Learning-based Rogue Edge Detection in VANETs with Ambient Radio Signals

Xiaozhen Lu*, Xiaoyue Wan*, Liang Xiao*†, Yuliang Tang*, Weihua Zhuang‡

*Dept. of Communication Engineering, Xiamen University, Xiamen, China. Email: lxiao@xmu.edu.cn
†The National Mobile Communications Research Laboratory, Southeast University, China.
‡Dept. of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada. Email: wzhuang@uwaterloo.ca

***Abstract*—Edge computing for mobile devices in vehicular ad hoc networks (VANETs) has to address rogue edge attacks, in which a rogue edge node claims to be the serving edge in the vehicle to steal user secrets and help launch other attacks such as man-in-the-middle attacks. Rogue edge detection in VANETs is more challenging than the spoofing detection in indoor wireless networks due to the high mobility of onboard units (OBUs) and the large-scale network infrastructure with roadside units (RSUs). In this paper, we propose a physical (PHY)-layer rogue edge detection scheme for VANETs according to the shared ambient radio signals observed during the same moving trace of the mobile device and the serving edge in the same vehicle. In this scheme, the edge node under test has to send the physical properties of the ambient radio signals, including the received signal strength indicator (RSSI) of the ambient signals with the corresponding source media access control (MAC) address during a given time slot. The mobile device can choose to compare the received ambient signal properties and its own record or apply the RSSI of the received signals to detect rogue edge attacks, and determines test threshold in the detection. We adopt a reinforcement learning technique to enable the mobile device to achieve the optimal detection policy in the dynamic VANET without being aware of the VANET model and the attack model. Simulation results show that the Q-learning based detection scheme can significantly reduce the detection error rate and increase the utility compared with existing schemes.**

***Index Terms*—VANETs, rogue edge detection, ambient radio signals, reinforcement learning, PHY-layer authentication.**

I. Introduction

With the development of computation intensive applications such as augmented reality techniques, mobile devices such as smart watches and smartphones can offload the computation tasks to the onboard units (OBUs) in vehicular ad hoc networks (VANETs) to utilize the computation, power, and storage resources of the edge node that can be an access point (AP) or even a laptop in the vehicle. The edge computing significantly reduces the processing delay, increases the battery lifetime, and reduces the privacy risks at cloud. The edge computing in VANETs has to address the rogue edge attacks. As a special type of spoofing attackers, an attacker can send spoofing signals to the mobile device claiming to be the serving edge node in the vehicle. Rogue edge attacks can result in the privacy leakage risks and further lead to man-in-the-middle attacks or denial-of-service (DoS) attacks [1].

Existing VANET authentication involves cryptography, trust, and certificate [2], [3]. However, mobile devices with restricted computation, storage and battery life in VANETs prefer to apply the lightweight authentication protocols that is robust against insider attacks. This issue can be addressed by physical (PHY)-layer authentications, which depend on the spatial distribution of the PHY-layer properties of wireless transmissions, such as received signal strength (RSS) of the message signals, received signal strength indicator (RSSI) [4], the channel impulse responses of the radio channels [5]–[7], and the ambient radio signals [8], [9]. For instance, the Q-learning based authentication with the ambient radio signals (QAAS) scheme as proposed in [9] and the Q-learning based authentication with RSSI (QAR) scheme as developed in [4] enable a wireless device to detect spoofing in indoor wireless networks without being aware of the radio propagation model and the spoofing model. However, these PHY-layer authentication techniques usually have degraded detection performance of the edge offloading in VANETs that has higher mobility and more strict resource constraints than the indoor wireless networks [10].

In this paper, we propose a rogue edge detection scheme for VANETs that exploits the spatial decorrelation of the ambient radio signals received by both the mobile device and the serving edge node. More specifically, both the mobile device and the serving edge node in a vehicle have the same location tracing and thus received radio signals from the same ambient radio sources along the road, such as the base stations (BSs), APs, and the roadside units (RSUs). On the other hand, a rogue node Eve located outside the serving vehicle of the target mobile device Bob cannot receive the same ambient radio signal trace with the legal edge node Alice during a long enough time. For example, Eve cannot obtain the radio signal sent from a RSU that she has never been close to while the serving vehicle of Alice does.

