channel or hardware. There are a variety of fingerprints/features exploited for PLA, including channel impulse response, channel frequency response, received signal strength indicator, transmission coefficient (S21), pathloss, I/Q imbalance, carrier offsets [7, 8].

A. Related Work

The authors in [9] use the angle of arrival of the transmitter vehicle as a feature at the physical layer for authentication in the V2X environment. This work assumes that the location information of the transmitter node is available at the receiver and therefore expects a ground truth. This assumption is not realistic as there is no mechanism for ground truth tracking, and the effect of mobility is not discussed.

Similarly, the authors in this paper [10] proposed using physical layer characteristics for authentication and then using the Kalman filter to refine the iterative and threshold model. The iterative model estimates the priori and posteriori of the current time based on the physical layer characteristics of the previous time, serving as the basis for the authentication process. The threshold model analyzes the mathematical characteristics of the priori estimation and provides a calculation

method for the authentication threshold. The authors also used an extended Kalman filter and unscented Kalman filter for nonlinear physical layer characteristics.

In [11], the authors proposed a novel authentication approach, referred to as Hopper-Blum based physical layer (HB-PL) authentication scheme, which incorporates an advanced physical layer key generation technique with the Hopper-Blum (HB) authentication scheme. In this scheme, information gathered from the shared channel is utilized as secret keys for the HB scheme, while the mismatched bits are applied as induced noise for solving the learning parity with noise (LPN) problem. The primary objective of the proposed technique is to offer a solution for the bit reconciliation process while ensuring that no information is exposed on a public channel.

The work [12] provides a PLA scheme that utilizes Gaussian process (GP) path loss prediction and channel state information (CSI) to track changes in channel characteristics and predict the next path loss (PL) of the signal from a transmitter for authentication. The scheme maps historical CSI attributes to PL features of the transmitter's signal to predict the next PL, which is then used to cross-verify the transmitter's reported location information [13].

More recently, the authors in [14] proposed a cross-layer authentication scheme for vehicular communication that uses short-term reciprocal features of the wireless channel to re-authenticate the corresponding terminal. By utilizing the reciprocal features of the wireless channel, the scheme aims to reduce the overall complexity and computation and communication overheads required for authentication.

B. Contribution

In this work, we systematically adopt a novel approach exploiting the position of the transmitter node as a feature/fingerprint for authentication in V2I communication. Although position/location is very recently reported for PLA in underwater acoustic communication networks [15], the scheme is limited to stationary nodes scenario. In this work, we assume a dynamic vehicular environment where vehicles are not stationary but moving at a certain speed. The main contributions of this work can be summarized as follows:

- We estimate the position of the transmitter nodes by using Time-of-Arrival (ToA) based localization method, where ToAs are estimated at the corresponding RSUs using the maximum likelihood approach and the coordinates are extracted at BS using the least square approach.
- We construct a test statistic on the extracted coordinates/estimated position for a binary hypothesis test to decide the legitimacy of the transmitter vehicle. To deal with the challenge of the mobility of the vehicle in hypothesis testing, we propose a machine-learning model to track the mobility of the legitimate node and predict the next position of the vehicle.

C. Organization

The rest of this paper is structured as follows: In Section II, we describe our system model. Section III presents the

proposed physical layer authentication (PLA) scheme including position estimation, hypothesis testing, and the machine learning model. Section IV presents the evaluation results of our proposed technique. Lastly, Section V concludes the paper with a few final remarks and suggestions for future research directions.

II. SYSTEM MODEL

We assume the uplink transmission in a 2D V2I environment where vehicles are communicating with the RSUs to inform the central system (i.e., BS) about its parameters (speed, engine transmissions, fuel level, etc.) for congestion control or traffic management. We further assume that RSUs are deployed at fixed locations on both sides of the road and are connected to the BS as illustrated in Fig. 1. We assume two

