Efficient Cross-Layer Handover Authentication for Secure Communication in VANETs

Mahmoud A. Shawky[†], Mohammad Al-Quraan[†], Mohammad Abualhayja'a[†], Khaled Alblaihed[†], Ahmed Adel[‡], Ahmed Gamal[§], Khalid Mostafa[‡], Jaspreet Kaur[†], Ahmad Taha[†], Syed T. Shah[*], Shuja Ansari[†], Qammer Abbasi[†]
[†] University of Glasgow, Glasgow, G12 8QQ, United Kingdom, m.shawky.1@research.gla.ac.uk
[‡] Faculty of Engineering, Ain Shams University, Cairo, 11566, Egypt
[§] Faculty of Engineering, Alexandria University, Alexandria, 21526, Egypt
[*] School of Computer Science and Electronic Engineering, University of Essex, Colchester, UK

***Abstract*—This paper addresses the critical need for secure and resilient handover authentication processes in modern vehicular communication systems, characterised by low latency and high reliability. Introducing a cross-layer handover technique, our approach utilises a physical layer handover method leveraging the substantial decorrelation of channel responses between diverse network terminals. Emphasising the lightweight nature of the solution, our method ensures efficient authentication during vehicular handovers. The proposed methodology, validated through experimental analysis, offers a promising solution to the increasing challenges posed by wireless communication vulnerabilities in the context of modern vehicles.**

***Index Terms*—Handover, Machine learning, PHY-layer authentication, Support vector machine, VANET, 5G-V2I.**

I. Introduction

According to the "2nd Global Status Report on Road Safety," road traffic accidents are anticipated to become the fifth leading cause of death by 2030, resulting in approximately 1.3 million deaths annually, with more than 3000 fatalities daily [1]. Vehicular ad-hoc networks (VANET) play a crucial role in supporting vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [2], see Fig. 1. The vehicular communication employs the dedicated short-range communication protocol with vehicles transmitting traffic messages every $100:300$ milliseconds [3]. However, the open nature of wireless communication poses security challenges [4]. In addition, the high-frequency range of the 5G-V2I communication reduces cell coverage, increasing the number of cells and consequently the handover authentication rate. This underscores the necessity for reliable and lightweight authentication techniques that can be achieved by leveraging the spatial and temporal characteristics of wireless channels.

II. Methodology

The proposed approach incorporates the lightweight processing of the physical (PHY)-layer authentication with cryptographic security robustness, introducing a scalable handover solution. Upon successful PHY-layer authentication, the delegation of trust occurs from the authenticated RSU (R_j) to the adjacent RSU (R_{j+1}). Accordingly, cryptographic authentication is initiated based on the PHY-layer handover outcome, as shown in Fig. 2. The following subsections detail the PHY-layer and crypto-based methodologies. Note that, we assume a low channel variation environment, specifically in rural areas.

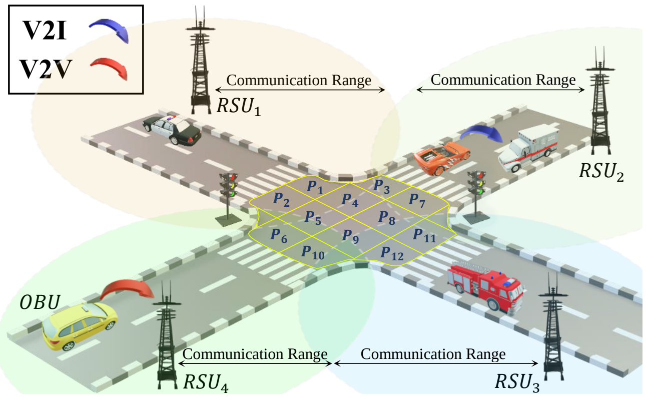

Fig. 1: System architecture.

