IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 5, 2019, accepted September 19, 2019, date of publication October 4, 2019, date of current version November 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2945610

A Secured and Efficient Communication Scheme for Decentralized Cognitive Radio-Based Internet of Vehicles

WEI YAO[1], ABID YAHYA[2], (Member, IEEE), FAZLULLAH KHAN[3,4], (Member, IEEE), ZHIYUAN TAN[5], (Member, IEEE), ATEEQ UR REHMAN[6], JOSEPH M. CHUMA[2], (Member, IEEE), MIAN AHMAD JAN[6], (Member, IEEE), AND MUHAMMAD BABAR[7]

[1]College of Information Science and Technology, Hebei Agriculture University, Baoding 071001, China
[2]Department of Electrical, Computer and Telecommunication, Faculty of Engineering and Technology, Botswana International University of Science and Technology, Palapye, Botswana
[3]Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam
[4]Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam
[5]School of Computing, Edinburgh Napier University, Edinburgh EH11 4DY, U.K.
[6]Computer Science Department, Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa 23200, Pakistan
[7]Department of Computer Science, Iqra University Islamabad, Islamabad 44000, Pakistan

Corresponding author: Fazlullah Khan (fazlullah@tdtu.edu.vn)

ABSTRACT The advancements in hardware technologies have driven the evolution of vehicular ad hoc networks into the Internet of Vehicles (IoV). The IoV is a decentralized network of IoT-enabled vehicles capable of smooth traffic flow to perform fleet management and accident avoidance. The IoV has many commercial applications due to improved security and safety on the roads. However, the rapidly increasing number of wireless applications have challenged the existing spectrum bands allocated to IoV. The IoV has only six communication channels that are congested during the peak hours. The limited number of channels and the presence of congestion on these channels are the challenging issues that affect the safety of vehicles on the road. To mitigate the congestion, Cognitive Radio (CR) can be an optimal solution for the existing IoV Paradigm. In this paper, we propose a secured and efficient communication scheme for a decentralized CR-based IoV (CIoV) network. In this scheme, the Roadside Unit (RSU) senses the spectrum using an energy detection method. Each vehicle independently predicts the Primary User (PU) activity pattern using a hidden Markov model (HMM). Once a vehicle detects a licensed channel free from the PUs, it informs the RSU to store the channel in a database alongside the dedicated direct short-range communication (DSRC) channels for data transmission. The RSU and vehicles are registered with a trusted authority and they mutually authenticate each other. Upon mutual authentication, the RSU assigns communication channels to the vehicles on the road, based on their density. When the density of the vehicles is high, the detected licensed channels are used, otherwise, the DSRC channels are used. We evaluate the performance of CIoV in terms of packet delivery and packet loss ratio, end-to-end delay, and throughput, using NS-2. The simulation results show that the CR-based approach of CIoV outperforms the existing schemes and significantly enhances the performance of the underlying network.

INDEX TERMS Authentication, trusted authority, internet of vehicles, channel detection and allocation, primary user activity, hidden markov model.

I. INTRODUCTION

Recent developments in hardware technologies have introduced a wide range of powerful processing devices such as cameras, radars, sensors etc. These devices have enabled vehicles to communicate with each other in a decentralized fashion [1], and have driven the evolution of self-organizing Internet of Vehicles (IoVs) from Vehicular Ad hoc NETworks (VANETs). Integrating IoVs with the artificial intelligence can bring significant opportunities. For example, when a huge number of smart vehicles and things need to interact with each other, the traditional centralized architectures

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaochun Cheng.

will face numerous challenges in terms of computation and resource utilization. Therefore, to mitigate these challenges, the amalgamation of artificial intelligence, and decentralized computation-based technologies may be an optimal solution. One such technology is Internet of Things (IoT)-based VANETs (IoVs). The IoVs have stringent requirements in terms of security and privacy due to the dynamic nature of their applications [2]. In general, a secured IoV consists of a trusted authority (TA), Roadside Units (RSUs), and a large number of vehicles equipped with On-Board Units (OBUs). The vehicles in an IoV communicate with each other, known as vehicle-to-vehicle communication (V2V) or with RSU, also termed as vehicle-to-infrastructure (V2I) through a direct short-range communication (DSRC) protocol. The DSRC has a common control channel (CCH) and six service channels (SCH) in the 5.9 GHz range as shown in Fig. 1. These six channels get congested during rush hours and as a result, safety control messages may not delivered on time. To mitigate the problem of limited channels, the concept of cognitive radio (CR) has been proposed and investigated in the IoV environment [3].

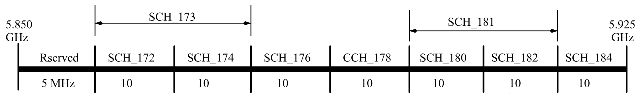


FIGURE 1. DSRC spectrum band and channels in the united states.

A CR-based IoV allows vehicles to detect the unoccupied channels in a licensed band to their bandwidth requirements. The concept of IoV has introduced various research challenges such as limited number of channels, security, safety, self-organization, etc. [4]. The limited number of communication channels in the IoV has raised serious concerns on the safety and smooth flow of traffic. To overcome these challenges, the IoV demands extra channels according to the network requirements. Therefore, in this paper, the CR paradigm is integrated with IoV to create an intelligent, self-organizing, decentralized, and distributed vehicular ad hoc network. The CR-based IoV (CIoV) is a new concept, and its evolution in shown in Fig. 2. The purpose of CIoV is to circumvent the common misconception of spectrum scarcity problem. As highlighted by the report of Federal Communication Commission (FCC) [5], the spectrum scarcity is a man-made problem, and is mainly due to the static spectrum allocation (SSA) of spectrum bands. The characteristics of CR have stimulated the regulatory bodies to officially allow the CR users to utilize the spectrum efficiently, based on the dynamic spectrum allocation (DSA) [6]. As a result, the CR paradigm has widely been accepted and adopted in IEEE 802.16.1, IEEE 802.16m and IEEE 802.20 standards [7], [8].

In CIoV, data transmission is mostly influenced by quality of the channel as well as by the usage pattern of PUs, i.e., if the PUs activity is unpredictable then either collision takes place and/or a primary user (PU) is wrongly deemed to be active. Therefore, precise modelling of PU activities over a channel is mandatory. In this regard, the authors in [6], [9]–[11] modelled the activities of PU over a channel using Discrete Time Markov chain, whilst, the authors have used other techniques for determining and modelling the activity of the PUs [12]–[14]. In this paper, we propose a secured and efficient communication scheme for a decentralized cognitive radio-based IoV. A secured and efficient communication scheme is useful in many application, such as securing any critical network from Denial of Service and fabrication attacks. The integrity of data and on-time delivery of information are the main requirements of patient monitoring and surveillance systems. This can be achieved via high bandwidth and large number of communication channels. Therefore, using a hidden Markov model (HMM), the proposed scheme increases the channel capacity by modelling the PU activities over a licensed channel [6]. In other words, the vehicles predict free channels in the licensed band using HMM. Once detected, the vehicle forwards the channel information to an RSU for storing in its database. When a vehicle requests for a channel, the RSU quickly senses the stored licensed channel using energy detection method, and assigns it to it. In comparison to the existing models, the HMM can be an optimal choice for determining the activity patterns of PUs. [13]. The existing models are mostly not feasible because they cannot accurately model the utilization pattern of PUs due to their dynamic and unpredictable nature. Hence, once the PU pattern is identified, and free channels are detected, the vehicles are programmed to use them only when the DSRC channels are congested or unavailable. The DSRC channels operate wirelessly, and a malicious node can easily manipulate any information exchange via them. Therefore, without authenticating the vehicles and RSUs, a malicious node can launch replay, Denial of Service (DoS), impersonation, and other attacks, through eavesdropping the DSRC channels and injecting, removing, and/or altering the transmitted information.

In general, the use of licensed channels and DSRC channels is not well-studied in the IoV context. Hence, this paper contributes in this context by considering a decentralized CIoV. The significant contributions of this work are as follow.