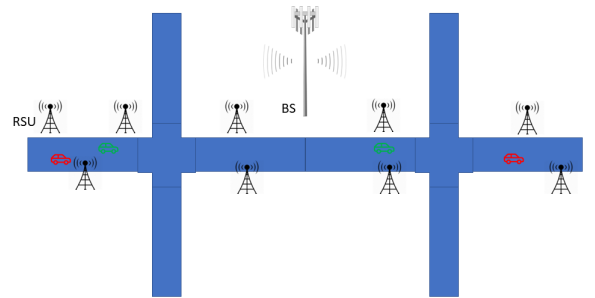


Fig. 1: An Illustration of our System Model

kinds of vehicles: legitimate vehicles and malicious vehicles. We assume a time-slotted communication system with no collision domain, i.e., only one transmitter node transmits at a given time slot. We assume that the malicious transmitter vehicle is smart enough and transmits in idle slots with the same transmit power as the legitimate vehicle so that she remains hidden in the network. All the RSUs are assumed to be connected with BS via an error-free secured communication link. We assume the malicious vehicle attacks on the vehicles to RSUs links. Such attacks are often known as impersonation attacks.

III. PROPOSED AUTHENTICATION SCHEME

The proposed physical layer authentication scheme consists of three main components as depicted in Fig. 2. We discuss the functionality of each component in detail in the following subsections.

A. Position Estimation

The estimation of the position of the transmitter vehicle is accomplished in two stages: distance estimation and coordinates extraction.

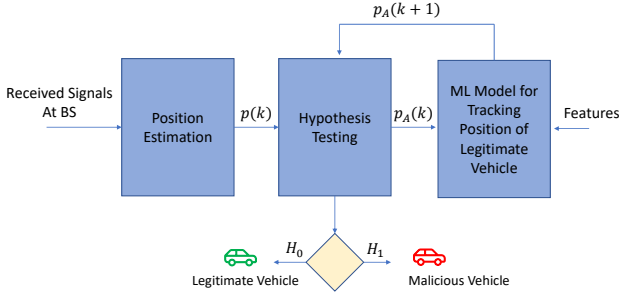


Fig. 2: Proposed Methodology

1) *Distance Estimation:* The distances at RSUs are estimated from the ToAs. Let \hat{t}_j be the estimated ToA at j -th RSU, which can be expressed as:

$$\hat{t}_j = \underset{t_j}{\operatorname{argmax}} \log f_{\mathbf{y}}(\mathbf{y} | t_j) = \underset{t_j}{\operatorname{argmax}} L(\mathbf{y} | t_j), \quad (1)$$

where $L(\mathbf{y} | t_j)$ is the log-likelihood function of the conditional random event $\mathbf{y} | t_j$ with \mathbf{y} being the received symbols vector. According to the framework in [16], $\hat{t}_j \sim \mathcal{N}(t_j, \sigma_t^2)$, where $\sigma_t^2 = \frac{\sigma^2 \psi_j}{4P}$ is the CRB or variance of the estimator with noise power σ^2 , pathloss ψ_j and transmit power P . Next, we use the famous distance equation, i.e., $\hat{r}_j = c\hat{t}_j$, to estimate the distance between the transmitter vehicle and j -th RSU, where $c = 3 \times 10^8$ m/s is the speed of the RF-carrier. The estimated distance is distributed as $\hat{r}_j \sim \mathcal{N}(r_j, \sigma_r^2)$, where $r_j = ct_j$ is the actual distance and $\sigma_r^2 = \frac{c^2 \sigma_t^2 \psi_j}{4P}$ is the variance of the distance estimator.

2) *Coordinates Extraction:* Assuming $\mathbf{p}_j = [x_j \ y_j]^T$ is the position vector of the j -th RSU, and that $\mathbf{p} = [x \ y]^T$ is the unknown position vector or coordinates of the transmitter vehicle, the distance r_j between the two nodes as per the definition of Euclidean distance is $r_j = \sqrt{(x - x_j)^2 + (y - y_j)^2}$. As ToA is susceptible to measurement error, the estimated measurement based on multiplying v and t_j is denoted as $\hat{r}_j = r_j + n_j$. By squaring both sides, we get $\hat{r}_j^2 = (r_j + n_j)^2 = r_j^2 + 2n_j r_j + n_j^2$, which can be expressed as:

$$\hat{r}_j^2 = (x - x_j)^2 + (y - y_j)^2 + 2n_j \sqrt{(x - x_j)^2 + (y - y_j)^2} + n_j^2. \quad (2)$$

