Computers, Materials & Continua CMC, vol.64, no.1, pp.359-371, 2020

Authentication of Vehicles and Road Side Units in Intelligent Transportation System

Muhammad Waqas[1, 2], Shanshan Tu[1, 3, *], Sadaqat Ur Rehman[1], Zahid Halim[2], Sajid Anwar[2], Ghulam Abbas[2], Ziaul Haq Abbas[4] and Obaid Ur Rehman[5]

Abstract: Security threats to smart and autonomous vehicles cause potential consequences such as traffic accidents, economically damaging traffic jams, hijacking, motivating to wrong routes, and financial losses for businesses and governments. Smart and autonomous vehicles are connected wirelessly, which are more attracted for attackers due to the open nature of wireless communication. One of the problems is the rogue attack, in which the attacker pretends to be a legitimate user or access point by utilizing fake identity. To figure out the problem of a rogue attack, we propose a reinforcement learning algorithm to identify rogue nodes by exploiting the channel state information of the communication link. We consider the communication link between vehicle-to-vehicle, and vehicle-to-infrastructure. We evaluate the performance of our proposed technique by measuring the rogue attack probability, false alarm rate (FAR), mis-detection rate (MDR), and utility function of a receiver based on the test threshold values of reinforcement learning algorithm. The results show that the FAR and MDR are decreased significantly by selecting an appropriate threshold value in order to improve the receiver's utility.

Keywords: Intelligent transportation system, authentication, rogue attack.

1 Introduction

The connection of vehicles is a new intelligent transportation system (ITS) to improve the safety of vehicles and efficiency by leveraging wireless transmission [Waqas, Niu, Li et

[1] Beijing Key Laboratory of Trusted Computing, Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China.

[2] Faculty of Computer Science & Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Topi, 23460, Pakistan.

[3] Beijing Electro-Meahnical Engineering Institute, Beijing, 100074, China.

[4] Faculty of Electrical Engineering, Ghulam Ishaq Khan Institute of Engineering Sciences & Technology, Topi, 23460, Pakistan.

[5] Department of Electrical Engineering, Sarhad University of Science and Information Technology, Peshawar, 25000, Pakistan.

[*] Corresponding Author: Shanshan Tu. Email: sstu@bjut.edu.cn.

Received: 20 January 2020; Accepted: 31 March 2020.

al. (2019)]. Decades ago, Vehicle-to-everything (V2X) communications attracted interest in terms of extensive research and development projects from academia, industries and standard organization [Salem, Elhillali and Niar (2018); Xu, Liu, Wang et al. (2018)]. However, with the advent of ITS, the main enthusiasm for the development of an ITS is safety, and the development of reliable and secure applications by providing information and help to vehicles for the prevention of road accidents, selection of appropriate direction and routes, speed control, pedestrian safety, hijacking and lane change warning [Marković, Sekuła, Vander et al. (2018); Wang, Liu, Yu et al. (2019)]. In this regard, security is the major concern of high-priority because the attackers with malicious threats are extremely dangerous, and can cause various consequences such as, accident, break failure, showing wrong directions and routes, and stealing personal information [Sedjelmaci, Hadji and Ansari (2019)]. The attackers may attack infrastructure as well as vehicles directly to cause these negative consequences [Hahn, Munir and Behzadan (2019); Waqas, Niu and Ahmed (2018)]. However, stealing the information from vehicles and private data of users is much more crucial [Msahli, Labiod and Ampt (2019)]. In this regard, the authentication of road side units (RSUs) and vehicles are extremely significant for the implementation of an ITS [Yu, Liu and Zhang (2019)].

Authentication helps to identify the rouge nodes in an ITS. The main objective is to achieve the authentication of vehicles and RSUs by leveraging physical layer security (PLS) and reinforcement learning algorithm (RLA) to get the authenticity and integrity [Moradikia, Bastami and Kuhestani (2019)]. RLA is employed to find out the probability of misdetection rate (MDR) and false alarm rate (FAR) by identifying the rouge vehicle/RSUs. Thus, we seek to tackle the rogue attack to stop stealing the data of the authentic vehicles during communication by leveraging RLA. It is due to the reason that a rogue node pretends to be a legitimate user for fraud with authorized users to steal the information. To cope with the challenge, the physical layer authentication (PLA) technique can be applied [Haus, Waqas and Ding (2017)]. The PLA techniques exploit the physical layer properties of wireless channels to detect the impersonation attack. These properties include received signal strength (RSS), channel impulse response (CIR), received signal strength indicators (RSSI), channel state information (CSI) and channel frequency response (CFR) [Zou, Wang and Shen (2013)]. These properties can be utilized as the characteristics of wireless channels to detect rogue vehicles/RSUs.

However, there are certain problems in wireless channels. One of the specific challenges is that the wireless channel is not static, and the channel characteristics are changing dynamically due to the mobility of vehicles [Xiao, Li, Han et al. (2016)]. Therefore, it is difficult to predict the channel information. For instance, the channel-based impersonator detector in Xiao et al. [Xiao, Wan, Su et al. (2018)] differentiates the transmitters at different locations due to which a hypothesis test in RLA compares the CFR of the data with the identical address. Thus, the accuracy of the PLA can be performed at the receiver that depends on the threshold test in the hypothesis test. Again, there is an issue of the test threshold because it becomes difficult for the receiver to select an appropriate threshold value to detect the rogue node without knowing the exact values of the channel parameters, especially in the dynamic environment. Moreover, the legitimate vehicle, as well as attackers, have autonomy and flexible control over their transmission. Thus, conventional methods such as game theory have shown strengths to improve the security

strength [Waqas, Ahmed, Li et al. (2018); Shanmugapriya, Baskaran and Nayanatara (2019)]. Still, they are mostly applicable in a static environment and not in a dynamic environment, particularly in case of a vehicle. Therefore, we utilize an RLA technique in which a user can achieve the optimal strategies in a dynamic environment without being aware of the system's information [Chen, Zhan, Chen et al. (2018)].