1) This paper proposes a lightweight mutual authentication scheme for a decentralized CIoV. In the proposed scheme, registration and authentication are required for each vehicle. Upon registration, each vehicle and its corresponding RSU mutually authenticate each other and perform data transmission. The proposed security scheme is efficient against replay, DoS, impersonation and Sybil attacks.
2) Using the DSRC protocol, the vehicular communication is performed by using the dedicated seven channels, i.e., one CCH and six SCH. The proposed scheme redesigned the operations of RSU and vehicles on the road to detect the activities' pattern of PUs using HMM and detect vacant channels in the licensed band.

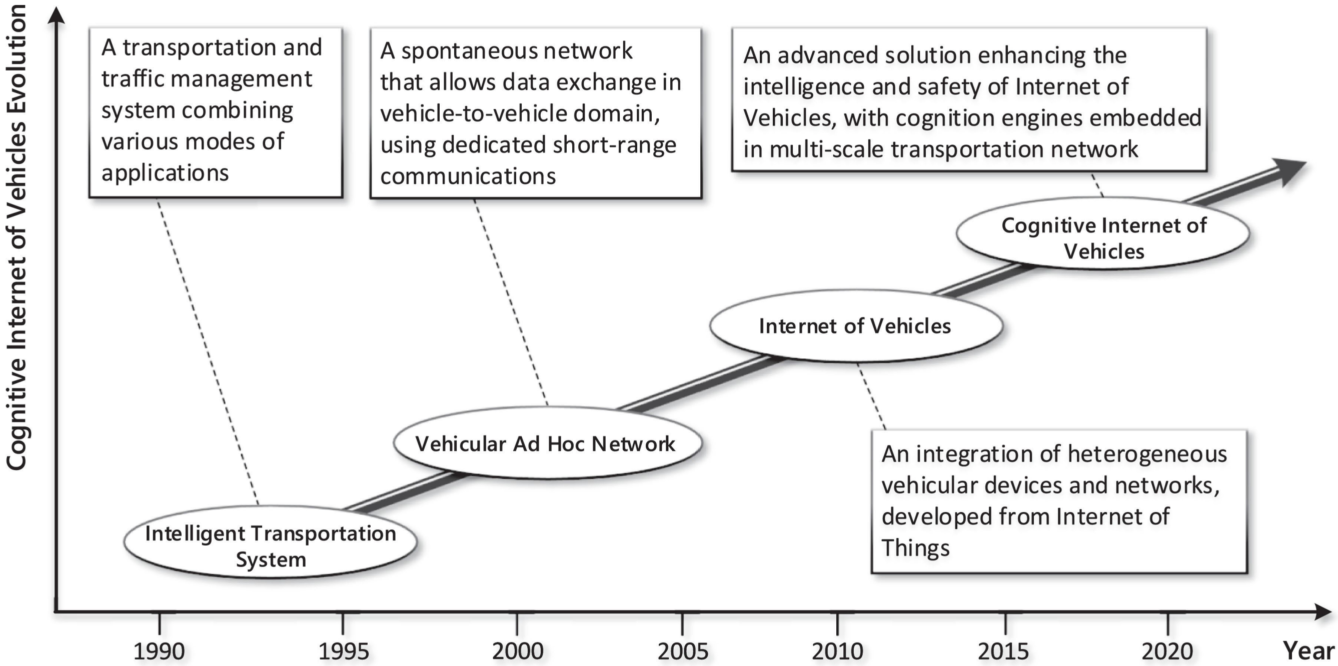


FIGURE 2. Evolution of cognitive internet of vehicles [3].

3) In our decentralized CIoV, the vacant channels are allocated using a novel channel allocation algorithm when the DSRC channels are congested or unavailable. An RSU is responsible for coordinating the channel allocation process to vehicles on the road.
4) The proposed decentralized scheme has been validated via extensive simulations, and the results for packet delivery and loss ratio, end-to-end delay, and throughput show the efficiency of the proposed scheme.

The rest of the paper is organized as follows. In Section II, existing literature is provided followed by system model in Section III. The PU activities' pattern using the HMM model is given in Section IV. The security scheme of CIoV is elaborated in Section V followed by channel allocation process in Section VI. Performance evaluation results are elaborated in Section VII. Finally, the paper is concluded, and future research directions are provided in Section VIII.

II. RELATED WORK

Cognitive Radio-based IoV plays a major role in a variety of applications, ranging from the Intelligent Transportation System (ITS) to e-health and itinerary planning. In the CIoV, vehicles collect data from a deployed region and share with other vehicles, RSUs, and cloud servers using their OBUs. The collected data include but not limited to air pollution, traffic congestion, accidents and passenger information on the roads. This data is analyzed on a local or cloud servers and actions are taken according to the application, i.e., healthcare, traffic control, emergency services. In CIoV, various communication technologies are used at different layers. For example, to have smooth connectivity in CIoV, various wireless technologies along with their requirements are tabulated in Table 1 [3]. However, the cost associated with these technologies for vehicular networks is higher [15], [16]. A cost-effective and efficient technology, i.e., Wireless Access in Vehicular Environments (WAVE) for VANETs was proposed in [17]. The WAVE technology is based on DSRC channels, and these channels are not sufficient, particularly when the number of vehicles increases, leading to network congestion [18], [19]. Therefore, alternate solutions for increasing the channel capacity in IoV need to be explored, and CR-based networks are among one such solutions.

There are numerous studies on different aspects of CR-based networks. For instance, working cycles, sensing and sharing, architectural designs, spectrum management, channel modelling, and CR/PU modelling, etc. [9], [20], [21]. Moreover, various techniques have been used for detecting

TABLE 1. The simulation conditions.

Parameters	Values
Channel data rate	2[Mbps]
Antenna type	Omni direction
Radio propagation	TwoRay ground
Transmission range	500[m]
PHY/MAC protocol	IEEE802.11p
Routing protocol	AODV
Connection type	UDP/CBR
Highway length	8 [Km]
Node speed	60 [Km/h]
Number of Vehicles	50 senders
Packet size	1024[Byte]
Simulation time	1000[s]

PU activities over a channel such as, Markov Chain [9], sensing algorithms [12], discrete-time Markov Chain [11], ON/OFF model, and hidden Markov model [6], [14]. These models predict the free channels in a licensed spectral band, and vehicles within the CIoV can use these channels once the DSRC channels are congested or unavailable. In CIoV, limited work has been conducted on the secured data transmission. Apart from eavesdropping, replay, DoS, Sybil and similar types of attacks, the sensing and learning ability of a CR user is one of the weakness that can easily be exploited by a malicious node [22]. Therefore, securing CIoV is a significant challenge due to its decentralized, distributed, and self-organizing nature [1], [4].

In ubiquitous networks, the security requirements are lenient. In comparison, these requirements are stringent in IoV because of various types of dynamic and on-demand services. For instance, location-based services, infotainment, and safety-related services. The data collected by vehicles are diverse in nature, and is prone to different kind of attacks. For example, if the traffic monitoring of a decentralised and distributed system is under an attack, the critical information is delivered with significant delay having a lower accuracy that result in a reduced users experience [1], [23], [24]. Therefore in literature, various techniques have been proposed to secure IoV. For example, in [23], the authors have proposed a decentralized authentication scheme using a consensus algorithm of blockchain technology. They have obtained the safety of mobile services by reducing the severity of various attacks and the greedy behaviour of vehicles. A blockchain-based IoV has been studied in [24]. The authors have proposed and analyzed a model of vehicle blockchain data. In this model, the decentralised IoV consists of small networks, i.e., sub-blockchains. In [25], the authors have designed a secured authenticated key management protocol, and have performed random-or-real analysis of their proposed model. In [26], the authors have redesigned the OBU of a vehicle with multilevel security. The proposed scheme can protect the vehicle from external threats as well as internal risks. In [27], the authors have studied secured enforcement in IoV and have considering the transmission delay and secured communication. The authors have designed a secured deployment for switches on core network, and have modeled the path selection of switches as a 0-1 programming problem. The problem is further converted to a convex optimization problem and has achieved a much lower delay with secured communication. Details about IoV architecture protocols and security can be studied in [2]. The proposed scheme may not work efficiently in a very dense high speed networks like flying ad hoc networks, Internet of Vehicles and Internet of drones. The possible reasons are the dynamic topology and ad hoc nature of data transmission with various signal strengths.