Both the legal edge node and the mobile device can extract the PHY-layer properties such as RSSIs of the ambient radio signals that are sent from multiple ambient radio sources such

This work was supported in part by the National Natural Science Foundation of China under Grant 61671396 and 91638204, the open research fund of National Mobile Communications Research Laboratory, Southeast University (No.2018D08).

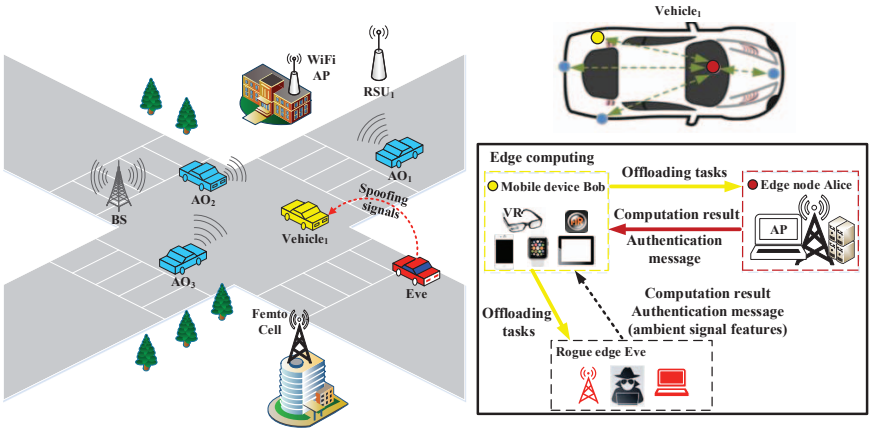


Fig. 1: Detection of rogue edge in VANETs based on the PHY-layer information of the ambient radio signals, in which mobile device Bob compares the PHY-layer information of the ambient radio signals received by the edge node under test with his copy to detect Eve.

as the ambient BSs, APs and RSUs at different locations. Bob asks the edge node under test to provide such PHY-layer information of the ambient radio signals for a given time duration and sends spoofing alarms if the received information is very different from his record. Compared with the traditional PHY-layer authentication that depends on a single radio transmitter, this scheme relies on more radio sources and more PHY-layer information to improve the detection accuracy.

The rogue edge detection has to choose the spoofing detection mode such as the length of the ambient signal PHY-layer trace and the test threshold in the detection in a dynamic VANET against a rogue edge node with time-varying frequency to send spoofing messages. The decision can be made according to the reinforcement learning such as Q-learning to achieve the optimal strategy via trials as the repeated spoofing detection game can be formulated as a Markov decision process (MDP). In this scheme, a mobile device applies Q-learning to choose the spoofing detection mode and the test threshold without knowing the network model and the attack model in dynamic VANET. Simulations based on learning-based rogue edge detection scheme are performed, showing that our proposed scheme exceeds the benchmark schemes such as QAR in [4] and QAAS in [9] with lower spoofing detection error and higher utility. The contributions of this work can be summarized as follows:

- We propose a PHY-layer rogue edge detection scheme based on ambient radio signals and the RSSI of packets that usually ignored in VANETs and formulate the rogue edge detection process as a dynamic spoofing detection game.
- We present a Q-learning based authentication scheme with RSSI and ambient radio signals to detect rogue edge in VANETs.

The rest of this paper is organized as follows. We review the related work in Section II and present the system model in Section III. We propose a PHY-layer rogue edge detection scheme with Q-learning in VANETs in Section IV and provide simulation results in Section V. Finally, conclusion is drawn in Section VI.

II. Related work

The channel impulse response (CIR) based authentication presented in [11] uses the two-dimension CIR quantization scheme and the logarithmic likelihood ratio test to reduce the false alarm rate in wireless communications. The PHY-layer challenge-response authentication proposed in [12] for orthogonal frequency division multiplexing systems modulates the challenge and response messages to improve the authentication accuracy. The AP localization framework proposed in [13] exploits the channel state amplitude and phase to improve the localization accuracy for the RSS-based localization in wireless local area networks.