The equation set obtained from the Eq. 2 can be expressed in a matrix-vector format for every instance of " j_s " as:

$$\mathbf{A}\theta + \mathbf{n} = \hat{\mathbf{b}}, \quad (3)$$

where all the vectors and matrices are given below:

$$\mathbf{A} = \begin{bmatrix} -2x_1 & -2y_1 & 1 \\ \vdots & \vdots & \vdots \\ -2x_L & -2y_L & 1 \end{bmatrix}, \quad \hat{\mathbf{b}} = \begin{bmatrix} \hat{r}_1^2 - x_1^2 - y_1^2 \\ \vdots \\ \hat{r}_L^2 - x_L^2 - y_L^2 \end{bmatrix}, \quad \theta = \begin{bmatrix} x \\ y \\ x^2 + y^2 \end{bmatrix},$$

$$\mathbf{b} = \begin{bmatrix} r_1^2 - x_1^2 - y_1^2 \\ \vdots \\ r_L^2 - x_L^2 - y_L^2 \end{bmatrix}, \quad \text{and } \mathbf{n} = \begin{bmatrix} 2n_1 \sqrt{(x - x_1)^2 + (y - y_1)^2} + n_1^2 \\ \vdots \\ 2n_L \sqrt{(x - x_L)^2 + (y - y_L)^2} + n_L^2 \end{bmatrix}.$$

Eq. 3 is a linear least square problem, where $\hat{\mathbf{b}}$ is the noisy observation vector. The solution for θ that minimizes the least square sum $\|\mathbf{A}\theta - \hat{\mathbf{b}}\|_2^2$ that can be obtained as:

$$\mathbf{A}^T \mathbf{A} \hat{\theta} = \mathbf{A}^T \hat{\mathbf{b}}, \implies \hat{\theta} = (\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T \hat{\mathbf{b}}. \quad (4)$$

The solution can be represented via Pseudo-Inverse as:

$$\hat{\theta} = \mathbf{A}^\dagger \hat{\mathbf{b}}. \quad (5)$$

The position estimate can be obtained from the first and second entries of $\hat{\theta}$ as: $\hat{\mathbf{p}} = [[\hat{\theta}]_1 \ [\hat{\theta}]_2]^T$. where $[\hat{\theta}]_1 = \hat{x}$, and $[\hat{\theta}]_2 = \hat{y}$. To determine the distribution of $\hat{\mathbf{p}}$, let's define $\hat{\mathbf{A}}^\dagger$ as \mathbf{A}^\dagger with dimensions of $2 * L$. Then the extracted estimated coordinates $\hat{\mathbf{p}}$ can be written based on eq. 5 with an addition of the uncertainty as:

$$\hat{\mathbf{p}} = \hat{\mathbf{A}}^\dagger \hat{\mathbf{b}} + \hat{\mathbf{A}}^\dagger \mathbf{n} \quad (6)$$

B. Hypothesis Testing

At this stage, we need to classify the estimated position at the BS into a legitimate vehicle and a malicious vehicle. Assuming \mathbf{x}_A represents the vector of actual coordinates for a legitimate node and \mathbf{x}_E represents the vector for a malicious node, we define \mathcal{H}_0 as the null hypothesis, indicating that the transmitter is the legitimate node, and \mathcal{H}_1 as the alternate hypothesis, suggesting that the transmitter is the malicious node. Then test statistics can be defined as:

$$\text{TS} = \|\hat{\mathbf{p}} - \hat{\mathbf{p}}_A\|_2. \quad (7)$$

where $\hat{\mathbf{p}}_A$ is the ground truth provided by ML model. The binary hypothesis test can be defined as

$$\begin{cases} \mathcal{H}_0(\text{no impersonation}) : & \text{TS} = \|\hat{\mathbf{p}} - \hat{\mathbf{p}}_A\|_2 < \epsilon_{th} \\ \mathcal{H}_1(\text{impersonation}) : & \text{TS} = \|\hat{\mathbf{p}} - \hat{\mathbf{p}}_A\|_2 > \epsilon_{th} \end{cases}, \quad (8)$$

where ϵ_{th} is a predetermined threshold. The binary hypothesis testing could also be defined as follows:

$$\text{TS} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \epsilon_{th}. \quad (9)$$

C. ML Models for Mobility Tracking

Mobility is a major challenge in VCNs. Typically, in PLA, one needs to get the ground truth information of the legitimate node in advance. In this work, to track the mobility pattern of the legitimate vehicle or get information about the ground truth of the legitimate vehicle, we employ the ML model(s).