In RLA, we conduct a hypothesis test that concerns the estimation of the channel information; whereas in the hypothesis test, we conclude the threshold test value between vehicles and vehicles-to-RSU by leveraging CSI. As a result, the precision to detect a rogue vehicle and RSU depends on the threshold test value, which can be achieved at the receiver end. Thus, the receiver itself is responsible for identifying between authentic and rogue vehicle/RSU. Therefore, we focus mainly on the rogue attack and receiver response in this work. Our main contributions of this work are summarized as follows.

- We derive an optimal threshold value in the hypothesis test. This helps us to distinguish between authentic and rogue vehicle/RSU. It also helps us to improve detection accuracy and receiver's utility (gain or loss) from the test threshold value.
- We evaluate the performance of our proposed technique by measuring attack probability, FAR, MDR, and average cost and gain based on test threshold values.
- With the help of the proposed technique, we find out that the FAR and MDR are decreased significantly by selecting an appropriate threshold value. Besides, the average gain is increased by approximately 40% by selecting an appropriate threshold value. Similarly, the average cost is decreased by 30% by our proposed technique.

The rest of the paper is structured as follows. After the introduction in Section I, we present the system model, problem formulation and proposed solution in Section II. The simulation results are discussed in Section III. Finally, we offer our conclusion in Section IV.

2 System model, problem formulation and proposed solution

We consider a communication link between vehicles-to-vehicle, vehicle-to-RSUs, and RSU-to-vehicle that are physically connected through wireless links as shown in Fig. 1. Hence, we exploit three cases to identify the rogue node. Here, node refers to a vehicle or an RSU.

Case #1: If there is a communication between vehicle-to-vehicle, then the vehicle at the receiver end will calculate the test threshold value to identify the transmitter vehicle as a legitimate node or rogue one.

Case #2: If there is a communication between vehicle-to-RSU, then the RSU at the receiver end will calculate the test threshold value to identify the transmitter vehicle as a legitimate node or rogue one.

Case #3: If there is a communication between RSU-to-vehicle, then the vehicle at the receiver end will calculate the test threshold value to identify the transmitter RSU as a legitimate node or rogue one.

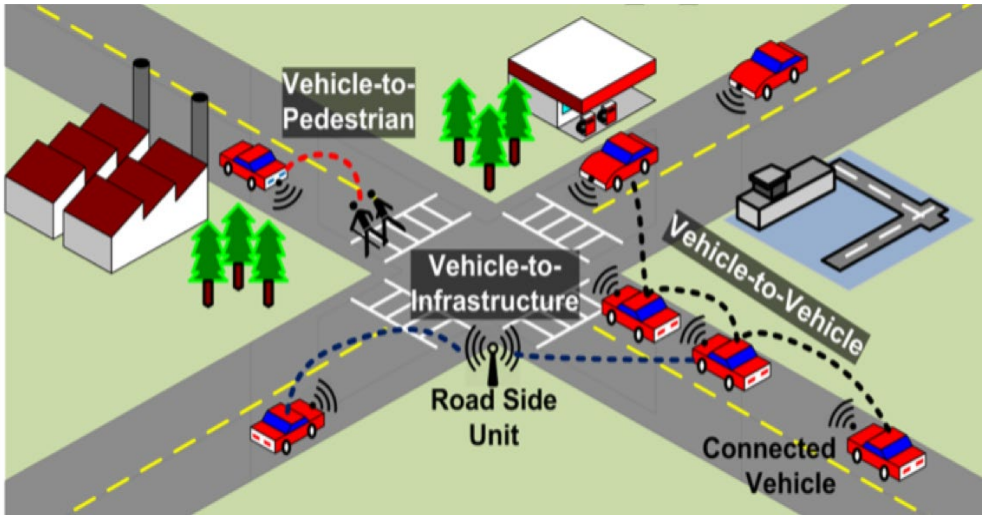

Figure 1: Communication scenario of vehicle-to-vehicle, vehicle-to-RSU and RSU-to-vehicle in an ITS

In this regard, we consider a network that consists of vehicles, i.e., $\mathcal{V}$ such that, $\mathcal{V} = \{1,2,\cdots,V\}, \forall V \in \mathcal{V}$. We also consider the number of RSUs, i.e., $\mathcal{B}$ such that, $\mathcal{B} = \{1,2,\cdots,B\}, \forall B \in \mathcal{B}$. For simplicity, we also assume the rogue nodes comprise of vehicles and RSUs i.e., $\mathcal{R}$, such that, $\mathcal{R} = \{1,2,\cdots,R\}, \forall R \in \mathcal{V}/\mathcal{B}$. The rogue node can either be an RSU that wants to steal the information of legitimate vehicle or a vehicle that wants to steal the information of other vehicles or a vehicle that wants to steal the information of RSU. Hence, the total number of nodes in the network is $\mathcal{D} = (\mathcal{V} \cup \mathcal{B})$. Among them, let $\mathcal{L}, \forall \mathcal{L} \in \mathcal{D}$ is the total number of legitimate transmitters (vehicle+RSU), and $\mathcal{I}, \forall \mathcal{I} \in \mathcal{D}$ is the total number of rogue transmitters (vehicle+RSU), such that $T = (\mathcal{L} \cup \mathcal{D})$. As a result, the receivers can be calculated as $S = \mathcal{D} - T$, where S is the total number receivers (vehicles+RSUs).