The ProxiMate system in [14] uses both ambient TV and FM radio signals for secure pairing and reduces the authentication error rates. The proximity test based on the infinite Gaussian mixture model in [8] exploits the PHY-layer features of the shared ambient radio signals of radio clients to improve the authentication accuracy in wireless networks. The active authentication proposed in [9] that utilizes the RSSIs of the ambient radio signals to detect spoofing mobile devices can provide accurate proximity test for indoor wireless networks.

The user-side authentication proposed in [15] that uses the global positioning system information to detect rogue APs in VANETs. The application-layer intrusion detection developed in [16] builds a hypothesis test to detect rogue nodes in VANETs. The certificateless aggregate signcryption in [3] uses RSUs for fog computing and storage units to reduce the computational cost of vehicular crowdsensing-based systems. The lightweight secure and privacy-preserving scheme in [17]

improves the reliability of the vehicle-to-grid connection and reduces the total communication and computation costs in VANETs.

III. System model

In this paper, we consider a mobile device (Bob) and the serving edge node (Alice) in a vehicle. Bob aims to offload real-time data such as pictures, videos and virtual reality information to Alice, and has to determine whether the edge node under test is indeed Alice instead of a rogue node (Eve) outside the vehicle with the goal to spoof Bob.

Equipped with computation and caching resources, the edge node can reduce the processing delay and save the computation energy consumption of the mobile device. These radio nodes (Alice and Bob) can receive the signals sent by the radio sources nearby, such as the ambient AP, BS, RSU, and OBUs along their traces, as shown in Fig. 1. Both Bob and Alice can observe the RSSI and arrival time of the ambient radio signals and their MAC addresses, which can be used to detect rogue nodes. Once receiving the message that contains the computation results of Alice, Bob has to detect whether the message is indeed sent by Alice.

The ambient radio environment of Bob, Alice and Eve changes over time due to the high mobility of OBUs. Both Bob and Alice can extract and store the PHY-layer properties such as RSSIs, MAC address and arrival time of the ambient radio signals that are sent from multiple ambient radio sources such as the ambient OBUs (AOs), BSs, WiFi APs and RSUs at different locations. Bob asks the edge node under test to provide the PHY-layer feature trace information of the ambient radio signals before offloading data. Upon receiving Bob's request, the edge node under detection sends a message about their feature trace information to Bob, and Bob compares the features trace of the edge node with his trace to identify their shared M ambient packets in each time slot.

Without loss of generality, the vehicle that carries both the mobile device and the edge node is assumed to move along the road at a speed denoted by $v_1^{(k)}$ at time slot k. Let $r^{(k)}(i)$ denote the RSSI of the i-th packet sent by the edge node under test at time slot k, with $1 \leq i \leq N$, where N is the number of the packets of the edge node under test. Let $\hat{r}(i)$ denote the RSSI record of the i-th signal sent by Alice at time slot k.

The rogue edge (Eve) is assumed to be located in another vehicle with moving speed denoted by $v_2^{(k)}$ at time slot k. By sending a spoofing message with Alice's MAC address, Eve aims to fool Bob with faked edge computation results or illegal access advantages. In this PHY-layer authentication framework, Eve has to provide the PHY-layer feature of the ambient radio signals to Bob in the spoofing signals. Denote the probability that Eve sends a spoofing message at time slot k as $y^{(k)} \in [0,1]$. Let $r_E^{(k)}(i)$ be the RSSI of the i-th packet sent by Eve at time slot k received by Bob.

Let $\hat{\mathbf{f}}^{(k)} = [\hat{r}_i^{(k)}, \hat{MAC}_i^{(k)}, \hat{t}_i^{(k)}]_{1\leq i\leq M}$ denote the feature trace record of Bob's ambient packets at time slot k, where $\hat{r}_i^{(k)}$, $\hat{MAC}_i^{(k)}$ and $\hat{t}_i^{(k)}$ are the RSSI, MAC address, and arrival time of the i-th ambient radio signal monitored by Bob, where M is the number of the ambient signals assigned by Bob. Similarly, let $r_i^{(k)}$, $MAC_i^{(k)}$ and $t_i^{(k)}$ denote the RSSI, MAC address, and arrival time of the i-th ambient packet monitored by the edge node under test. The ambient signal feature of the edge node under test denoted by $\mathbf{f}^{(k)} = [r_i^{(k)}, MAC_i^{(k)}, t_i^{(k)}]_{1\leq i\leq M}$ at time slot k.