Generally, mobility models generate mobility traces by continuously predicting the next locations of the nodes. Such a location prediction process is basically a regression problem. Hence, in this work, we use support vector regression (SVR) and decision tree (DT) as ML model(s). To train our models, we use eight input features: link quality (LQ), three TOAs and their three differences at the corresponding RSUs, and the current position of the vehicle to train our model. Our ML model(s) structure is shown in Fig. 3. Note that we do not need extra efforts or estimation mechanisms to acquire these features as they are already available to BS. SVR is based on support vector machines (SVMs), which use a distinctive method for handling anticipated values that involves establishing a tolerance margin and predicts continuous output values differently than prior regression techniques. In this work, the trained SVR is used to forecast the output values for the x - and y -coordinates. Due to its decreased sensitivity to outliers and capacity to handle datasets with high-dimensional features, SVR is considered superior to other regression techniques. On the other hand, the decision tree (DT) regression approach divides the input data into smaller subgroups according to the values of the input features in order to forecast the outcome variable. DT can make precise, comprehensible forecasts.

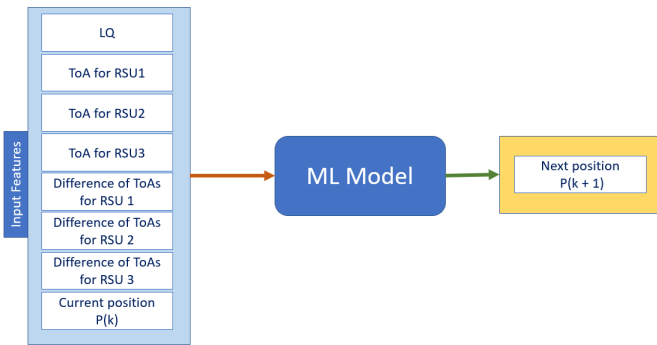


Fig. 3: Model Structure

IV. SIMULATION

A. Setup

To evaluate the performance of our authentication scheme, we use MATLAB. Unless stated otherwise, the simulation parameters are listed in TABLE I. We consider a long linear road of size $3000m \times 20m$. We deploy RSUs at both sides of the road at fixed positions, i.e., we separate any two RSUs at each roadside by 300m. We assume RSUs are in LoS and with a distance from the transmitter vehicle of less than 400m. Furthermore, we consider both vehicles moving at a certain speed. We assume that the malicious vehicle is smart enough and exactly following the legitimate node in speed and direction so that she can enhance the chances of missed detection. We also implement a scheme from the literature as a baseline scheme [9] that uses the angle of arrival for authentication. It is implemented in MATLAB with the assumption that the actual ground truths of a moving legitimate

vehicle are already available at BS. This assumption is taken because there is no explicit mechanism provided in [9] to track or acquire the ground truths for a moving legitimate vehicle.

Parameter(s)	Value
Road Dimensions (Length and Width)	3000 m and 20 m
Legitimate node position	[1,10]
Malicious node position	[0,10]
Speed of the vehicle	1m/s
Frequency	18×10^8 Hz
path loss exponent	2
Transmission power	100mW
Noise power	$\frac{P}{LQ}$

TABLE I: Monte Carlo Simulation Parameters

1) *Dataset*: We generated a dataset for input features size of $9 \times 3.15 \times 10^5$ and output labels of size $2 \times 3.15 \times 10^5$. We randomly deploy 100 RSUs in a 2D region of size $5km \times 5Km$, define the starting position of the legitimate vehicle at a random position, and select the closest RSUs in LoS, which are under a predefined range, i.e., 400m. Next, we vary the LQ in the unit step from 0dB to 20 dB, and for each LQ, We vary the speed of the legitimate vehicle from 0 – 33mps (0-120kmph) randomly according to a uniform distribution. We then record the ToA for the selected three RSUs along with their differences (i.e., ToA in the previous slot subtracted from ToA in the current slot) and the extracted coordinate in k -th slot.