Next, we consider the set of MAC addresses, denoted by $\mathcal{M}$, of all the transmitters. For instance, the MAC-Address of t^{th} transmitter (vehicle/RSU), $\forall t \in T$ is represented by $\gamma_t \in \mathcal{M}$. The rogue node can send fake address in a time slot with probability, i.e., $P_{\gamma_t} \in [0,1]$. The receiver $s \in S$ calculates the CSI related to the packet, once the packet is arrived at the receiver. The receiver $s \in S$ samples the CSI of each packet and reserves the channel vector of the z^{th} packet from the t^{th} transmitter. This channel vector is denoted by $\mathbb{K}^z_{\gamma_t} = \left[\mathbb{K}^z_{\gamma_t,x}\right]_{1\le x\le X}$. Another important factor for sampling the CSI of each packet is the channel record. Here, we denote the channel record of the z^{th} packet from the t^{th}transmitter by$\mathbb{L}^z_{\gamma_t} = \left[\mathbb{L}^z_{\gamma_t,x}\right]_{1\le x\le X}$. Hence, $\mathbb{K}^z_{\gamma_t}$ and $\mathbb{L}^z_{\gamma_t}$ are the channel vector and channel record, respectively of the x^{th} tone of the z^{th} packet from the transmitter $t \in T$.

In the view of above discussion, we now perform the hypothesis value test to evaluate the authentication of each packet at the receiver i.e., S. The transmitter transmits a MAC

addresses where the channel vectors are denoted by $\mathcal{M}\left(\mathbb{K}_{\gamma_t}^z\right)$. Now, the set of receivers S implies the hypothesis value test by considering two cases as follows.

Case #1: The hypothesis test $\mathcal{W}_\circ$considers $\mathcal{M}\left(\mathbb{K}_{\gamma_t}^z\right)$from the authentic vehicle/RSU, i.e., $\mathcal{W}_\circ: \mathcal{M}\left(\mathbb{K}_{\gamma_t}^z\right) \geq \mathcal{M}$.

Case #2: The hypothesis test $\mathcal{W}_\star$ considers $\mathcal{M}\left(\mathbb{K}_{\gamma_t}^z\right)$ from the rogue vehicle/RSU, i.e., $\mathcal{W}\_\star: \mathcal{M}(\mathbb{K}\_(\gamma\_t)\hat{}z) \neq \mathcal{M}$.

As we know, CSI is unique and is the property of PLS. Thus, the vehicle/RSU can authenticate the z^{th} packet based on CSI. In contrast, the authentic packet can be identified if and only if $\left[\mathbb{K}_{\gamma_t,x}^z\right]_{1\leq x\leq X} = \left[\mathbb{L}_{\gamma_t,x}^z\right]_{1\leq x\leq X}$. Hence, if the channel vector and channel record remain the same, we will consider the packet as authentic packet sent by authentic vehicle/RSU. Otherwise, the packet is sent by rogue node, i.e., $\left[\mathbb{K}_{\gamma_t,x}^z\right]_{1\leq x\leq X} \neq \left[\mathbb{L}_{\gamma_t,x}^z\right]_{1\leq x\leq X}$. However, for this purpose, we need to formulate the hypothesis statistics to find out the rogue attack in a precise manner. The statistics of the hypothesis test is

$$\mathcal{G}\left(\left(\mathbb{K}_{\gamma_t}^z\right),\left(\mathbb{L}_{\gamma_t}^z\right)\right) = \frac{\|(\mathbb{K}_{\gamma_t}^z - \mathbb{L}_{\gamma_t}^z)\|^2}{\|\left(\mathbb{L}_{\gamma_t}^z\right)\|^2} \tag{1}$$

In Eq. (1), ||•|| represents the Frobenius norm, and $\mathcal{G}$ is the normalized Euclidean distance between $\mathbb{K}_{\gamma_t}^z$ and $\mathbb{L}_{\gamma_t}^z$, respectively. $\mathcal{G}\left(\left(\mathbb{K}_{\gamma_t}^z\right),\left(\mathbb{L}_{\gamma_t}^z\right)\right)$ must be illustrated by introducing a fix threshold value test denoted by Ψ. Once, the threshold value test is fix, we can illustrate that if $\mathcal{G}\left(\left(\mathbb{K}_{\gamma_t}^z\right),\left(\mathbb{L}_{\gamma_t}^z\right)\right) < \Psi$, the receiver vehicle accepts $\mathcal{W}_\circ$, otherwise it will accept $\mathcal{W}_\star$. Consequently, the overall illustration of identifying the real and rogue vehicles/RSU is given by

$$\mathcal{G}\left(\left(\mathbb{K}_{\gamma_t}^z\right),\left(\mathbb{L}_{\gamma_t}^z\right)\right) < \Psi \Rightarrow \mathcal{W}_\circ, \tag{2}$$

$$\mathcal{G}\left(\left(\mathbb{K}_{\gamma_t}^z\right),\left(\mathbb{L}_{\gamma_t}^z\right)\right) > \Psi \Rightarrow \mathcal{W}_\star. \tag{3}$$

We now define the probability of FAR and MDR for our three cases, as mentioned above. FAR and MDR are defined as follows.