TABLE I: Summary of symbols and notations

$r^{(k)}(i)$	RSSI of the i-th packet sent by the edge node under test at time slot k
$\hat{r}(i)$	RSSI record of the i-th signal sent by Alice at time slot k
$\hat{\mathbf{f}}^{(k)}$	Feature trace record of Bob's ambient packets at time slot k
$\mathbf{f}^{(k)}$	Ambient signal feature of the edge node under test at time slot k
$v_{1/2}^{(k)}$	Speed of the target/attack OBU at time slot k
$y^{(k)}$	Spoofing rate at time slot k
α	Learning rate of Bob
δ	Learning discount factor of Bob
$P_{f/m}^{(k)}$	False alarm rate/miss detection rate at time slot k
$\alpha_{f/m}$	Weight factors between the false alarm rate and the miss detection rate at time slot k
$u^{(k)}$	Utility of Bob at time slot k
$I^{(k)}$	Importance of Bob's sensing data at time slot k
$C_f^{(k)}$	Spoofing detection mode cost at time slot k

The path loss of a radio channel in the VANET for the link of distance d at time slot k is denoted by $L^{(k)}$. Similar to [18], we model the path loss in dB as

$$L^{(k)}[dB] = \bar{L}[dB] + 10n_0\log(\frac{d}{d_0}) + \sigma \tag{1}$$

where d_0 is the reference distance, $\bar{L}[dB]$ is the average large-scale path loss at d_0, n_0 is the path loss exponent and σ is the normal random variable corresponding to the shadowing fading. For ease of reference, some important notations are summarized in TABLE 1.

IV. PHY-layer rogue edge detection with Q-learning

We propose a PHY-layer rogue edge based authentication scheme for VANETs, which exploits the physical properties of the ambient radio signals received by both the mobile device and the edge node in a vehicle. More specifically, the mobile device and the edge node in the same vehicle have the same location tracing and thus can receive similar ambient radio signals from the source nodes such as the APs, BSs, RSUs and OBUs along the road. On the contrary, a rogue edge node Eve usually stays outside the target vehicle, and thus receive different ambient radio signals during the given time duration.

This scheme requires the edge node under test to send the PHY-layer feature such as the RSSIs of the ambient radio signals for a specific time duration and compares it with the record of the mobile device. Spoofing alarm is sent if the received PHY-layer feature trace is very different from the record of the mobile device at that time.

Let $I^{(k)} \in [0,1]$ denote the importance of the computation task of the mobile device at time slot k. If the computation task is very important, the mobile device chooses a more advanced authentication scheme to detect rogue edge nodes. The false alarm rate at time slot k, denoted by $P_f^{(k)}$, is calculated, which is the ratio of the legitimate packets rejected by the PHY-layer authentication scheme by mistake. The mobile device evaluates the miss detection rate, denoted by $P_m^{(k)}$, which is the ratio of the spoofing packets falsely accepted at time k. The mobile device also estimated the ratio of the spoofing signals in each time slot denoted by $y^{(k)} \in [0,1]$.

In the dynamic VANET authentication game, the mobile device chooses the spoofing detection mode and the test threshold based on the current state denoted by s^k. As the basis of the authentication, the state consists of the previous detection accuracy, the estimated spoofing probability in the last time slot, and the importance of the computation task of the mobile device in current time slot, i.e., $\mathbf{s}^{(k)} = [P_f^{(k-1)}, P_m^{(k-1)}, y^{(k-1)}, I^{(k)}]$.

As the next state observed by the mobile device is independent of the previous states and actions, for a given current state and authentication policy, the rogue edge detection process in the dynamic game can be formulated as an MDP. Therefore, the mobile device can apply reinforcement learning techniques such as Q-learning to derive the optimal strategy via trials without the knowledge of the VANET network model and the spoofing model.