III. SYSTEM MODEL

This section elaborates the network model, spectrum sensing model, and primary user modelling.

A. NETWORK MODEL AND ASSUMPTIONS

The network model consists of primary users (PUs), secondary users[1] (vehicles), Roadside Units (RSUs), and Trusted Authority (TA). A vehicle is programmed to communicate with other vehicles and RSU using the DSRC channels. To build the proposed decentralized network, we assumed that vehicles are equipped with a tamper-proof device (TPD), the TA is trustworthy, and RSU is authentic, i.e., they do not require registration with the TA. The TA generates two large numbers, i.e., an s_v for generating signature values, and an s_c for establishing a secured communication link between a vehicle and the RSU. The TA broadcasts a certificate of RSU to vehicles within the RSU communication range. For example, the certificate of j^{th} RSU is $\mathbf{C}_{\mathrm{RSU}_j} = (\mathrm{ID}_{\mathrm{RSU}_j}, \mathrm{TRP}_j, \mathrm{TKP}_j, \mathrm{S}_{R_j})$, where, $\mathrm{ID}_{\mathrm{RSU}_j}$ is the identity of j^{th} RSU, $\mathrm{TRP}_j = s_v \cdot \delta$ is used for generating signature values on various points, $\mathrm{TKP}_j = s_c \cdot \delta$ is used for establishing secured communication among various nodes, S_{R_j} is the signature on first three terms, i.e., $\mathrm{sig}(\mathrm{ID}_{\mathrm{RSU}_j}, \mathrm{TRP}_j, \mathrm{TKP}_j)$, and δ is generator of S_P, a set of points. The TA shares $\{s_v, s_c, \mathrm{TRP}_j, \mathrm{TKP}_j\}$ with j^{th} RSU on a private secured channel.

B. SPECTRUM SENSING MODEL

In this paper, the energy detection model for spectrum sensing is used because it is widely accepted and does not require any prior knowledge of PUs [28]. It simply detects a PU based on the sensed energy of a received signal. However, it is unable to perform well under a low signal-to-noise ratio and a fading environment. In our network scenario, the RSU is fixed and obtains various samples of the same signal, resulting in an accurate detection. Each RSU senses C channels for time t and collects P samples of the licensed band. The RSU senses the presence of a PU as formulated by Neyman Pearson and Bayes binary hypothesis given in Eq. (1) below,

$$r_i(j) = \begin{cases} \sum_{j=1}^{P} |n_i(j)|^2, & \text{for } \mathrm{H}_0 \\ \sum_{j=1}^{P} |h_i(j)\dot{s}_i(j) + n_i(j)|^2, & \text{for } \mathrm{H}_1. \end{cases} \tag{1}$$

where, $r_i(j)$ represents the signal received by an RSU for channel C_i, $\forall\ i \in \{1, 2, 3, \ldots, n\}$ observed over j samples, where $j \in \{1, 2, 3 \ldots, \mathrm{P}\}$, $s(j)$ is the signal of a PU, $h(j)$ represents channel gain, and $n(j)$ represents an independent and identically distributed additive white Gaussian noise (AWGN) with zero-mean and variance σ^2. In this equation, P is equal to $2DB$, where D represents the detection time, and B is the bandwidth in Hertz (Hz). The H_1 and H_0 represent the hypothesis test of the existence and non-existence of PU, respectively.

[1] The secondary users (SUs) do not pay for using a channel in licensed bands, also known as cognitive radio users. However, an SU should not interfere with the PU and must vacate the channel when a PU arrives.

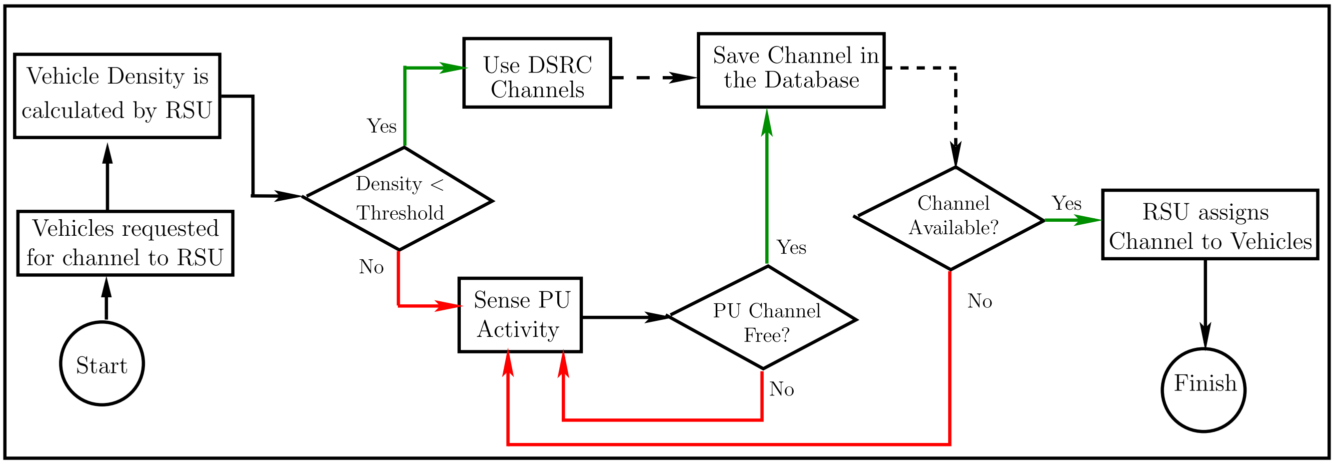


FIGURE 3. The channel sensing and allocation in the proposed CIoV environment.

C. PRIMARY USER MODELLING AND ASSUMPTIONS

In our model, it is assumed that the location of an RSU[2] and the spectrum is immovable during sensing. It is also assumed that each RSU and the vehicles are mounted with multi-radio interfaces. The DSRC has six service channels (SCH), and a common control channel (CCH). The SCHs are used for data exchange, whereas, a CCH is used for control signalling. In our network model, one radio of the vehicle is set to CCH for smooth connectivity to the network, whereas, another radio is used for data exchange. The scenario used in our model is that each segment of a highway is covered by an RSU, which is responsible for spectrum sensing. The RSU can obtain various free samples of PU activities at a particular time. Our network consists of S vehicles (SUs) contending for C channels in a licensed band. Upon acquiring the channels, they are stored in the database with DSRC channels and are assigned to vehicles, based on the channel utilization and location of PUs. The working model of our decentralized CIoV environment is shown in Fig. 3. When a vehicle requests for a channel, the RSU decides the channel allocation based on vehicle density. For example, if vehicle density is less than the specified threshold a DSRC channel is assigned, otherwise identify vacant channels in the licensed spectrum band and allocate to the vehicle.

IV. PRIMARY USER ACTIVITY MODELING USING HMM

The hidden Markov model (HMM) is derived from the Markov model. It can handle real-world applications and is used for sequential or temporal data chain in which the states are partially observable. Fig. 4 depict the graphical representation of the HMM.

The HMM has discrete random variables $\mathbf{Z} = Z_1, Z_2, \ldots, Z_n \in \{1, 2, \ldots, n\}$, and $X = X_1, X_2, \ldots, X_n \in \mathbf{X} = \{$discrete values, real values, R^d $\}$. The $\mathbf{X}$ are observed random variables, and $\mathbf{Z}$ are hidden variables. In our model, the hidden variables represents the actual PU activity, whereas, the observed

[2]The RSU senses the licensed spectrum, to ensure the availability of predicted free channels by vehicles.