Definition 1. *FAR is defined as the probability that a receiver rejects the packets and consider it as unauthentic packet, although the packet is sent by legitimate node. Mathematically, it is given by* $P_F = P(\mathcal{W}_\star|\mathcal{W}_\circ)$.

Definition 2. *MDR is defined as the probability that a receiver accepts the packets and considers it as authentic packet, although the packet is sent by rogue node. Mathematically, it is given by* $P_M = P(\mathcal{W}_\circ|\mathcal{W}_\star)$.

Here, $P(\cdot \mid \cdot)$is the conditional probability. Now, we consider the three cases.

In **Case #1**, the transmitter and receiver both are vehicles. Hence, the probability for receiver to accept the authentic packet from authentic transmitter vehicle by reducing the FAR is $P_{\mathcal{V}}(\mathcal{W}_\circ|\mathcal{W}_\circ) = 1 - P_{\mathcal{V}}$.

In **Case #2**, the transmitter is a vehicle, and the receiver is RSU. The transmitter (vehicle) to send signals for getting some valuable information or requesting to act as a relay for

better communication. Hence, in this case, the RSU must be active in tackling rogue vehicles. Therefore, the RSU to accept the authentic packet from authentic transmitter vehicle by reducing the FAR is $P_{\mathcal{B}}(\mathcal{W}_\circ|\mathcal{W}_\circ) = 1 - P_{\mathcal{V}}$.

The last **Case #3** is about RSU-to-vehicle communication. In this case, the transmitter is RSU and receiver is vehicle. Therefore, the vehicle to accept the authentic packet from authentic RSU transmitter by reducing the FAR is $P_{\mathcal{V}}(\mathcal{W}_\circ|\mathcal{W}_\circ) = 1 - P_{\mathcal{B}}$. For simplicity, we assume all the three cases in a generalized form by

$$P(\mathcal{W}_\circ|\mathcal{W}_\circ) = 1 - P_F. \tag{4}$$

Similarly, the MDR is also calculated for all the three cases in mathematical form given by $[P_{\mathcal{V}}(\mathcal{W}_\star|\mathcal{W}_\star) = 1 - P_{\mathcal{V}}]$, $[P_{\mathcal{B}}(\mathcal{W}_\star|\mathcal{W}_\star = 1 - P_{\mathcal{V}}]$, $[P_{\mathcal{V}}(\mathcal{W}_\star|\mathcal{W}_\star) = 1 - P_{\mathcal{B}}]$, respectively. Generally, it is

$$P(\mathcal{W}_\star|\mathcal{W}_\star) = 1 - P_M. \tag{5}$$

However, the FAR and MDR accuracy of PLA depends on the threshold value, i.e., Ψ. Thus, if we increase the threshold value test Ψ, the MDR increases while decreasing Ψ, the FAR increases. Therefore, the receiver must select an appropriate value of Ψ to identify the rogue packets from a rogue node. However, it is assumed in this work that higher-layer authentication (HLA) is also necessary to accept the packets. Hence, we use both PLA and HLA to accept the legitimate packets from a legitimate node. For instance, the channel record $\mathbb{L}_{\gamma_t}^z$ is only updated if the packet is acknowledged by HLA, i.e., $\mathbb{L}_{\gamma_t}^z \leftarrow \mathbb{K}_{\gamma_t}^z$, otherwise, $\mathbb{L}_{\gamma_t}^z \leftarrow \mathbb{L}_{\gamma_t}^{z-1}$.

The RLA has the ability to point out the optimal strategy in a dynamic environment without adequate information of the channel/system [Tu, Waqas and Rehman (2018)]. In this regard, the receiver nodes are oblivious of the CSI and delude frequencies in a dynamic environment. Thus, the optimal threshold value Ψ can be attained by the receivers through trial and error to find out rogue nodes. The precision to detect rogue packets from rogue nodes depend on the utility of receiver. Thus, we define the gain and cost of the receiver to figure out FAR and MDR.

Definition 3. *The gain of the receiver is defined as to accept legitimate packet or reject rogue packets, and are denoted by $\mathbb{G}_a$ and $\mathbb{G}_r$, respectively.*

Definition 4. *The cost of the receiver is defined as to accept rogue packets or reject legitimate packets, and are denoted by $\mathbb{C}_a$ and $\mathbb{C}_r$, respectively.*

In this regard, we apply Bayesian risk [Ma, Lai and Kleijn (2018)] under a prior distribution function which is given by

$$\mathbb{E}(\lambda, \mathbb{R}) = \Big(\mathbb{G}_a\big(1 - P_F(\lambda)\big) - \mathbb{C}_a P_F(\lambda)\Big)\left(1 - \sum\nolimits_{\gamma=1}^{\mathcal{M}} P_{\gamma_t}\right) + \Big(\mathbb{G}_r\big(1 - P_M(\lambda)\big) - \mathbb{C}_r P_M(\lambda)\Big)\left(\sum\nolimits_{\gamma=1}^{\mathcal{M}} P_{\gamma_t}\right). \tag{6}$$

In Eq. (6), $\mathbb{R}$ is the set of all rogue packets sent by rogue nodes and is given as $\mathbb{R} = \left[P_{\gamma_t}\right]_{1\le\gamma\le\mathcal{M}}$, and $\left(1 - \sum_{\gamma=1}^{\mathcal{M}} P_{\gamma_t}\right)$ is the probability of receiver to reject rogue packet.