The mobile device chooses the spoofing detection mode $x^{(k)} \in \mathbf{A}_0 = \{1,2\}$ with a cost $C_f^{(k)}(x)$ and the mobile device also chooses the test threshold $\theta^{(k)}$ that is quantized into $X+1$ levels, i.e., $\theta^{(k)} \in \mathbf{A}_1 = \{l/X\}_{0 \le l \le X}$. For convenience, we define $\mathbf{x}^{(k)} = \{x^{(k)}, \theta^{(k)}\} \in \mathbf{A} = \{\mathbf{A}_0, \mathbf{A}_1\}$, where $\mathbf{A}$ is the action set of the mobile device. The time index k in the superscript is omitted unless necessary. The spoofing detection mode cost is denoted by $C_f^{(k)}(x)$, which increases with x. For simplicity, we define $C_f^{(k)}(x) = x^2$.

Since the detection error rates depend on the test threshold, the mobile device has to select a proper value for $\theta^{(k)}$ in the detection. The utility of the mobile device at time slot k denoted by $u^{(k)}$ depends on the detection accuracy and the detection cost as follows,

$$u^{(k)}(\mathbf{x}, y) = -y^{(k)} I^{(k)} \left(\alpha_f P_f^{(k)} + \alpha_m P_m^{(k)} \right) - \beta C_f^{(k)} \quad (2)$$

where α_f (or α_m) is the weight factor of the false alarm (or the miss detection) in the detection, and $\beta \in [0,1]$ is the cost of the spoofing detection mode cost.

Let $\mathbf{R}^{(k)}$ denote the trace vector under detection at time slot k. Similarly, we define the record trace vector of Bob at time slot k as $\hat{\mathbf{R}}$. The proposed rogue edge detection scheme provides two spoofing detection modes to detect whether the packet that Bob receives is indeed sent by Alice. Let $x = \{1,2\}$ denote the spoofing detection modes, where $x = 1$ represents that Bob applies the historical RSSI records of the transmitter, i.e., $\mathbf{R}^{(k)} = r^{(k)}(i)$ and $\hat{\mathbf{R}} = \hat{r}(i)$, and $x = 2$ represents that Bob applies the transmitter historical RSSI records and the features records of the shared ambient radio signals, i.e., $\mathbf{R}^{(k)} = [r^{(k)}(i), \mathbf{f}^{(k)}]$, $\hat{\mathbf{R}} = [\hat{r}(i), \hat{\mathbf{f}}^{(k)}]$.

In the spoofing detection, Bob asks the edge node under detection to provide the PHY-layer feature traces. Once receiving the authentication message of the edge node under test, Bob authenticates the the edge under test with the calculating physical information. If the trace vector based on the RSSI and the PHY-layer properties of the shared ambient radio signals, $\mathbf{R}^{(k)}$, is similar to the record trace of Bob, the authentication message is sent by Alice, or is sent by Eve otherwise. Bob calculates the test statistic of the hypothesis test denoted by Δ, and given by

$$\Delta = \frac{\left\| \mathbf{R}^{(k)} - \hat{\mathbf{R}} \right\|^2}{\left\| \hat{\mathbf{R}} \right\|^2} \quad (3)$$

where $\|\cdot\|$ is the Frobenius norm.

The test statistic is compared with the test threshold denoted by $\theta^{(k)} \ge 0$. If $\Delta < \theta^{(k)}$, the mobile device accepts the edge node under test. Otherwise, if $\Delta \ge \theta^{(k)}$, a spoofing alarm is sent. The mobile device applies higher-layer authentication techniques if the packet passes the PHY-layer authentication. If the i-th packet under test is accepted by the higher-layer authentication, the mobile device updates the RSSI record $\hat{r}(i)$ with $\hat{r}(i) \leftarrow r^{(k)}(i)$.

The rogue edge detection with Q-learning is based on the learning rate, denoted by $\alpha \in (0,1]$, which shows the weight of the current experience. The discount factor $\delta \in [0,1]$ corresponds to the uncertainty on the future utility. The Q-function of the action vector $\mathbf{x}^{(k)}$ at state $\mathbf{s}^{(k)}$ is denoted by $Q\left(\mathbf{s}^{(k)}, \mathbf{x}^{(k)}\right)$, and is updated according to iterative Bellman equation as follows:

$$\begin{aligned} Q(\mathbf{s}, \mathbf{x}) \leftarrow & (1-\alpha) Q(\mathbf{s}, \mathbf{x}) \\ & + \alpha \left(u(\mathbf{s}, \mathbf{x}) + \delta V\left(\mathbf{s}'\right) \right) \end{aligned} \quad (4)$$

$$V(\mathbf{s}) = \max_{x \in \mathbf{A}_0, \theta \in \mathbf{A}_1} Q(\mathbf{s}, \mathbf{x}) \quad (5)$$

where $V\left(\mathbf{s}^{(k)}\right)$ maximizes the Q value over the rogue detection scheme.