2) *ML Models Configurations*: We use sequential minimal optimization (SMO) as a solver with loss function as MSE, given in Eq. 13 for SVR and least-square solver for DT. Note that these are default solvers used by MATLAB. We randomly divided the whole dataset into 0.7 and 0.3 segments for training and testing, respectively.

B. Performance Evaluation Metrics

1) *Analytical Model*: The performance metrics for the analytical model we adopt in this paper (i.e., hypothesis testing) are two error probabilities: the probability of false alarm P_{fa} and the probability of missed detection P_{md} . The probability of false alarm is defined as the probability of incorrectly classifying a legitimate node as malicious during the binary hypothesis test, which can be expressed as:

$$P_{fa} = P[TS | \mathcal{H}_0 \geq \epsilon_{th}] = \int_{\epsilon_{th}}^{\infty} f_{TS|\mathcal{H}_0}(ts | h_0) d_{ts|h_0} \quad (10)$$

The probability of missed detection is the probability of incorrectly classifying a malicious node as legitimate during the binary hypothesis test, which can be expressed as:

$$P_{md} = P[TS | \mathcal{H}_1 \leq \epsilon_{th}] = \int_0^{\epsilon_{th}} f_{TS|\mathcal{H}_1}(ts | h_1) d_{ts|h_1} \quad (11)$$

Note that the probability density functions ($f_{TS|\mathcal{H}_0}(ts | h_0)$ and $f_{TS|\mathcal{H}_1}(ts | h_1)$) are very challenging to find. We believe this requires dedicated long efforts to find out the nature of the conditional events (TS | \mathcal{H}_0 and TS | \mathcal{H}_1) and thus their density functions due to unknown uncertainty in the ground truths provided by the ML model and inherent uncertainty in the test statistics. Therefore, we compute these probabilities empirically in the simulations.

2) *ML Model*: Mean squared error (MSE), mean absolute error (MAE), and coefficient of determination R^2 are used as performance metrics to evaluate the performance of both SVR and DT models.

MAE measures how far apart the expected and actual values are. The MAE can be expressed as:

$$\text{MAE} = \frac{1}{2n} \sum_{i=1}^n \|\mathbf{p}_A^i - \hat{\mathbf{p}}_A^i\|_1, \quad (12)$$

where \mathbf{p}_A^i and $\hat{\mathbf{p}}_A^i$ stand for the i -th observation's actual value and predicted value, respectively, while n indicates the total number of observations and $\|\cdot\|_1$ denotes l_1 norm operation.

MSE represents the difference between real and anticipated values, which can be mathematically defined as:

$$\text{MSE} = \frac{1}{2n} \sum_{i=1}^n \|\mathbf{p}_A^i - \hat{\mathbf{p}}_A^i\|_2^2, \quad (13)$$

where $\|\cdot\|_2$ denotes l_2 norm operation. Finally, the coefficient of determination R^2 expresses how much of the variation in the dependent variable can be predicted from the independent variables. An R^2 value close to 1 indicates better performance, whereas an R^2 value significantly close to 0 indicates worse performance. The following defines the equation for R^2 :

$$R^2 = 1 - \frac{\text{SS}_{\text{res}}}{\text{SS}_{\text{tot}}} \quad (14)$$

where SS_{tot} is the total sum of squares and SS_{res} is the sum of squared residuals.