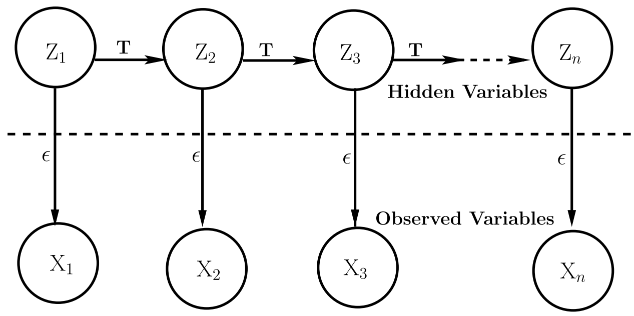


FIGURE 4. Pictorial representation of HMM.

variables are energy on a spectrum under sensing by RSU. The joint distribution of these random variables corresponds to the HMM model, as shown in Fig. 4.

$$P(X_1, X_2, \ldots, X_n, Z_1, X_2, \ldots, Z_n) = P(Z_1)P(X_1|Z_1)\Pi_{k=2}^{n}P(Z_k|Z_{k-1})P(X_k|Z_k). \quad (2)$$

A. Hidden Markov Model Parameters

The HMM has three parameters/probabilities, i.e., a transition probability $T_{(ij)}$, emission probability $\varepsilon_i(X)$, and the initial probability $\pi(i)$. The transition probability is shown in Eq. (3), where $\{1,2,\ldots,m\}$ is a set of hidden variables,

$$T_{(ij)} = P(Z_{k+1} = j|Z_k = i), \quad \forall i,\ j \in \{1, 2, \ldots, m\}. \quad (3)$$

The emission probability in Eq. (4) is a probability distribution on $\mathbf{X}$ as a probability density function (pdf) for $\{1,2,\ldots,m\}$ hidden variables and X observed variables, $\forall_X \in \mathbf{X}$,

$$\varepsilon_i(X) = P(X|Z_k = i), \quad \text{for } i \in \{1, \ldots, m\},\ \textit{and}\ X \in \mathbf{X}. \quad (4)$$

When $\mathbf{X}$ takes discrete random values, then Eq. (4) can be written as probability mass function (pmf), as shown in Eq. (5),

$$\varepsilon_i(x) = P(X_k = X|Z_k = i), \quad \text{for } i \in \{1, \ldots, m\},\ \text{and } X \in \mathbf{X}. \quad (5)$$

The initial distribution of the HMM is given in Eq.(6),

$$\pi(i) = P(Z_1 = i), \quad \text{for } i \in \{1, \ldots, m\}. \tag{6}$$

The joint distribution in terms of the above three parameters may be written as,

$$P(X_1, \ldots, X_n, Z_1, \ldots, Z_n) = \pi(i)\varepsilon_{Z_1}(X_1)\Pi_{k=2}^{n} T_{(Z_k-1,Z_k)}\varepsilon_{Z_k}(X_k). \tag{7}$$

Forward-Backward Algorithm: The fundamental working principles of HMM is based on probability distribution. In other words, HMM gives us tractable inference using combined parameters. The engine that drives the HMM is the inference algorithm, and its fundamental part is called forward-backward algorithm. The forward-backward algorithm is a dynamic programming and it assumes that the transition probability $P(Z_k|Z_{k-1})$, emission probability $P(X_k|Z_k)$, and initial distribution $P(Z_1)$ are known. The goal of forward-backward algorithm is to compute $P(Z_k|X)$, and the hidden values $\mathbf{Z}_k$ on the given observed values $\mathbf{X}$. The two parts of the posterior distribution on $P(Z_k|X)$ are shown in Eq. (8),

$$P(Z_k|X) \propto_{Z_k} P(Z_k, X) = P(X_{k+1:n}|Z_k, X_{1:k})P(Z_k, X_{1:k}). \tag{8}$$

Applying the separation properties with $X_{1:k}$ is conditionally independent of Z_k on Eq. (8), which yields Eq. (9),

$$P(Z_k|X) \propto_{Z_k} P(Z_k, X) = P(X_{k+1:n}|Z_k)P(Z_k, X_{1:k}). \tag{9}$$

The forward algorithm computes the joint probability distribution of Z_k and $X_{1:k}$, i.e., $P(Z_k, X_{1:k})$ ∀ k = {1,2,…,n}, which is exactly the second part (right side) of Eq. (9). The backward algorithm computes the joint distribution of $Z_{k+1:n}$ for a given Z_k, i.e., $P(X_{k+1:n}|Z_k)$ ∀ k = {1,2,…, n}, which is exactly the first part (right side) of Eq. (9). Once $P(Z_k|X)$ is known, the change detection such as, $P(Z_k \neq Z_{k+1}|X)$, can be inferred. The Baum-Welch algorithm can be used to estimate the HMM parameters by computing the forward-backward algorithm with Expectation Maximization. The forward-backward algorithm can obtain sampling from the posterior distribution, i.e., $Z_k|X$, which is required as PU activity.

Forward algorithm: The goal of this part is to compute joint distribution on Z_k and $X_{1:k}$, i.e., $P(Z_k, X_{1:n})$. Introducing the HMM parameters $T_{(ij)}$, $\varepsilon_i(X)$, and $\pi(i)$ with factoring and marginalization property, it yields

$$P(Z_k, X_{1:k}) = \sum_{Z_{k-1}=1}^{m} P(Z_k, Z_{k-1}, X_{i:k}). \tag{10}$$

Factoring Eq. (10) results in,

$$P(Z_k, X_{1:k}) = \sum_{z_{k-1}}^{m} P(X_k|Z_k, Z_{k-1}, X_{1:k-1})P(Z_k|Z_{k-1}, X_{i:k-1}) \times P(Z_{k-1}|X_{i:k-1})P(X_{1:k-1}). \tag{11}$$

The desired results can be obtained by combining the last two terms of Eq. (11), and it gives

$$P(Z_k, X_{1:k}) = \sum_{z_{k-1}}^{m} P(X_k|Z_k, Z_{k-1}, X_{1:k-1}) \times P(Z_k|Z_{k-1}, X_{i:k-1})P(Z_{k-1}, X_{i:k-1}). \tag{12}$$

Putting condition on Z_k in first term, whereas in second term Z_{k-1} in conditionally independent on $X_{i:k-1}$, gives Eq. (12) as,

$$P(Z_k, X_{1:k}) = \sum_{Z_{k-1}}^{m} P(X_k|Z_k)P(Z_k|Z_{k-1})P(Z_{k-1}, X_{i:k-1}). \tag{13}$$

Let $\alpha_k(Z_k) = P(Z_k, X_{1:k})$, this results in Eq. (13) as,

$$\alpha_k(Z_k) = \sum_{Z_{k-1}}^{m} P(X_k|Z_k)P(Z_k|Z_{k-1})\alpha_{k-1}(Z_{k-1}) \quad \text{for } k \geq 2. \tag{14}$$

which is the recursion function for forward algorithm. By putting $\alpha = 1$, in Eq. (14), the initial distribution of forward algorithm can be computed as,

$$\alpha_1(Z_1) = P(Z_1, X_1) = P(Z_1)P(X_1|Z_1). \tag{15}$$

Backward algorithm: The goal of the backward algorithm is to compute $P(X_{k+1:n})|Z_k$ ∀ k = 1,…,n-1 and $\forall Z_k = 1, \ldots, m$. Applying the rules of probability and Markov properties yields the following equation,

$$P(X_{k+1:n})|Z_K) = \sum_{Z_{k+1}=1}^{m} P(X_{k+1:n}, Z_{k+1}|Z_k). \tag{16}$$

Introducing the conditional independence properties can reduce Eq. (16) to $Z_{k+1}|Z_k$ as,

$$P(X_{k+1:n})|Z_K) = \sum_{Z_{k+1}=1}^{m} P(X_{k+2:n}, Z_{k+1}, Z_k, X_{k+1}) \times P(X_{k+1}|Z_k)Z_{k+1}, Z_K)P(Z_{k+1}|Z_k). \tag{17}$$

Applying the deseparation properties on Eq. (17), results in

$$P(X_{k+1:n})|Z_K) = \sum_{Z_{k+1}=1}^{m} P(X_{k+2:n}, Z_{k+1}) \times P(X_{k+1}|Z_k)Z_{k+1}P(Z_{k+1}|Z_k). \tag{18}$$

Let $\beta_k(Z_k) = P(X_{k+1:n})|Z_K)$, then Eq. (18) can be written as follow, which is the recursive function of backward algorithm.

$$\begin{aligned}\beta_k(Z_k) &= P(X_{k+1:n})|Z_k) \\ &= \sum_{Z_{k+1}=1}^{m} \beta_{k+1}(Z_{k+1})P(X_{k+1}|Z_{k+1}) \\ &\quad \times P(Z_{k+1}|Z_k) \quad \text{for } k = 1, \ldots, n-1.\end{aligned} \tag{19}$$

The initial distribution of backward algorithm can be obtained by putting $k = n - 1$ in Eq. (19),

$$\beta_n(Z_n) = 1. \quad \forall Z_n. \tag{20}$$

Finally, by combining the forward and backward algorithms, Eq. (9) can be written as,

$$P(X_k|X) = \beta_k(Z_k)\alpha_k(Z_k). \quad (21)$$

Based on Eq. (21), vehicles predict the presence or absence of a PU over a channel.