The mobile device applies the ε-greedy policy to select the optimal action vector that maximizes the utility with a high probability $1-\varepsilon$, and chooses the suboptimal action vectors with a small probability ε, i.e.,

$$\Pr(\mathbf{x}^*) = \begin{cases} 1-\varepsilon, & \mathbf{x}^* = \arg \max_{x \in \mathbf{A}_0, \theta \in \mathbf{A}_1} Q(\mathbf{s}, \mathbf{x}) \\ \varepsilon / X, & \text{o.w.} \end{cases} \quad (6)$$

The PHY-layer rogue edge node detection with Q-learning is

summarized in Algorithm 1.

Upon the chosen detection mode and test threshold $\mathbf{x}^{(k)}$, the mobile device calculates the test statistic Δ according to Eq. (3) and compares Δ with $\theta^{(k)}$ to determine whether the authentication message at time slot k is indeed sent by Alice. If Δ is less than the test threshold $\theta^{(k)}$, the mobile device updates the trace vector record and estimates the corresponding false alarm rate at time slot k. Otherwise, the mobile device sends a spoofing alarm, and estimates the miss detection rate at time slot k. For convenience, we define QARAS as the abbreviation of our proposed scheme.

Algorithm 1: Rogue detection with Q-learning

Initialize α, δ, ε, $P_f^{(0)}$, $P_m^{(0)}$, $y^{(0)}$, N, M, $\mathbf{A}$ and $\mathbf{s}^{(0)}$.
$\mathbf{Q} = \mathbf{0}$, $\mathbf{V} = \mathbf{0}$
for $k = 1, 2, \cdots$ **do**
  Evaluate the current data importance $I^{(k)}$
  $\mathbf{s}^{(k)} = [P_f^{(k-1)}, P_m^{(k-1)}, y^{(k-1)}, I^{(k)}]$
  Choose the spoofing detection mode $x^{(k)}$ and the test threshold $\theta^{(k)}$ via (6)
  Broadcast the time duration and the features of monitoring the ambient radio signals
  Store the feature information of the ambient radio packets as $\mathbf{f}^{(k)}$
  Receive the authentication message from the edge node under test
  Obtain $r^{(k)}(i)$ and $\mathbf{f}^{(k)}$ from the edge node under test
  for $i = 1, 2, \cdots, N$ **do**
    if $x^{(k)} = 1$ **then**
      $\mathbf{R}^{(k)} = r^{(k)}(i)$, $\hat{\mathbf{R}} = \hat{r}(i)$
    else
      $\mathbf{R}^{(k)} = [r^{(k)}(i), \mathbf{f}^{(k)}]$, $\hat{\mathbf{R}} = [\hat{r}(i), \hat{\mathbf{f}}^{(k)}]$
    end
    Calculate Δ via (3)
    if $\Delta \leq \theta^{(k)}$ **then**
      Accept the i-th authentication message
      $\hat{r}(i) \leftarrow r^{(k)}(i)$
    else
      Send spoofing alarm
    end
  end
  Calculate $P_f^{(k)}$ and $P_m^{(k)}$
  Estimate the spoofing rate $y^{(k)}$ according to the detected illegal packets
  Evaluate $u^{(k)}$ via (2)
  Update $Q\left(\mathbf{s}^{(k)}, \mathbf{x}^{(k)}\right)$ via (4) and (5)
end

V. Simulation Results

Simulations have been performed to evaluate the rogue edge detection scheme in a VANET with the VANET channel model given by Eq. (1) and initial network topology as shown in Fig. 2. In the simulations, we set $n_0 = 3$, $d_0 = 10$ m, $\alpha_f = 0.5$, $\alpha_m = 1$, $\beta = 0.01$, and $M = 5$. Bob and Alice moved along the road at the same speed $v_1 = 10$ m/s.