Hence, $\left(\mathbb{G}_a\left(1-P_F(\lambda)\right)-\mathbb{C}_a P_F(\lambda)\right)\left(1-\sum_{\gamma=1}^{\mathcal{M}} P_{\gamma_t}\right)$ represents the gain of the legitimate packets, and $\left(\mathbb{G}_r\left(1-P_M(\lambda)\right)-\mathbb{C}_r P_M(\lambda)\right)\left(\sum_{\gamma=1}^{\mathcal{M}} P_{\gamma_t}\right)$ represents the gain under rogue attack. It is also believed that the optimal threshold value Ψ will automatically decrease when the number of rogue nodes increases. Hence, the receiver needs to evaluate Ψ with each z^{th} packet acknowledged in the time slot τ. Hence, Ψ is chosen from the experience of states, i.e., β. Hence, the state (β) calculated by receiver at time τ is denoted by β_τ, and given as $\beta_\tau = [P_F^\tau - 1, P_M^\tau - 1] \in \Gamma$, where Γ is the set of all the states calculated by the receiver. The receiver selects Ψ based on β_τ to maximize the expected utility sum, given as

$$\Pi_\tau = \sum_{\tau=1}^{T} \mathcal{U}_{\mathcal{N}}^{\tau}.(\lambda, \mathbb{R}), \tag{7}$$

where

$$\mathcal{U}_{\mathcal{N}}^{\tau}.(\lambda, \mathbb{R}) = \mathbb{E}(\lambda, \mathbb{R}) = \left(\mathbb{G}_a\left(1-P_F(\lambda)\right)-\mathbb{C}_a P_F(\lambda)\right)\left(1-\sum_{\gamma=1}^{\mathcal{M}} P_{\gamma_t}\right)+\left(\mathbb{G}_r\left(1-P_M(\lambda)\right)-\mathbb{C}_r P_M(\lambda)\right)\left(\sum_{\gamma=1}^{\mathcal{M}} P_{\gamma_t}\right).$$

$\mathcal{U}_{\mathcal{N}}^{\tau}$ is basically the immediate utility function that indicates the suboptimal strategy with a small probability ϵ on the basis of ϵ-greedy policy. On the other side, the preference of the utility that is maximized by the optimal Ψ is$1-\epsilon$.

$$P_\gamma(\Psi) = \left\{\left(1-\epsilon, \Psi = \Psi^*, \frac{\epsilon}{L}, \Psi \in \{l/L\}_{\Psi \le l \le L}, \Psi \neq \Psi^*.\right)\right. \tag{8}$$

where L are the stages to select an optimal threshold value Ψ. The error rates are also quantized into $L+1$ levels, i.e., $P_F, P_M, \in \{l/L\}_{0 \le l \le L}$. Hence, the optimal value of $\Psi\_\star$ is

$$\Psi^* = \text{argmax}_{\Psi \in \{l/L\}_{0 \le l \le L}} \mathcal{Q}(s_\tau, \Psi). \tag{9}$$

As we consider Q-learning, hence we denote the learning rate as $\mu \in (0,1]$. The weight is given by $\mathcal{Q}(s_\tau, \Psi)$, and the discount factor is $\sigma \in (0,1]$. The maximum value of the Q-function is $\mathcal{V}(s_\tau) \leftarrow \max_{\Psi \in \{l/L\}_{0 \le l \le L}} \mathcal{Q}(s_\tau, \Psi)$. Consequently, the receiver updates the Q-function as

$$\mathcal{Q}(s_{\tau+1}, \Psi_{\tau+1}) = (1-\mu)\mathcal{Q}(s_\tau, \Psi_\tau) + \mu\left(\Pi_\tau + \delta \mathcal{V}(s_\tau + 1)\right). \tag{10}$$

The overall discussion is summarized in our proposed Algorithm 1.

Algorithm 1: Rogue Attack Detection Algorithm

Step # I Initialization:
Compute ϵ, μ, δ, $\mathcal{Q}(s,\Psi)$, $\mathcal{V}(s)=0$, $\forall\Psi\in\{l/L\}_{0\leq l\leq L}$.
Step # II: Current State:
while $\tau=1,2,3,\cdots$ **do**
  Find s_τ
  Select Ψ_τ;
  for $t=1$ *to* T **do**
    Observe MAC-Address $\gamma_t\in\mathcal{M}$
    Extract $\left((\mathbb{K}^z_{\gamma_t})\right.$ and $\left.(\mathbb{L}^z_{\gamma_t})\right)$
    Calculate $\mathcal{G}\big((\mathbb{K}^z_{\gamma_t}),(\mathbb{L}^z_{\gamma_t})\big)$,
    if $\mathcal{G}\big((\mathbb{K}^z_{\gamma_t}),(\mathbb{L}^z_{\gamma_t})\big)\leq\Psi_\tau$ **then**
      Pass zth packet for HLA
      $(\mathbb{L}^z_{\gamma_t})\big)\leftarrow\big((\mathbb{K}^z_{\gamma_t})$
      Accept the z^{th} packet
      else;
      Reject the z^{th} packet;
    end
  end
  Step # III: Next State:
  Observe $s_{\tau+1}$
  Observe Π_τ
  Update $\mathcal{Q}(s_\tau,\lambda_\tau)$
  Update $\mathcal{V}(s_\tau)$
end