V. AUTHENTICATION SCHEME

In this section, we provide details of vehicle registration in the network, and mutual authentication of vehicles and roadside unit. The assumptions used in this section are given in subsection III-A.

A. PRE-DEPLOYMENT PHASE

In the beginning, the TA selects a set of points S_P of order κ, and δ is a generator of S_P. The TA generates $\Psi \in Z_\kappa^*$ and calculates $\Phi = \Psi \times \delta$, where Ψ and Φ are the private and public keys of the system. Then TA chooses four secure hash functions h_s: $\{0, 1\}^* \rightarrow Z_\kappa^*$, where s = {1,2,3,4}. The TA stores Ψ into its memory and publishes the system parameters S_P, δ, Φ, h_1, h_2, h_3, h_4, which are available to all vehicles and RSUs.

B. VEHICLE REGISTRATION PHASE

When a new vehicle S_i wants to join the network, it has to register with the TA. After registration, the TPD of S_i must be initialized. Vehicles registration is two steps process given below,

1) The vehicle S_i first chooses a unique identity ID_i and password PW_i of its choice, and a 128-bit random key u_i. The on-board-unit (OBU_i) of S_i calculates the masked password $MPW_i = h(PW_i \parallel u_i)$ and sends the registration request $\langle ID_i, (MPW_i \oplus \Phi)\rangle$ to the TA through secure channel.
2) Upon reception of $\langle ID_i, (MPW_i \oplus \Phi)\rangle$, the TA checks if the vehicles is already registered? If not, the TA generates $RID_{T_i} = \{RID_{T_0}, RID_{T_1}, \ldots, RID_{T_{m-1}}\}$ and $PK_{T_i} = \{PK_{T_0}, PK_{T_1}, \ldots, PK_{T_{m-1}}\}$, the sets of pseudo random identities and their corresponding private keys, respectively. The number of elements in each set are m, and are generated using Eq. (22).

$$PK_{T_i} = (r_i + h_2(RID_i||r_i \cdot \delta||L_t) \times \Psi \ mod \ \kappa) \oplus MPW_i \quad (22)$$

where r_i is a random number and δ is the generator of S_P. Once PK_{T_i} is generated, then TA updates the vehicle (S_i) identity information table with $\{ID_i, RID_i, r_i \cdot \delta \parallel L_t\}$, and writes $\{RID_i, r_i \cdot \delta, PK_{T_i}, L_t\}$ into the TPD of S_i.

C. MUTUAL AUTHENTICATION

When a vehicle S_i enters into the communication range of RSU_i and send a join requests. If S_i is already registered and not authenticated yet, then mutual authentication is performed using the following steps,

1) The S_i extracts (ID_{RSU_j}, TRP_j, TKP_j, S_{R_j}) from the certificate of jth RSU, $\mathbf{C}_{RSU_j}$.
2) Upon reception of a valid $\mathbf{C}_{RSU_j}$, the S_i generates $RID_{S_i} = \{RID_{S_0}, RID_{S_1}, \ldots, RID_{S_{n-1}}\}$ and $PK_{S_i} = \{PK_{S_0}, PK_{S_1}, \ldots, PK_{S_{n-1}}\}$, a random number $\xi \in Z_\kappa^*$, and calculates $\chi = \xi \cdot \delta$, $CT_1 = (RID_{S_i} \parallel r_i \cdot \delta \parallel L_t) \oplus h_1(\xi \cdot TKP_j \parallel T_1)$, $V_1 = h_3(\chi \parallel RID_{S_i} \parallel r_i \cdot \delta \parallel T_1) \times \xi + PK_{S_i} \bmod \kappa$, where T_1 is current timestamp. Finally, S_i sends $\{\chi, CT_1, V_1, T_1\}$ to RSU_j.
3) Upon reception of $\{\chi, CT_1, V_1, T_1\}$, the RSU_j checks validity of the received message using the timestamp T_1. If valid, then the RSU decrypts the cipher text using the secret key s_v by computing $(RID_{S_i} \parallel r_i \cdot \delta \parallel L_t) = CT_1 \oplus h_1(s_v \cdot \chi \parallel T_1)$. Then RSU_j checks lifetime validity, L_t, and checks if Eq. (22) hold.

$$V_1 \cdot \delta = h_3(\chi||RID_{S_i}||r_i \cdot \delta||T_1) \cdot \chi + r_i \cdot \delta + h_2(RID_{S_i}||r_i \cdot \delta||L_t) \cdot \Phi \quad (23)$$

If Eq. (23) holds, it means that S_i is a legitimate vehicle. Then RSU_j computes $CT_2 = (s_v \parallel L_t) \oplus h_1(s_c \cdot \chi \parallel T_2)$, $V_2 = h_4(RID_{S_i} \parallel s_v \parallel L_t \parallel T_2)$ and sends $\{CT_2, V_2, T_2\}$ to S_i through a public channel.
4) Upon receipt of the messages from RSU_j, S_i checks the validity of the timestamp T_2. If valid, then S_i computes $s_v \parallel L_t = CT_2 \oplus h_1(\xi \cdot TKP_j \parallel T_2)$, $V_2' = h_4(RID_{S_i} \parallel s_v \parallel L_t \parallel T_2)$ and compares V_2' with the received value V_2. If they are not equal, S_i terminates this session. Otherwise, S_i believes the legitimacy of RSU_j. Finally, S_i stores $\{_v, L_t\}$ into its secret memory.

VI. CHANNEL ASSIGNMENT

In this section, we elaborate the assignment of PU channels to the vehicles by an RSU. The detection of free channels in the licensed spectral band can be calculated based on Eq. (21) by the RSU. The RSU gets a list of available channels, stores it in the channel database, and allocates channels to the vehicles on the road using Algorithm 1. The vehicles will not create harmful interference to the PUs if channels assignment is performed appropriately. Note that, the detected channels in the licensed band will be assigned when the DSRC channels are not available or congested. Hence, it is important to determine weather to use DSRC channels or the channels free from PU. The channels are categorized based on the weight (μ) reported by vehicles. The μ is decided according to channel conditions (ρ and η), where ρ and η show a channel on which various vehicles perform successful and unsuccessful transmission, respectively. The RSU then updates the list of ρ channels based on communication results.

Let $\beta(L, I)_{S,C}$ is a list of free channels obtained using Eq. (21) , and ∂_n is the channel a single user get from $\beta(L, I)_{S,C}$ list. The ∂_n can be shown as in the following equation.

$$\partial_n = \sum_{c=0}^{C-1} a_{s,c}.b_{s,c} \quad (24)$$

Algorithm 1 Licensed Channel Allocation to Vehicles

procedure
RSU senses spectrum using energy detection and each node prdicts a list of free channels **C** based on Eq. (21)
  if $d_S(S, C) < d_{min}$ **do**; ▷ where $d_S(S, C)$ is the interference range of user S for channel C, d_{min} is the minimum interference range (d_S), and $l_{(S,C)}$ shows that channel C is available for user S.
  $l_{(S,C)} = 0$
  else
  $l_{S,C} = 1$
   if $d_S(S, C) \leq d_{max}$ **do**
    $b(S, C) = d_S(S, C)^2$; ▷ where $b(S, C)$ is channel m bandwidth for user n, and d_{max} is the maximum interference range d_S.
   else if $(Dist(S, T) \leq d_S(S, C) + d_S(T, C)$ **do**
    $I_{S,T,C} = 1$
    else
    $I_{S,T,C} = 0$; ▷ where $I_{S,T,C}$ shows that channel C is occupied by both user S & T, I is the interference on channel C between these users, and $Dist(S, T)$ is the distance between users.
   if $(a_{(S,C)} + a_{(T,C)} \leq 1$ **do**
    $a_{(S,C)} = 1$; ▷ where $a_{(S,C)}$ is the assignment of channel m to user n.
   end if
   end else if
   end if
  end if
end procedure