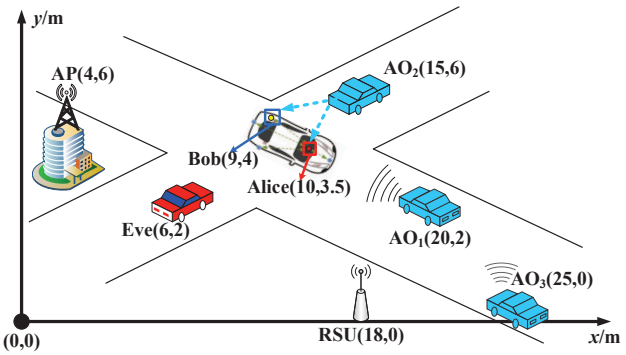


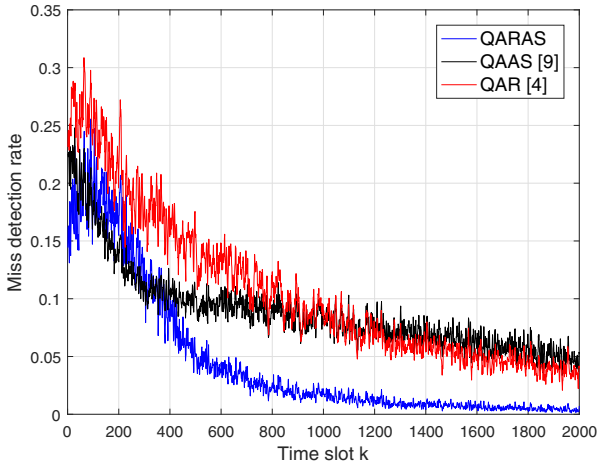
Fig. 2: Network topology in the simulation setting in meters, in which Bob, Alice and Eve extract and store the PHY-layer feature information of the ambient radio signals during the specific time duration to detect rogue edge Eve in a VANET with 5 ambient radio sources, including the AP, RSU, and three OBUs.

As shown in Fig. 3(a), the miss detection rate of QARAS decreases with time, from 16.3% at the beginning of the game to 0.26% after 2000 time slots, which is about 90.9% and 86.2% less than the QAR scheme developed in [4] and the QAAS scheme developed in [9], respectively. As shown in Fig. 3(b), this scheme decreases the false alarm rate by 13.1% to 2.3% after 2000 time slots, which is 50.6% and 74.3% less than the benchmark QAR and QAAS, respectively.

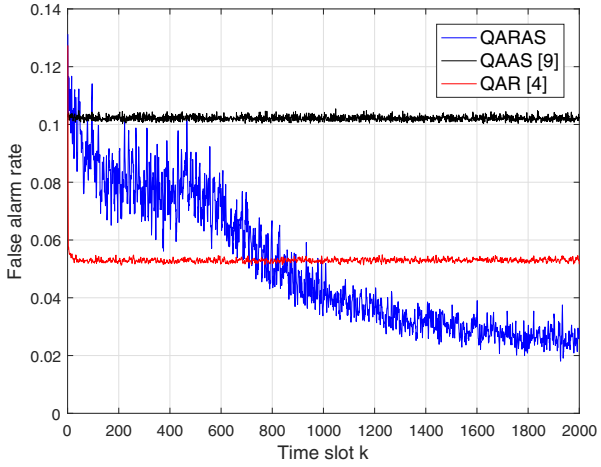
As shown in Fig. 3(c), the utility of the mobile device increases with time, and this scheme increases the utility than the benchmark schemes. For example, the utility of the mobile device increases by about 65.7% after 2000 time slots at convergence, which is about 39.1% and 73.9% higher than QAR and QAAS, respectively. In addition, the QARAS scheme has a faster learning speed, e.g., this scheme takes about 1200 time slots (about 2.65 seconds) to achieve the optimal authentication policy, while it will take more time slots to converge for QAR and QAAS.