A. The PHY-layer handover method

This method relies on the high decorrelation coefficient observed in the channel responses between the vehicle V_i and R_j, and that between V_i and R_{j+1} at time instance t, where R_j and R_{j+1} are separated by a distance of $\geq \lambda/2$. This approach comprises offline and online phases, outlined as follows.

1) The offline phase: During this phase, the intersection area between the coverage zones of R_j and R_{j+1} is partitioned into L positions with an inter-position spacing of x meters, see Fig. 1. This designated region is denoted as "the mapped area." The following describes the stages involved in this phase.

- *Channel mapping*: This stage has the following steps.
  1) *Step 1*: In each position P_l, the channel is probed M times by the transmitter Tx located in P_l and received by two receivers representing R_j and R_{j+1}. This process yields a set of M channel estimates, denoted as $Ch_{R_j}^{T_m}$ and $Ch_{R_{j+1}}^{T_m}$, recorded at the timestamp T_m. This probing step is repeated for each position P_l, where l ranges from 1 to L.
  2) *Step 2*: In this step, the mapped estimates are obtained and represent the data set, formulated as $DS = \{\{Ch_{R_j}^{T_1}, Ch_{R_{j+1}}^{T_1}\}, \cdots, \{Ch_{R_j}^{T_M}, Ch_{R_{j+1}}^{T_M}\}\}$.
- *ML training*: In this stage, the obtained DS is used for training the machine learning models in R_j and R_{j+1}.

2) The online phase: This phase is executed when a moving vehicle V_i is authenticated for R_j and moving towards R_{j+1}, involving the following stages.

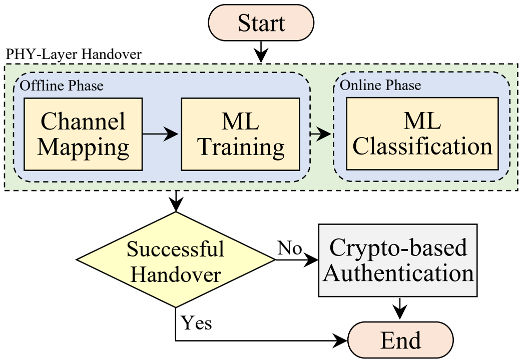

Fig. 2: Flowchart of the proposed method.

- *Stage 1*: In this stage, the moving vehicle V_i, located in a specific location P_l, sends a handover authentication request $\langle Cert_{V_i}, PP, P_l, T_1, \sigma_{V_i} \rangle$, where $Cert_{V_i}$ is V_i's certificate, PP is the probing packet, σ_{V_i} is the V_i's signature at timestamp T_1.
- *Stage 2*: In this stage, R_j and R_{j+1} computes its related channel estimates $\hat{Ch}_{R_j}^{T_1}$ and $\hat{Ch}_{R_{j+1}}^{T_1}$, respectively. Then, R_j sends $\langle Cert_{V_i}, \hat{Ch}_{R_j}^{T_1} \rangle$ to R_{j+1} via a secure channel.
- *Stage 3*: Once R_{j+1} receives $\hat{Ch}_{R_j}^{T_1}$ from R_j, it uses $\{\hat{Ch}_{R_j}^{T_1}, \hat{Ch}_{R_{j+1}}^{T_1}\}$ as an input to the trained machine learning model, obtaining the classified position $\hat{P}_l$.
- *Stage 4*: Under binary hypothesis testing, if $\hat{P}_l \overset{?}{=} P_l$, the delegation of trust occurs. Otherwise, the crypto-based authentication is executed.

B. The crypto-based authentication method

This method is considered a public key infrastructure-based authentication in which R_{j+1} checks if $Cert_{V_i}$ is in the revocation list to verify V_i's legitimacy. Then, R_{j+1} check the freshness of T_1, avoiding replay attacks. Next, it verifies σ_{V_i}. If the crypto-based authentication happened, then the ML model is retrained with the new data set $\{\hat{Ch}_{R_j}^{T_1}, \hat{Ch}_{R_{j+1}}^{T_1}\}$.