If the total utilization of the network is represented by $\mathbf{U}(T)$, then we can define channel allocation by the following optimization function:

$$A^* = \underset{A \in \beta(L,I)_{S,C}}{argmax} \ \mathbf{U}(T) \tag{25}$$

VII. RESULTS AND DISCUSSION

To evaluate our proposed system, we performed simulation based investigation. In this section, we aimed to study the impact of using licensed bands when the number of vehicles is large. In this paper, a traffic scenario with node mobility on a highway was designed using Simulation of Urban Mobility (SUMO) and MObility generator for VEhicular networks (MOVE) [29]. The generated mobility files were converted and sent to the network simulator (NS-2) to configure the network by assigning UDP, AODV, and IEEE 802.11p MAC protocol based on CSMA/CA algorithm. The simulations conditions are shown in Table 1. Further, the results show that the PU channels have a significant impact on the performance CIoV. This section discussed the performance results in terms of packet delivery ratio, throughput, and end-to-end delay.

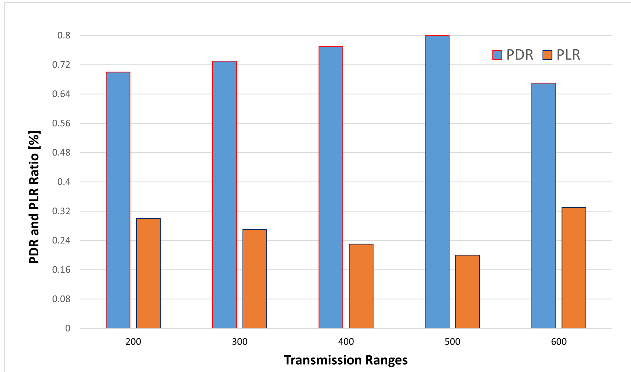


FIGURE 5. PDR and PLR ratio against transmission ranges in the IoV and CIoV.

A. PACKET DELIVERY RATIO

The packet delivery ratio (PDR) can be defined as the packets correctly received at the final destination. The PDR is calculated using Eq. (26).

$$pdr = \frac{P_{rec}}{P_{snd}} \tag{26}$$

where, P_{rec} is the number of packets successfully received at the destination, and P_{sen} is the number of packets transmitted from a source.

The PDR and packet loss ratio (PLR) against various transmission ranges for IoV and CIoV are illustrated in Fig. 5. Note that, the exact values of PDR and PLR for CIoV and IoV are due to the similar effect of transmission ranges on these. The increase in PDR and decrease PLR upto transmission range of 500 meters is due to single-hop communication. It is achieved by high power signal that can cover wider area where maximum packets are received successfully. In comparison to the transmission range of 500 meters, that is, at 600 meters or above the PDR decreased and PLR increased due to the higher contention at the MAC layer causing higher interference rate. The MAC layer contention restricts many vehicles from communication due to carrier sense multiple access that reduces the use of bandwidth. In contrast, when the transmission range is 200 meter the value of PDR is about 70% and PLR is 30% due to increased number of hops between the source and destination. It is because decreasing the transmission range causes increase number of hops, that may lead to frequent dis-connectivity. It is important to mention here that Fig. 5 and Fig. 7 show the results of IoV only. It is because the transmission range has same affect on IoV and CIoV.

Similarly, in the environment of IoV and CIoV the PDR and PLR against different number of vehicles are presented in Fig. 6. When the number of vehicles are upto 20, the PDR and PLR of IoV and CIoV is the same due to same number of available channel. In contrast, when the number of vehicles are more than 20, the higher values of PDR and the lower values of PLR for CIoV is due to the free channels detected in the licensed band. As a result, maximum packets can be transmitted in the network. Moreover, in both cases the PDR ratio

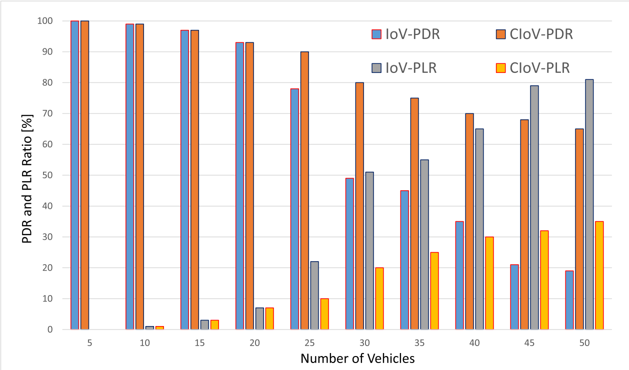


FIGURE 6. PDR and PLR ratio against number of vehicles.

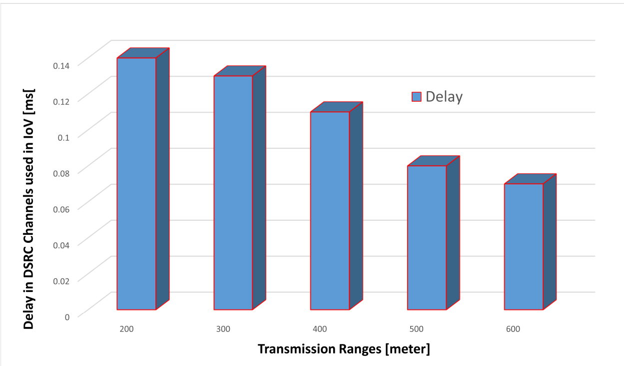


FIGURE 7. End-to-End delay in the IoV against different transmission ranges.

decreased when the number of vehicles increases. The reason for IoV environment is due to limited channels, whereas high contention between vehicles and higher computational cost of channel detection and allocation in the CIoV environment. However, the decrease is minimum in CIoV environment compare to the IoV environment because in CIoV we can use extra channels detected free in the licensed band.

B. END TO END DELAY

In this section, we define the end-to-end delay for IoV and CIoV environment. In Fig. 7, the end-to-end delay against different transmission ranges in the IoV environment is depicted. In the IoV environment, when the transmission range is lower, the number of hops may increase which causes higher delay. In contrast, when the transmission range is higher, i.e., 600 meters the delay is lower. It is because, a vehicle can cover a wider area resulting the decreased number of hops with a high vehicular density resulting in higher connectivity between senders and receivers. On the other hand, when the transmission range is 100 meter the delay is higher due to increase number hops between senders and receivers. Similarly, in Fig. 8, the end-to-end delay against different number of vehicles are shown. The increasing number of communicating vehicles causes higher end-to-end delay in the IoV environment. When the number of vehicles are less the end-to-end delay is minimum due to minimum utilization of DSRC channels. However, the

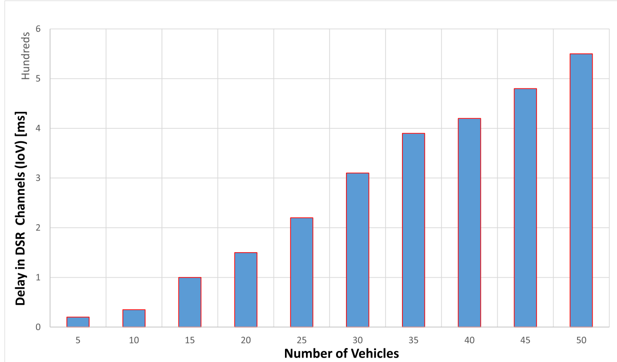


FIGURE 8. End-to-End delay in the IoV against different number of vehicles.