VI. Conclusion

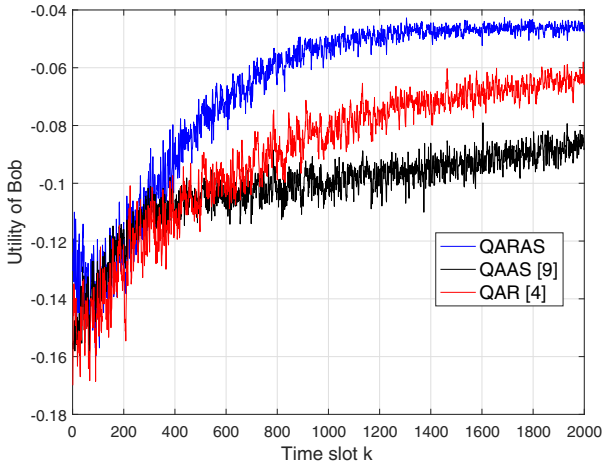
In this paper, we have presented a PHY-layer authentication scheme to detect rogue edge nodes for VANETs. This scheme depends on the physical properties of the ambient radio signals received by both the mobile device and the serving edge node and uses Q-learning to enable a mobile device to achieve the optimal authentication policy in the dynamic VANET without knowing of the VANET model or the attack model. Simulation results show that our proposed scheme exceeds the benchmark schemes such as QAR and QAAS with higher detection accuracy and higher utility. For instance, the miss detection rate and the false alarm rate of this scheme are 0.26% and 2.3% after 2000 time slots, which are



(a) Miss detection rate



(a) False alarm rate



(b) Utility of Bob

Fig. 3: Performance of the PHY-layer rogue edge detection in the VANET as shown in Fig. 2, with $n_0 = 3$, $d_0 = 10$ m, $\alpha_f = 0.5$, $\alpha_m = 1$, $\beta = 0.01$, and $M = 5$.

86.2% and 74.3% less than the benchmark strategy QAAS, respectively.

REFERENCES

[1] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, 2010.

[2] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," *IEEE Trans. Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.

[3] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 772–782, Jun. 2017.

[4] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Vehicular Technology*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.

[5] C. Pei, N. Zhang, X. Shen, and J. W. Mark, "Channel-based physical layer authentication," in *Proc. IEEE Global Commun. Conf.*, pp. 4114–4119, Austin, TX, Dec. 2014.

[6] N. Wang, T. Jiang, S. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Commun. Letters*, vol. 35, no. 3, pp. 1089–7798, Jul. 2017.

[7] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sept. 2013.

[8] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2089–2100, Oct. 2013.

[9] J. Liu, L. Xiao, G. Liu, and Y. Zhao, "Active authentication with reinforcement learning based on ambient radio signals," *Springer Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3979–3998, Oct. 2015.

[10] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed-certificate-service scheme for vehicular networks," *IEEE Trans. Vehicular Technology*, vol. 59, no. 2, pp. 533–549, Jul. 2009.

[11] F. J. Liu, X. Wang, and S. L. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int'l Conf. Commun. (ICC)*, pp. 4724–4728, Budapest, Jun. 2013.

[12] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *Proc. IEEE INFOCOM*, pp. 1276–1284, Toronto, ON, Apr. 2014.

[13] C. Wang, X. Zheng, Y. Chen, and J. Yang, "Locating rogue access point using fine-grained channel information," *IEEE Trans. Mobile Computing*, vol. 16, no. 9, pp. 2560–2573, Sept. 2017.

[14] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proc. ACM Int'l Conf Mobile systems, applications, and services*, pp. 211–224, Jun. 2011.

[15] H. Han, F. Xu, C. C. Tan, Y. Zhang, and Q. Li, "VR-defender: Self-defense against vehicular rogue APs for drive-thru internet," *IEEE Trans. Vehicular Technology*, vol. 63, no. 8, pp. 3927–3934, Oct. 2014.

[16] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," *IEEE Trans. Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.

[17] A. Abdallah and X. Shen, "Lightweight authentication and privacy-preserving scheme for V2G connections," *IEEE Trans. Vehicular Technology*, vol. 66, no. 3, pp. 2615–2629, Mar. 2017.

[18] X. Wan, L. Xiao, Q. Li, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced communication overhead," in *Proc. IEEE Int'l Conf. Commun. (ICC)*, Paris, France, May 2017.