C. Results

1) *Error behavior against link quality (LQ)*: In this section we evaluate the performance of both error probabilities against LQ. We define LQ as the ratio of transmit power and noise power. Typically, to measure the LQ, a ratio of received power and noise power is taken but in our case due to multiple receivers (RSUs) a common variable is the ratio of transmit power and noise power among them, therefore, we redefine LQ as per our system model. We sweep the LQ parameter from the 0 dB to 20 dB range in Figures 4, 5, and keep 1m separation between legitimate and malicious vehicles. We observe as the LQ enhances both errors decrease for our proposed scheme. On the other hand, if the design parameters of test statics, i.e., ϵ_{th} increases then a decrease in the probability of false alarm but an increase in the missed detection can be observed. We also investigate the impact of the velocity of the transmitter vehicles on the error probabilities. We notice that the increase in velocity has a positive impact (i.e., decreases in error) on the probability of missed detection but a slight negative impact on the probability of false alarm. We also observe that the baseline scheme provides a very low false alarm for the same set of parameters but collapses on the probability of the missed detection which is an important or critical probability. The collapse (increase in error with the increase in LQ) of a fingerprint occurs when the fingerprints of both nodes are too close and the proposed scheme is unable to differentiate them.

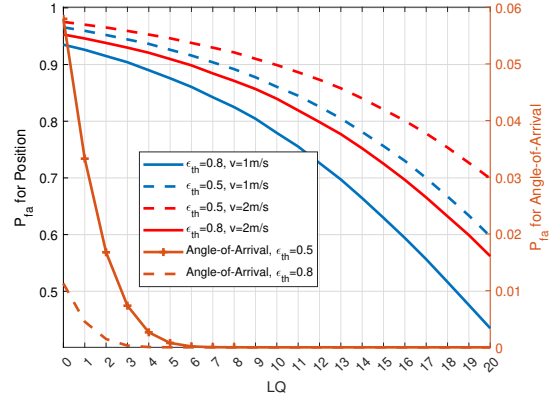


Fig. 4: P_{fa} vs LQ[db]

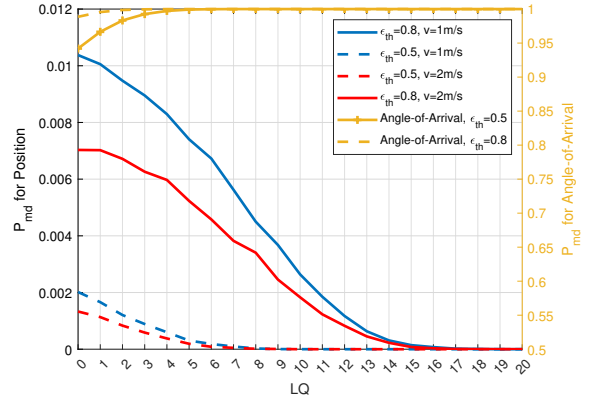


Fig. 5: P_{md} vs LQ[db]

2) *Receiver Operating Characteristic (ROC) curve*: ROC curves provide a comprehensive overview of our model, which allows us to evaluate the performance of our authentication scheme w.r.t. both errors. It shows the relationship between the detection rate (true positive) and the false alarm rate (false positive). ROC is generated by varying the threshold ϵ_{th} over a long range and then for every single value of ϵ_{th} , both errors are recorded in arrays, and then plotted against each other. In Fig. 6, we observe that the LQ has a positive impact on the detection rate ($P_d = 1 - P_{md}$), the increase in LQ enhances the detection rate enhances. One can also see the impact of the speed of vehicles on the detection rate. Overall, speed has a negative impact on the performance of the proposed scheme.

3) *ML Models Performance Results*: We present the performance of the above-mentioned two ML models in TALBE II based on the test dataset of size 9×10^5 generated as per the considered mobility pattern. Note that root MSE (RMSE)

Model	RMSE	MSE	MAE	R^2
DT	0.40837	0.166765	0.227203	0.498604
SVR	0.27982	0.078298	0.169555	0.764588

TABLE II: Comparison between DT and SVR based on RMSE, MSE, MAE, and R^2

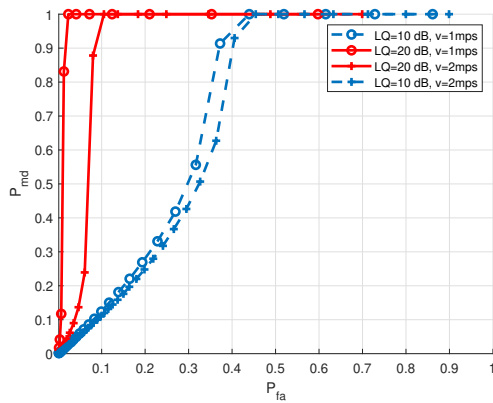


Fig. 6: ROC: P_d vs P_{fa}

is the square root of MSE. Overall, SVR model's predictions appear to have better performance than DT model. As a result, it is more suitable for this study based on RMSE, MSE, MAE, and R^2 measurements.