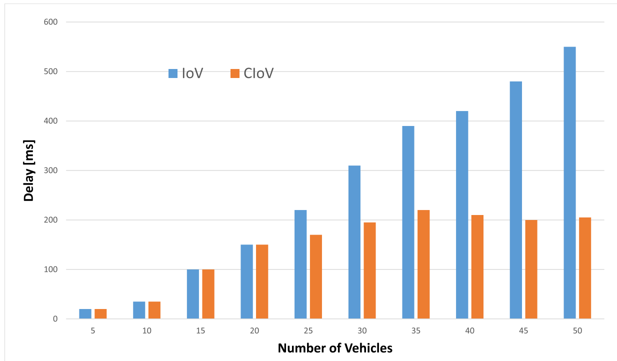


FIGURE 9. End-to-End delay against different number of vehicles.

end-to-end delay is continuously increasing when the number of vehicles increase as shown in Fig. 8. For example, for 50 vehicles the end-to-end delay is about 5.5 seconds. It is because, the six DSRC channels are insufficient for such a high number of vehicles. Furthermore, the end-to-end delay for different number of vehicles in IoV and CIoV is elaborated in Fig. 9. In this figure, the end-to-end delay of CIoV is less than the IoV because in the first case more channels are available for communication. When the number of vehicles are upto 20, the end-to-end delay of IoV and CIoV is the same because the DSRC channels are sufficient for these vehicles. In contrast, when the number of vehicles are more than 20, the lower end-to-end delay for CIoV is due to the free channels detected in the licensed band. As a result, maximum packets take less time to be successfully transmitted in the network. Moreover, with the increase number of vehicles the end-to-end delay increases in the IoV environment. On the other hand, the increase number of vehicles has reduced effect on end-to-end delay in the CIoV environment. It is because in CIoV environment we use extra channels detected free in the licensed band.

C. THROUGHPUT

In this section, we elaborated the network throughput, which is the number of total bits successfully transmitted in a particular period. The network throughput against various number of vehicles in IoV and CIoV environment is demonstrated in Fig. 10. In this figure, throughput of CIoV is higher than

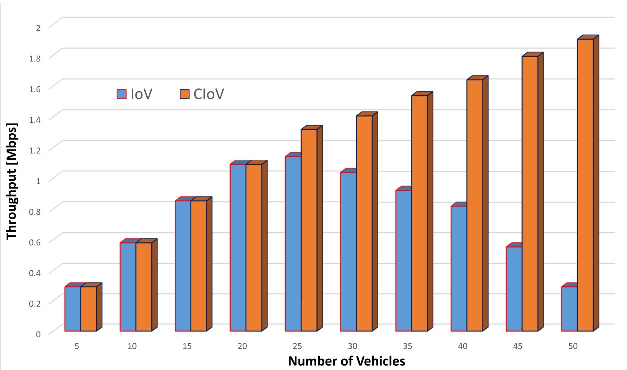


FIGURE 10. Throughput of the network against different number of vehicles.

the IoV, especially when the number of vehicles are large. The reason for higher throughput in CIoV is due to the usage of free channels detected in the licensed band. When the number of vehicles are less the throughput in both environment is the same. However, when the number of vehicles are more than 20, then the throughput of the IoV is dramatically decreases. In contrast, the throughout of the CIoV increases with the increase in the number of vehicles. It is because in CIoV environment we get extra channels detected free in the licensed band.

VIII. CONCLUSION

In this paper, we have proposed a cognitive radio-based Internet of Vehicles (CIoV). In our proposed scheme, the RSU senses the channels using an energy detection method, whereas, the vehicles predict free channels in the licensed spectral band using a hidden Markov model (HMM). The detected channels are reported to the RSU and are stored in its database. In addition, we have used a lightweight authentication scheme, where the vehicles and RSU mutually authenticate each other. The authentication scheme prevents the impersonation, replay, DoS, and different kinds of attacks. The simulation results prove the efficiency of the proposed scheme in terms of PDR, PLR, end-to-end delay, and throughput. The PDR of CIoV is higher than the IoV due to the use of extra channels in the licensed band. The CIoV also has a smaller delay and higher throughput, especially when the number of vehicles increases. It is because of getting extra channels in the licensed band using HMM. The experimental results show that the mutual authentication and the PU modelling via HMM have promising results in predicting the free channels. In future, we plan to use two-state and four-state HMM to predict the misdetection and false alarm of the system.

REFERENCES

[1] F. A. Milaat and H. Liu, "Decentralized detection of GPS spoofing in vehicular Ad HOC networks," *IEEE Commun. Lett.*, vol. 22, no. 6, pp. 1256–1259, Jun. 2018.

[2] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[3] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, "Cognitive Internet of Vehicles," *Comput. Commun.*, vol. 120, pp. 58–70, May 2018.

[4] A. Allouch, A. Koubâa, M. Khalgui, and T. Abbes, "Qualitative and quantitative risk analysis and safety assessment of unmanned aerial vehicles missions over the Internet," *IEEE Access*, vol. 7, pp. 53392–53410, 2019.

[5] P. Kolodzy and I. Avoidance, "Spectrum policy task force report," FCC, Washington, D.C., USA, Tech. Rep. ET Docket, 2002, vol. 40, no. 4, pp. 147–158.

[6] F. Khan, A. U. Rehman, A. Yahya, Z. Tan, M. A. Jan, J. Chuma, and M. Babar, "A secured and efficient communication scheme for decentralized cognitive radio-based Internet of vehicles," *IEEE Access*, to be published.

[7] *IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 3: Advanced Air Interface*, Standard IEEE Std 802.16m-2011(Amendment to IEEE Std 802.16-2009), May 2011, pp. 1111–1112.

[8] *IEEE Standard for Wireless Man-Advanced air Interface for Broadband Wireless Access Systems*, Standard IEEE Std 802.16.1-2012, Sep. 2012, pp. 1090–1091.

[9] F. Khan, A. U. Rehman, M. Usman, Z. Tan, and D. Puthal, "Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-wait," *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 479–488, Jun. 2018.

[10] A. U. Rehman, C. Dong, L.-L. Yang, and L. Hanzo, "Performance of cognitive stop-and-wait hybrid automatic repeat request in the face of imperfect sensing," *IEEE Access*, vol. 4, pp. 5489–5508, 2016.

[11] A. U. Rehman, C. Dong, V. A. Thomas, L.-L. Yang, and L. Hanzo, "Throughput and delay analysis of cognitive go-back-n hybrid automatic repeat reQuest using discrete-time Markov modelling," *IEEE Access*, vol. 4, pp. 9659–9680, 2016.

[12] D.Z. Chen, J. Ren, N. Zhang, M. K. Awad, H. Zhou, and X. S. Shen, "Energy-harvesting-aided spectrum sensing and data transmission in heterogeneous cognitive radio sensor network," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 831–843, Jan. 2017.

[13] E. Esenogho and T. Walingo, "Primary users on/off behaviour models in cognitive radio networks," in *Proc. Int. Conf. Wireless Mobile Commun. Syst. (WMCS)*, 2014, pp. 209–214.

[14] F. Azmat, Y. Chen, and N. Stocks, "Analysis of spectrum occupancy using machine learning algorithms," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 6853–6860, Sep. 2016.

[15] W. Xu, W. Shi, F. Lyu, H. Zhou, N. Cheng, and X. Shen, "Throughput analysis of vehicular Internet access via roadside WiFi hotspot," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3880–3991, Apr. 2019.

[16] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[17] M. D. Nathanson and N. Fairbanks, "Vehicle communications via wireless access vehicular environment," U.S. Patent 9 503 968 B2, Mar. 20, 2018.

[18] S. A. Ahmad, A. Hajisami, H. Krishnan, F. Ahmed-Zaid, and E. Moradi-Pari, "V2v system congestion control validation and performance," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2102–2110, Mar. 2019.

[19] D. Tian, J. Zhou, Y. Wang, Z. Sheng, X. Duan, and V. C. M. Leung, "Channel access optimization with adaptive congestion pricing for cognitive vehicular networks: An evolutionary game approach," *IEEE Trans. Mobile Comput.*, to be published.

[20] A. U. Rehman, V. A. Thomas, L. L. Yang, and L. Hanzo, "Performance of cognitive selective-repeat hybrid automatic repeat request," *IEEE Access*, vol. 4, pp. 9828–9846, 2016.