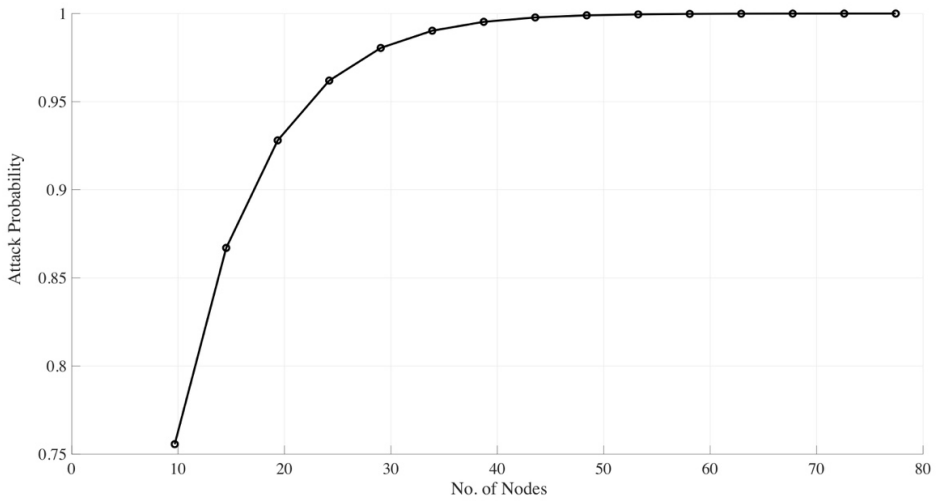

Figure 2: Attack probability of rogue nodes by varying no. of nodes

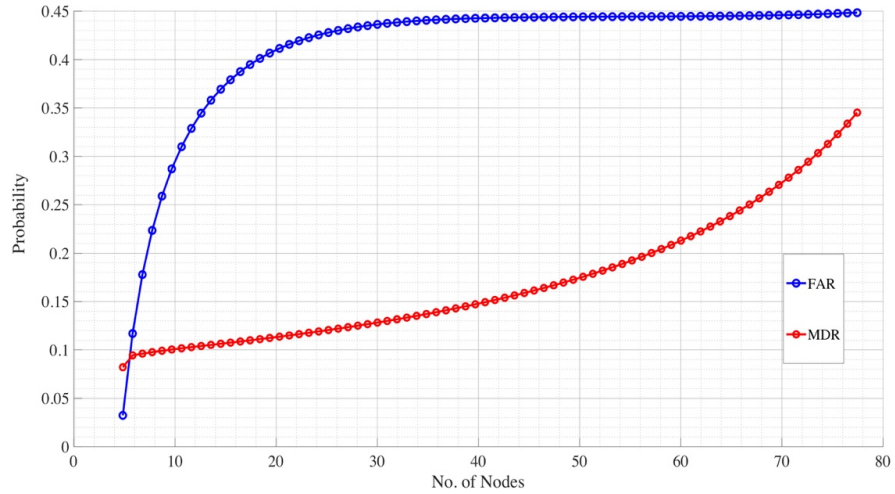

Figure 3: Probability of FAR and MDR according to no. of nodes

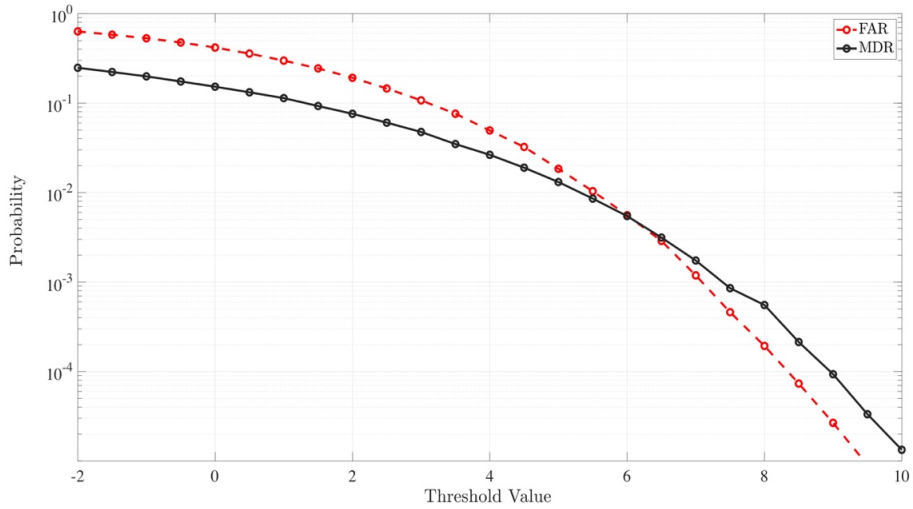

Figure 4: Probability of FAR and MDR according to threshold values

3 Simulation results

We perform our simulation results to evaluate FAR and MDR along with attack probability, gain and cost of a receiver during detection. In the simulation environment, we assume randomly scattered nodes by assuming 80 nodes. All the channels' gains are rendered accordingly to the normal distribution. In our first analysis, we find out the attack probability by varying the number of nodes, as depicted in Fig. 2. It is obvious that as the number of nodes (whether vehicles, RSUs or both), the rogue devices (vehicles/RSUs) may also increase due to which the attack probability increases. It can be