V. CONCLUSION

In this paper, we developed a novel hybrid physical layer authentication scheme with ML for V2I communication that uses the location of the transmitter as a fingerprint. We consider a dynamic environment for transmitter vehicles where nodes are mobile. The proposed authentication scheme is tested against various parameters of the system, i.e. speed of the vehicles, link quality, and controlled parameter threshold. The performance is also compared with a baseline scheme that exploits the angle of arrival as a device fingerprint. We showed that position is a strong candidate feature for PLA, where one can achieve high detection rates even at with low link quality.

This work can be extended by studying our proposed scheme with more realistic and non-linear mobility models, and trying more ML models for better accuracy. Similarly, this work can be extended by incorporating multiple legitimate and malicious vehicles, which is novel in the context of PLA in VCNs.

REFERENCES

- [1] S. Zeadally, M. A. Javed, and E. B. Hamida, "Vehicular communications for its: Standardization and challenges," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 11–17, 2020.
- [2] A. Bazzi and B. M. Masini, "Taking advantage of v2v communications for traffic management," in *2011 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2011, pp. 504–509.
- [3] M. N. Tahir, P. Leviäkangas, and M. Katz, "Connected vehicles: V2v and v2i road weather and traffic communication using cellular technologies," *Sensors*, vol. 22, no. 3, p. 1142, 2022.
- [4] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity chal-

- lenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.
- [5] M. A. Alia, A. A. Tamimi, and O. N. AL-Allaf, "Cryptography based authentication methods," in *Proceedings of the world congress on engineering and computer science*, vol. 1, 2014, pp. 1–6.
- [6] C. Gidney and M. Ekerå, "How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021.
- [7] N. Wang, W. Li, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical layer authentication for 5g communications: Opportunities and road ahead," *IEEE Network*, vol. 34, no. 6, pp. 198–204, 2020.
- [8] W. Aman, S. Al-Kuwari, M. Muzzammil, M. M. U. Rahman, and A. Kumar, "Security of underwater and air-water wireless communication: State-of-the-art, challenges and outlook," *Ad Hoc Networks*, vol. 142, p. 103114, 2023.
- [9] A. Abdelaziz, C. E. Koksal, R. Burton, F. Barickman, J. Martin, J. Weston, and K. Woodruff, "Beyond pki: Enhanced authentication in vehicular networks via mimo," in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE, 2018, pp. 1–5.
- [10] J. Wang, Y. Shao, Y. Wang, Y. Ge, and R. Yu, "Physical layer authentication based on nonlinear kalman filter for v2x communication," *IEEE Access*, vol. 8, pp. 163 746–163 757, 2020.
- [11] A. K. Jadoon, J. Li, and L. Wang, "Physical layer authentication for automotive cyber physical systems based on modified hb protocol," *Frontiers of Computer Science*, vol. 15, pp. 1–8, 2021.
- [12] D. Xu and J. A. Ritcey, "Post-quantum phy-layer authentication for secure initial access in v2x communications," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 1758–1762.
- [13] M. Umar, J. Wang, L. Liu, Z. Guo, and S. Wang, "Physical layer authentication in the internet of vehicles based on signal propagation attribute prediction," *Journal of Networking and Network Applications*, vol. 3, no. 1, pp. 1–10, 2023.
- [14] M. A. Shawky, M. Bottarelli, G. Epiphaniou, and P. Karadimas, "An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, 2023.
- [15] W. Aman, S. Al-Kuwari, and M. Qaraqe, "Location-based physical layer authentication in underwater acoustic communication networks," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, 2023, pp. 1–6.
- [16] W. Aman, M. M. U. Rahman, J. Qadir, H. Pervaiz, and Q. Ni, "Impersonation detection in line-of-sight underwater acoustic sensor networks," *IEEE Access*, vol. 6, pp. 44 459–44 472, 2018.