III. Results and Discussion

For performance evaluation, an experiment is conducted using LabView and two universal software radio peripherals (USRPs) Ettus X300 at the University of Glasgow. The operating frequency is set at 3.75 GHz, employing an orthogonal frequency division multiplexing (OFDM) communication system with 256 subcarriers. The inter-position spacing x is varied at values of 0.5, 0.75, and 1 meter for $L = 9$ positions, as depicted in Fig. 3. The experiment initiates with the transmission of $M = 500$ OFDM symbols as probing packets, capturing the received signal strength and channel phase responses for each channel associated with Rx_1 and Rx_2. For validation, 80% of the channel estimates are employed for ML training, while the remaining 20% is used for testing. Various ML algorithms, including support vector machine (SVM) among others, are tested, and the classification accuracy results are presented in Table I. It can be seen that SVM consistently achieves perfect accuracy at 1 m distance, while neural network and random forest models also exhibit high accuracy across all distances, with SVM outperforming other models overall. Furthermore, the classification accuracy decreases as the value of x decreases, highlighting the trade-off between accuracy and resolution.

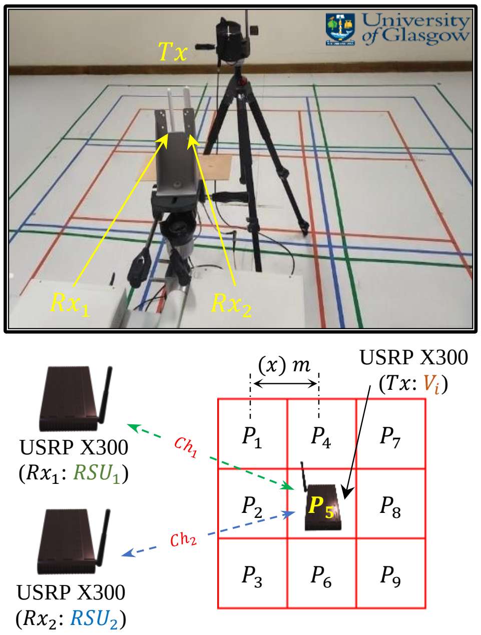

Fig. 3: Experimental setup for the implemented method.

TABLE I: Classification accuracy (%) for different ML models

Dist.	SVM	Neural Network	Random Forest	Decision Tree	Naïve Bayes
1 m	100	99.7 ± 0.1	98.6 ± 0.4	92.1 ± 0.9	88.1 ± 1.1
0.75 m	99.7 ± 0.1	99.1 ± 0.3	98.3 ± 0.4	89.2 ± 1	85.9 ± 1.2
0.5 m	96.9 ± 0.2	94.2 ± 0.8	98.2 ± 0.4	81.4 ± 1.3	76.9 ± 1.4

IV. Conclusions

The proposed method combines PHY-layer authentication and cryptographic security for efficient handovers in low channel variation conditions, reducing the signature verification overhead for each transmission. The delegation of trust occurs upon successful PHY-layer authentication. Experimental results illustrate high classification accuracy, with SVM consistently achieving perfect accuracy at a 1 m distance. The observed trade-off between accuracy and resolution underscores the method's efficiency in real-world applications.

References

[1] World Health Organization, "2nd Global Safety Report on Road Safety 2011-2020," 2020.

[2] M. A. Shawky et al., "Efficient Blockchain-Based Group Key Distribution for Secure Authentication in VANETs," *IEEE Networking Letters*, vol. 5, no. 1, pp. 64-68, Mar. 2023.

[3] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," Proc. IEEE, vol. 99, no. 7, pp. 1162-1182, Jul. 2011.

[4] M. A. Shawky et al., "Cross-Layer Authentication based on Physical-Layer Signatures for Secure Vehicular Communication," IEEE Intelligent Vehicles Symposium, Aachen, Germany, pp. 1315-1320, Jun. 2022.