seen that there is an abrupt change when the number of nodes is varying from 10 to 40. However, as the number of nodes increases, the attack probability is maximum, i.e., 1. Hence, after 40 number of nodes, the attack probability is always maximum, and the receivers must be careful while establishing a link with other vehicles or RSUs. Keeping this point in view, we find out FAR and MDR by varying the number of nodes, as shown in Fig. 3. Obviously, when the attack probability is increased, the FAR and MDR will automatically increase. It is due to the reason that as the number of nodes increases in the network, it becomes difficult for the receivers to detect these attacks. Thus, the receivers reject the packets and consider it as an unauthentic packet, although the packet is sent by legitimate node due to a large number of other nodes (vehicles/RSUs), and hence the probability of FAR increases. Similarly, the probability of MDR also increases due to a large number of other nodes. This is because, due to high attack probability, the receivers accept the packets and consider it an authentic packet, although the rogue node sends the packet. For instance, the probability of FAR and MDR is 0.43 and 0.25, respectively, when the number of nodes is 40, and increases accordingly.

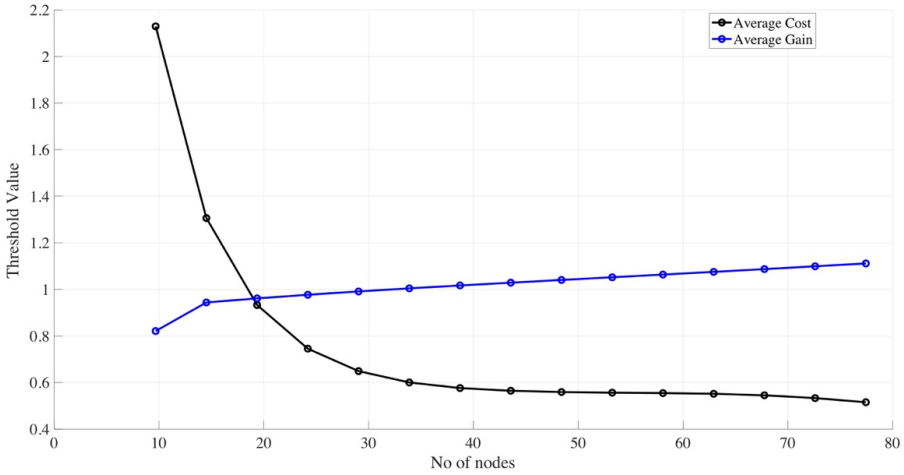

Figure 5: Average cost and an average gain of a receiver by varying no. of nodes at different threshold values

In addition, we also investigate the probability of FAR and MDR of the receivers by selecting their optimal threshold value. Since by selecting an optimal threshold value, the probability of FAR and MDR at the receivers is decreased. Hence, this is an important experiment to find out P_F and P_M at a given threshold value. Observed from Fig. 4, as the threshold value increases, P_F and P_M decreases. For instance, when the threshold value is in negative, i.e., -2, P_F and P_M are at maximum value. However, as the threshold value increases, i.e., to find optimal value by the receivers, P_F and P_M exponentially decreases. It means that certain receivers have diverse threshold value to reduce P_F and P_M, respectively. Suppose the receiver selects the optimal threshold value "4", the probability to miss-detect or false alarm rate for that specific receiver is approximately equal to $10^{-2.5}$ and 10^{-1}, respectively.

Similarly, the utilities of a receiver, i.e., gain and cost, are also essential factors for verification. Thus, we illustrate the average loss and average profit of the receiver by exploiting the threshold values and a varying number of nodes, as shown in Fig. 5. It is clear from Fig. 5 that as the number of nodes increases, the average gain increases due to the rise in the threshold value. For instance, As the number of nodes increases from 10 to 40, the threshold value increases from 0.8 to 1.1 based on the average gain of the receiver. Similarly, the threshold value decreases as the number of nodes increases based on the average cost of the receiver. For example, the threshold value is dropping from 2.1 to 0.6 when the number of nodes increases from 10 to 30, respectively. Thus, the average cost is reduced due to the threshold value of the receiver decreases.

4 Conclusion

The connection of vehicles is a new intelligent transportation system to improve the safety of vehicles and efficiency by leveraging wireless transmission. However, security threats to smart and autonomous vehicles cause potential consequences such as traffic accidents, economically damaging traffic jams, hijacking, motivating to wrong routes, and financial losses for businesses and governments. One of the problems is a rogue attack, in which the attacker is trying to be a legitimate user or access point (AP) by utilizing fake identity. Thus, we apply RLA to tackle rogue attacks during communication between vehicle-to-vehicles, vehicle-to-RSU, and RSU-to-vehicle. In this regard, we derive an optimal threshold value to distinguish between authentic and rogue nodes. It helps us to improve detection accuracy and receiver's utility (gain or cost) from the test threshold value. Hence, we evaluate the performance of our proposed technique by measuring attack probability, FAR, MDR, and utility function of receivers. With the help of our proposed technique, we find out that the FAR and MDR are decreased significantly by selecting an appropriate threshold value. Moreover, the average gain is increased by approximately 40% by selecting an appropriate threshold value. Similarly, the average cost is decreased by 30% by our proposed technique.