[21] F. Khan and K. Nakagawa, "Comparative study of spectrum sensing techniques in cognitive radio networks," in *Proc. World Congr. Comput. Inf. Technol. (WCCIT)*, Jun. 2013, pp. 1–8.

[22] D.-T. Ta, N. Nguyen-Thanh, P. Maillé, and V.-T. Nguyen, "Strategic surveillance against primary user emulation attacks in cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 3, pp. 582–596, Sep. 2018.

[23] X. L. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for Internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45061–45072, 2019.

[24] T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2018.

[25] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. H. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[26] L. Wang and X. Liu, "NOTSA: Novel OBU with three-level security architecture for Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3548–3558, Oct. 2018.

[27] Y. Qian, M. Chen, J. Chen, M. S. Hossain, and A. Alamri, "Secure enforcement in cognitive Internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1242–1250, Apr. 2018.

[28] S. K. Yoo, P. C. Sofotasios, S. L. Cotton, S. Muhaidat, O. S. Badarneh, and G. K. Karagiannidis, "Entropy and energy detection-based spectrum sensing over F composite fading channels," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4641–4653, Jul. 2019.

[29] M. Behrisch and M. Weber, *Simulating Urban Traffic Scenarios: 3rd SUMO Conference 2015 Berlin, Germany*. Springer, 2018.

WEI YAO received the Ph.D. degree from Hebei Agriculture University, China. He is currently an Associate Professor with the College of Information Science and Technology, Hebei Agriculture University. He has published research work in prestigious journals and conferences. His research interests include intelligent information processing, machinery learning, and pattern recognition.

ABID YAHYA received the M.Sc. and Ph.D. degrees in wireless and mobile systems from the Universiti Sains Malaysia, Malaysia.

He is currently with the Botswana International University of Science and Technology. He began his career on an engineering path, which is rare among other researcher executives. He has applied the combination of practical and academic experience to a variety of consultancies for major corporations. He has more than 115 research publications to his credit in numerous reputable journals, conference papers, and book chapters. His recent two books are *Steganography Techniques for Digital Images* and *LTE-A Cellular Networks: Multi-Hop Relay for Coverage, Capacity and Performance Enhancement* (Springer International Publishing, July 2018 and January 2017) and are being followed in national and international universities.

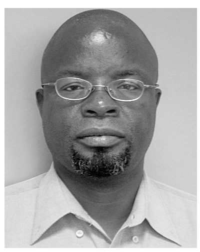
Prof. Yahya has received several awards and grants from various funding agencies and supervised a number of Ph.D. and master's candidates. He was assigned to be an External and Internal Examiner for postgraduate students. He has been invited a number of times to be a Speaker or Visiting Lecturer at different multinational companies. He sits on various panels with the Government and other industry-related panels of study.

FAZLULLAH KHAN is currently a Researcher with Ton Duc Thang University, Ho Chi Minh City, Vietnam, and an Assistant Professor with Abdul Wali Khan University Mardan, KPK, Pakistan (regular) and the School of Software, Northwestern Polytechnical University, Xi'an, Shaanxi, China (visiting). His research interests include performance analysis of cognitive-aided ad hoc networks. Recently, he has been involved in the Internet of Things, the Internet of Vehicles security and privacy issues, and big data analytics. He has published his research work in various IEEE, Elsevier, Springer Journals and has two edited books to his name. He received the gold medal in his B.S. degree and studied higher education on prestigious Japanese Scholarships of MEXT. He has been the Chair of various conferences and special sessions, such as IEEE EAI Future5v-2017, CCODE-2017, EAI IoT-BC2, and OS-RAS in IEEE-GCCE-2019 Japan. He has been a Guest Editor of Springer MONET and *Inderscience Business Intelligence Journal*. He is also an Active Reviewer for high cited and highly ranked international journals, including *MONET* (Springer), *IET Wireless Sensor Systems*, *IEEE Communication Magazine*, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE ACCESS, and *Future Generation Computer Systems*.

ZHIYUAN TAN received the B.Eng., M.Eng., and Ph.D. degrees.

He currently holds a Lectureship of cyber security at the School of Computing, Edinburgh Napier University (ENU), U.K. He is also an EAI and BCS Member. Prior to joining ENU, in 2016, he held different research positions at three research intensive universities. He was a Postdoctoral Researcher of cybersecurity with the University of Twente (UT), The Netherlands, from 2014 to 2016, a Research Associate with the University of Technology, Sydney (UTS), Australia, in 2014; and a Senior Research Assistant with La Trobe University, Australia, in 2013. His research interests include cybersecurity, machine learning, pattern recognition, data analytics, virtualization, and cyber-physical system. He has played various Chair roles at International workshops and conferences, such as SECSOC, SITN, EAI Future 5V, and EAI BD:TA 2018. He serves on the Editorial Board of the International Journal of Computer Sciences and its Applications. He is currently an Associate Editor of IEEE ACCESS and has organised Special Issues for *Ad Hoc and Sensor Wireless Networks Journal*, *International Journal of Distributed Sensor Networks*, *Computers and Electrical Engineering*, and IEEE ACCESS.

ATEEQ UR REHMAN received the Ph.D. degree from the University of Southampton, in 2017. He is currently an Assistant Professor of computer science with Abdul Wali Khan University Mardan, KPK, Pakistan. He has an interdisciplinary background in optical and wireless communication. As a Ph.D. student, he was with the Southampton Wireless Research Group, University of Southampton, where he focused reliable data transmission in Cognitive Radio Networks. He was a recipient of the several academic awards, such as the Faculty development program, Islamic University of Technology (OIC) Dhaka, Bangladesh Distinction Award and the Higher Education Commission Pakistan OIC Scholarship for undergraduate studies. His main research interests include next-generation wireless communications and cognitive radio networks, particularly cross layer approach and Hybrid ARQ, the Internet of Things, the Internet of Vehicles, and blockchain technology.



JOSEPH M. CHUMA received the B.Eng. degree in electrical and electronic engineering from the University of Nottingham, U.K., in 1992, and the M.Sc. degree in telecommunications and information systems and the Ph.D. degree in electronic systems engineering from the University of Essex, U.K., in 1995 and 2001, respectively. He is currently the Head of the Department and an Associate Professor of telecommunication and wireless communications with the Department of Electrical, Computer and Telecommunications Engineering, Botswana International University of Science and Technology. His main research interests include design of compact single and dual mode dielectric resonator filters for mobile and wireless communications. His research work has led to successful results in the development of dielectric loaded filters and shown that the size of the conventional combline filter can be reduced in excess of 75%. In this example, a dielectric ring has been used to load a conventional combline resonator. He has served as the Dean and the Deputy Dean of the Faculty of Engineering and Technology, University of Botswana. He is also serving as the Vice Chairman of the Botswana Communications Regulatory Authority Board, the Chairman of the Professional Assessment Committee of the Electrical Discipline of the Botswana Engineers Registration Board, and a member of the Registration Committee of Botswana Engineers Registration Board. He has served as a Postgraduate and Undergraduate External Examiner in a number of Universities.

MIAN AHMAD JAN received the Ph.D. degree in computer systems from the University of Technology Sydney (UTS), Australia, in 2016. He is currently an Assistant Professor with the Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan. His research interests include security and privacy in the Internet of Things and wireless sensor networks. His research has been published in various prestigious IEEE Transactions and Elsevier Journals. He was a recipient of various prestigious scholarship during his studies, notably the International Research Scholarship (IRS), UTS, and the Commonwealth Scientific Industrial Research Organization (CSIRO) Scholarships. He was awarded the Best Researcher Award, at the UTS, Australia, in 2014. He has been the General Co-Chair of Springer/EAI 2nd International Conference on Future Intelligent Vehicular Technologies, in 2017. He has been Guest Editor of numerous special issues in various prestigious journals, such as *Elsevier Future Generation Computer Systems*, *Springer Mobile Networks and Applications* (MONET), *Ad Hoc and Sensor Wireless Networks*, and *MDPI Information*.

MUHAMMAD BABAR is currently an Assistant Professor with Iqra University, Islamabad, Pakistan. His research interests include big data analytics, the Internet of Things, smart city design and planning, security and privacy, and social web of things. He has published his research work in various IEEE and ACM/Springer International conferences and journals.