Funding Statement: This work was partially supported by The China's National Key R & D Program (No. 2018YFB0803600), Natural Science Foundation of China (No. 61801008), Beijing Natural Science Foundation National (No. L172049), Scientific Research Common Program of Beijing Municipal Commission of Education (No. KM201910005025) and Defense Industrial Technology Development Program (No. JCKY2016204A102) sponsored this research in parts.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Ahmed, S. A.; Dogra, D. P.; Kar, S.; Patnaik, R.; Lee, S. C. et al. (2019): Query-based video synopsis for intelligent traffic monitoring applications. *IEEE Transactions on Intelligent Transportation Systems*.

Chen, G.; Zhan, Y.; Chen, Y.; Xiao, L.; Wang, Y. et al. (2018): Reinforcement learning based power control for in-body sensors in WBANs against jamming. *IEEE Access*, vol. 6, pp. 37403-37412.

Hahn, D. A.; Munir, A.; Behzadan, V. (2019): Security and privacy issues in intelligent transportation systems: classification and challenges. *IEEE Intelligent Transportation System*.

Haus, M.; Waqas, M.; Ding, A. Y.; Li, Y.; Tarkoma, S. et al. (2017): Security and privacy in device-to-device (D2D) communication: a review. *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054-1079.

Marković, N.; Sekuła, P.; Laan, V. Z.; Andrienko, G.; Andrienko, N. (2018): Applications of trajectory data from the perspective of a road transportation agency: literature review and maryland case study. *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 5, pp. 1858-1869.

Msahli, M.; Labiod, H.; Ampt, G. (2019): Security interoperability for cooperative ITS: architecture and validation. *10th IFIP International Conference on New Technologies, Mobility and Security*, pp. 1-6.

Moradikia, M.; Bastami, H.; Kuhestani, A.; Behroozi, H.; Hanzo, L. (2019): Cooperative secure transmission relying on optimal power allocation in the presence of untrusted relays, a passive eavesdropper and hardware impairments. *IEEE Access*, vol. 7, pp. 116942-116964.

Ma, Z.; Lai, Y.; Kleijn, W. B.; Song, Y. Z.; Wang, L. et al. (2018): Variational bayesian learning for dirichlet process mixture of inverted dirichlet distributions in non-gaussian image feature modeling. *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 2, pp. 449-463.

Sedjelmaci, H.; Hadji, M.; Ansari, N. (2019): Cyber security game for intelligent transportation systems. *IEEE Network*, vol. 33, no. 4, pp. 216-222.

Salem, F.; Elhillali, Y.; Niar, S. (2018): Efficient modelling of IEEE 802.11p MAC output process for V2X interworking enhancement. *IET Networks*, vol. 7, no. 4, pp. 210-219.

Shanmugapriya, P.; Baskaran, J.; Nayanatara, C.; Kothari, D. P. (2019): IoT based approach in a power system network for optimizing distributed generation parameters. *Computer Modeling in Engineering and Science*, vol. 119, no. 3, pp. 541-558.

Tu, S.; Waqas, M.; Rehman, S. U.; Aamir, M.; Rehman, O. U. et al. (2018): Security in fog computing: a novel technique to tackle an impersonation attack. *IEEE Access*, vol. 6, pp. 74993-75001.

Waqas, M.; Niu, Y.; Ahmed, M.; Li, Y.; Jin, D. et al. (2018): Mobility-aware fog computing in dynamic environments: understandings and implementation. *IEEE Access*, vol. 7, pp. 38867-38879.

Waqas, M.; Niu, Y., Li, Y.; Ahmed, M.; Jin, D. et al. (2019): Mobility-aware device-to-device communications: principles, practice and challenges. *IEEE Communications Surveys & Tutorials*.

Waqas, M.; Ahmed, M.; Li, Y.; Jin, D.; Chen, S. (2018): Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays. *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 3918-3930.

Wang, Q.; Liu, W.; Yu, H.; Zheng, S.; Gao, S. et al. (2019): CPAC: energy efficient algorithm for IoT sensors network based on enhanced hybrid intelligent swarm. *Computer Modeling in Engineering and Science*, vol. 121, no. 1, pp. 83-103.

Xu, X.; Liu, Y.; Wang, W.; Zhao, X.; Sheng, C. et al. (2018): ITS-frame: a framework for multi-aspect analysis in the field of intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*.

Xiao, L.; Li, Y.; Han, G.; Liu, G.; Zhuang, W. (2016): PHY-layer spoofing detection with reinforcement learning in wireless networks. *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10037-10047.

Xiao, L.; Wan, X.; Su, W.; Tang, Y. (2018): Anti-jamming underwater transmission with mobility and learning. *IEEE Communications Letters*, vol. 22, no. 3, pp. 542-545.

Yu, S.; Liu, J.; Zhang, X.; Wu, S. (2019): Social-aware based secure relay selection in relay-assisted D2D communications. *Computers, Materials and Continua*, vol. 58, no. 2, pp. 505-516.

Zou, Y.; Wang, X.; Shen, W. (2013): Physical layer security with multiuser scheduling in cognitive radio networks. *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103-5113.